HARVARD INTERNATIONAL LAW JOURNAL

FEATURE ARTICLE
DECEMBER 2012

Online
Volume 54

International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed

Michael N. Schmitt[1]

In 2011, the White House issued the *International Strategy for Cyberspace*, which noted that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[2] However, the document cautioned

[1] *Chairman and Professor, Department of Law, United States Naval War College. Professor Schmitt is also Honorary Professor at Durham University in the United Kingdom and former Dean of the Marshall Center in Germany. From 2009–2012, he served as Director of the NATO Cooperative Cyber Defence Centre of Excellence's Tallinn Manual project. The views expressed in this article are those of the author in his personal capacity and do not necessarily reflect those of the United States government.*

[2] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), *available at*

that the "unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."[3]

On September 18, 2012, State Department Legal Adviser Harold Koh took an important step towards publically elucidating the U.S. positions on how international law applies to cyberspace.[4] At a conference sponsored by United States Cyber Command (USCYBERCOM), Mr. Koh offered brief answers to what he labeled the "fundamental questions" on the issue. He also identified several "unresolved questions" with which the United States would likely be forced to grapple in the future. Since the speech had been fully cleared in the interagency process, it can be viewed as reflecting the U.S. Government's views on the issues, not just those of Mr. Koh or the State Department.

The timing of the speech was propitious. Less than three weeks earlier, NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) had released a draft the long-awaited *Tallinn Manual*, due for formal publication in early 2013.[5] The Manual is the product of a three-year project sponsored by the Centre in which an "International Group of Experts" examined, *inter alia*, the very issues cited in the Koh Speech, supra note 4. Participants included distinguished legal academics and practitioners, supported by a team of technical experts.[6] USCYBERCOM, the

---

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[3] *Id.*

[4] Harold Honhgu Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm. A footnoted version of the Koh Address is forthcoming on the Harvard International Law Journal Online. 54 Harv. Int'l L.J. Online 1 (Forthcoming, 2012). The United States has participated in meetings of the U.N. "Group of Governmental Experts" on cyber issues. It provided a paper on the U.S. position which was largely appended to the 2011 report issued by the Group. United Nations, *Developments in the Field of Information and Telecommunications in the Context of International Security 31* (2011), http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf (hereinafter GGE Report). Of note was the U.S. acceptance of the applicability of the *jus ad bellum* and *jus in bello* to activities in cyberspace. *Id.* at 35–37. Note that the U.S. submission was, on matters of law, somewhat less detailed than the Koh speech and not draw significant attention beyond the expert community.

[5] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, gen. ed., forthcoming Cambridge University Press 2013), http://www.ccdcoe.org/249.html.

[6] Although numerous members of the group were serving in senior posts in their countries, all participated in their personal capacity.

International Committee of the Red Cross, and NATO each provided an observer who participated actively throughout the project, albeit in a non-voting capacity.

The *Tallinn Manual* consists of "rules" adopted unanimously by the International Group of Experts that are meant to reflect customary international law, accompanied by "commentary" that delineates their legal basis and highlights any differences of opinion among the Experts as to their interpretation in the cyber context. A select group of peer reviewers offered comments on the various drafts, as did a number of states that were willing to informally and unofficially do so. The author served as Director of the Project.

The relative congruency between the U.S. Government's views, as reflected in the Koh speech, and those of the International Group of Experts is striking. This confluence of a state's expression of *opinio juris* with a work constituting "the teachings of the most highly qualified publicists of the various nations" significantly enhances the persuasiveness of common conclusions. [7] Of course, the limited differences that exist as to particular points of law render the respective positions on those points somewhat less compelling.

This article serves two purposes. First, it functions as a concordance between the positions articulated in the Koh speech and those found in the *Tallinn Manual.* The comparison is particularly apropos in light of the parallels in their content. Second, drawing on the *Tallinn Manual*, the article provides analytical granularity as to the legal basis for the positions proffered in the Koh Speech, supra note 4. In doing so, it usefully catalogues the various competing interpretive perspectives. The article is crafted around Mr. Koh's "Questions and Answers," which are reordered topically and set forth at the beginning of each section.

I. APPLICABILITY OF INTERNATIONAL LAW

"Do established principles of international law apply to cyber space? Yes, international law principles do apply in cyberspace."

"Is cyber-space a 'law-free' zone where anything goes? Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraints."

"Do *jus in bello* rules apply to computer network attack? Yes. In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity

---

[7] Statute of the International Court of Justice, art. 38(1)(d), June 26, 1945, 59 Stat. 1055.

and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances."[8]

The *sine qua non* issue for the *Tallinn Manual* was whether international law applies to cyber activities at all, for absent an affirmative response the project would have been pointless. In unanimously agreeing that it does, the International Group of Experts adopted precisely the same position as the U.S. Government on each of the answers set forth above. Since their work was focused on cyber conflict, the Experts took particular note of the International Court of Justice's *Nuclear Weapons* Advisory Opinion.[9] In that case, the Court had to consider whether the prohibition on the use of force found in Article 2(4) and related articles of the U.N. Charter (elements of the *jus ad bellum*) governed the use of nuclear weapons.[10] It opined that they "apply to any use of force, regardless of the weapons employed."[11] Applying this normative logic analogously, the Experts concluded, "the mere fact that a computer (rather than a more traditional weapon, weapon system, or platform) is used during an operation has no bearing on whether that operation amounts to a 'use of force'. Similarly, it has no bearing on whether a State may use force in self-defence."[12]

The International Group of Experts espoused the same view with regard to the *jus in bello* (international humanitarian law), which the International Court of Justice did not hesitate to apply to nuclear weapons. It began by highlighting the well-known pronouncement in the 1907 Hague Convention IV Regulations that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[13] The Court then turned to the "cardinal" international humanitarian law principles of distinction and unnecessary suffering as baselines for analyzing the legality of the use of nuclear weapons.[14] This approach confirmed that, for the Court, international humanitarian treaty and customary law that predated the fielding of nuclear weapons governs their

---

[8]Koh Speech, *supra* note 4, at 2–4

[9] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (hereinafter, Nuclear Weapons).

[10] *Id.*; U.N. Charter art. 2, para. 4; art. 51; art. 42. The text of the first two articles is set forth in the text accompanying sec. II and III, respectively. Article 42 provides, in relevant part, that "[s]hould the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."

[11] Nuclear Weapons, *supra* note 8, para. 39.

[12] Tallinn Manual, *supra* note 5, para. 1 of commentary accompanying chapeau to ch. II.

[13] Nuclear Weapons, *supra* note 8, para. 77, *citing* 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. 22, Oct. 18, 1907, 36 Stat. 2277.

[14] Nuclear Weapons, *supra* note 8, para. 78.

employment. The Experts found no reason to deviate from this position in the cyber context.

Like the International Court of Justice in the *Nuclear Weapons* Advisory Opinion, the International Group of Experts also emphasized the Martens Clause's relevance to cyber operations.[15] The clause, which first appeared in the 1899 Hague Convention II, finds its contemporary expression in the 1977 Additional Protocol I to the 1949 Geneva Conventions: "[i]n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[16] For over a century, therefore, it has been well accepted that a lack of directly applicable treaty law does not create an international humanitarian law-free zone. Indeed, international humanitarian law's requirement for a legal review of weapons prior to fielding, which is discussed below, confirms the fact that cyber weapons, as with other new weapons, are subject to preexisting law.[17]

Simply put, the Experts rejected any characterization of cyberspace as a distinct domain subject to a discrete body of law. The fulcrum of their conclusion was the fact that a person located at a particular place uses tangible cyber infrastructure to conduct cyber activities.[18] Application of international law to cyber activities is accordingly a matter of identifying the relevant legal principles that bear on the person, place, object, or type of activity in question.

Although there was no dissent over international law's applicability, it became clear during the project's proceedings that interpretation of international law norms in the cyber context can be challenging. For instance, crafting a consensus understanding of how international humanitarian law's definition of "attacks" applies to cyber operations proved arduous. The Experts also discovered that applying international law principles to cyberspace raises many of the same controversies that attend their application on land, at sea, or in the air. The best illustration of this reality concerns the dispute over "war-sustaining" military objectives. The debates on both issues are discussed below. In light of these are similar challenges, the Experts involved in drafting the *Tallinn Manual* would emphatically agree with Mr. Koh's assertion that

---

[15] *Id.*; Tallinn Manual, *supra* note 5, R. 20 cmt. 10.
[16] Convention (II) with Respect to the Laws and Customs of War on Land, pmbl., July 29, 1899, 22 Stat. 1803; Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), art. 1(2), June 8, 1977, 1125 U.N.T.S. 3.
[17] Additional Protocol I, art. 36; Tallinn Manual, *supra* note 5, R. 48.
[18] Tallinn Manual, *supra* note 5, para. 2 of commentary accompanying chapeau to Part 1.

"we must articulate and build consensus around how [international law] applies and reassess from there whether and what additional understandings are needed."[19]

II. THE USE OF FORCE

"**Do cyber activities ever constitute a use of force? Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law."**

"How can a use of force regime take into account all of the novel kinds of *effects* that States can produce through the click of a button? Unresolved."[20]

International law's prohibition of the use of force is set forth in Article 2(4) of the U.N. Charter: "All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[21] The article undoubtedly represents a norm of customary international law.[22]

In *jus ad bellum* analyses, the notion of "use of a force" is often confused that of "armed attack." The former bears on whether an action violates international law as codified in Article 2(4). By contrast, act(s) that cross the armed attack threshold found in Article 51 of the U.N. Charter (and customary international law) concern a target-state's entitlement to respond defensively with its own kinetic or cyber use of force. Moreover, while the use of force prohibition only applies to the acts of states (or those attributable to states under the law of state responsibility), the right of self-defense arguably encompasses attacks mounted by nonstate actors.[23]

Although it is incontrovertible that the prohibition on the use of force applies to cyber operations, the question remains as to when such operations amount to uses of force, such that they are prohibited absent one of the two recognized exceptions to

---

[19] Koh Speech, *supra* note 4, at 3, 7.
[20] *Id.*
[21] U.N. Charter, art. 2, para. 4.
[22] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, (hereinafter, Nuclear Weapons) at para. 188–90.
[23] See Tallinn Manual, s*upra* note 5, R. 10 cmt. 5, R. 13 cmt. 16, for a discussion setting forth the specifics of this issue.

the prohibition (self-defense and mandate or authorization by the Security Council).[24] For the U.S. Government, the physical effects of a cyber operation are the key. In particular, Mr. Koh asserted that "[c]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[25] For him, it is a matter of common sense: "if the physical consequences of a cyber attack work the kind of physical damages that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force." Mr. Koh goes on to suggest that "[i]n 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."[26]

The International Group of Experts came to a similar conclusion regarding physical effects in the *Tallinn Manual*: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[27] For the Experts, "[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force,"[28] so long as the effects are not trivial in nature and the cyber operations have been carried out by, or are attributable to, a state. The Experts were even more categorical than Mr. Koh, who cautiously noted that such acts "would likely be viewed" as uses of force, and suggested that factors such as those mentioned above would have to be evaluated when making the use of force determination.[29] Despite the minor difference in confidence level, the U.S. Government and the International Group of Experts would likely come to the same conclusions in specific cases. For instance, Mr. Koh cited cyber operations triggering a nuclear plant meltdown, opening a dam upriver from a populated area, and disabling air-traffic control as examples of uses of force.[30] The Experts discussed these very examples during their sessions.

As pointed out in the speech, some cyber incidents lack a clear kinetic parallel. Most noteworthy are those involving cyber operations that do not result in physical damage or injury. With regard to these incidents, the Experts took the position that "[a] use of force need not involve the employment of military or other armed forces by the

---

[24] U.N. Charter, arts. 42 & 51.
[25] Koh Speech, *supra* note 4, at 4.
[26] *Id.*
[27] Tallinn Manual, s*upra* note 5, R. 11. Note that the phrase "scale and effects" is drawn from Nicaragua, *supra* note 20, para. 195. Although the International Court of Justice used it there with reference to the "armed attack" standard of Article 51, the International Group of Experts also found it a useful approach with respect to evaluating potential uses of forces.
[28] Tallinn Manual, s*upra* note 5, R. 11 cmt. 8.
[29] Koh Speech, *supra* note 4, at 4.
[30] *Id.*

State in question."[31] As support, they pointed to the *Nicaragua* case, in which the International Court of Justice held that although merely funding guerrillas who were conducting hostilities against another State did not reach the use of force threshold, arming and training them did.[32] The holding suggests that an act need not have immediate physical consequences to comprise a use of force.

While this may be so, the dilemma of how to determine where the use of force threshold lies in cases not involving physical harm remains unresolved. Given the absence of a definitive threshold, the International Group of Experts adopted an approach that seeks to determine the probability that States (and others) will characterize a cyber operation as a use of force. They identified eight key non-exclusive factors likely to be considered on a case-by-case basis during such assessments.[33]

Of these, the most significant is "severity". Indeed, as noted, a cyber operation that results in damage, destruction, injury, or death is "highly likely to be considered a use of force" irrespective of the other factors.[34] Those other factors include: immediacy (the speed with which consequences manifest), directness (the causal relation between a cyber operation and its consequences), invasiveness (the degree to which a cyber operation intrudes into targeted systems), measurability of the effects, military character of the cyber operation, extent of State involvement, and presumptive legality (acts not expressly prohibited by international law).[35] Depending on the circumstances, additional factors like the prevailing political environment, whether the operations portend imminent military force, the attacker's identity, the attacker's cyber operations track record, and the nature of the target could also prove influential.[36] Based on the aforementioned factors and the *Nicaragua* judgment, the Experts concluded, for example, that providing an organized armed group with malware to be used against another State would constitute a use of force, whereas merely providing sanctuary to that group would, for a majority of the Experts, not rise to that level.[37] Ultimately every determination depends on a holistic assessment of the incident in light of the attendant circumstances.

---

[31] Tallinn Manual, s*upra* note 5, R. 11 cmt. 4.
[32] Nicaragua, *supra* note 18, para. 228.
[33] Tallinn Manual, s*upra* note 5, R. 11 cmt. 9.
[34] *Id.*
[35] *Id.*
[36] Tallinn Manual, s*upra* note 5, R. 11 cmt. 10.
[37] Tallinn Manual, s*upra* note 5, R. 11 cmts. 4,5.

III. SELF-DEFENSE

"May a State ever respond to a computer network attack by exercising a right of national self-defense? Yes. A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."[38]

Article 51 of the United Nations Charter sets forth the right of self-defense: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." In his speech, Mr. Koh reiterated the U.S. position on self-defense against a cyber armed attack, one that had previously been announced in the *International Strategy for Cyberspace*: "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[39]

The *Tallinn Manual* is in accord. It provides that "[a] State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense."[40] The Experts and the US Government agree that cyber operations that kill or seriously injure individuals or cause serious damage to objects qualify as armed attacks. Defensive actions are, as with kinetic actions, subject to the requirements of necessity, proportionality, imminency, and immediacy.[41]

The question remains, however, as to when a cyber operation amounts to an armed attack. On this point, the U.S. Government and the International Group of Experts part ways. The government is of the view that "the inherent right of self-defense potentially applies against *any* illegal use of force.… [T]here is no threshold for a use

---

[38] Koh Speech, *supra* note 4, at 4.

[39] The *International Strategy for Cyberspace* notes: "The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace." International Strategy for Cyberspace, *supra* note 3, at 9.

[40] Tallinn Manual, s*upra* note 5, R. 13.

[41] *Id.*, R. 13– 5. *See also* Nicaragua, s*upra* note 20, paras. 176, 194; Nuclear Weapons, s*upra* note 8, para. 41; Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, at paras. 43, 73–74, 76; 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 (1950), at 435 (referring to the *Caroline* formula).

of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[42] This has long been its official position.[43]

No member of the International Group of Experts agreed that an armed attack was nothing more than a use of force, *sans plus*. Instead, they endorsed the International Court of Justice's requirement to "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less great forms."[44] In other words, whereas all armed attacks are uses of force, not all uses of force are armed attacks. Whether a cyber use of force qualifies as an armed attack depends on its "scale and effects."[45]

Uncertainty as to what those scale and effects are plagued the *Tallinn Manual* deliberations. The Experts observed, for instance, that the International Court of Justice differentiated a "mere frontier incident" from an armed attack,[46] but later opined that an attack on a single warship might qualify as an armed attack.[47] Such inexplicable distinctions obfuscated their attempt to identify practicable legal thresholds.

Most of the Experts adopted "serious death, injury, damage, or destruction" as the apposite effects-based threshold for armed attack.[48] However, several argued that the severity of a cyber operation's effects was of greater relevance in qualifying it as an armed attack than their physical nature. For instance, although a massive cyber operation against the economy might cause no physical harm, the magnitude of its economic impact would better justify characterizing the operation as an armed attack than would limited physical damage.[49] In their opinion, it was incongruent, and therefore contrary to the object and purpose of the right to self-defense, to characterize the latter as an armed attack, and not the former. The other Experts were willing to entertain the prospect of States eventually accepting this interpretive approach, but believed that it presently represented *lex ferenda*, not *lex lata*.[50]

The International Group of Experts also examined the possibility of a State being targeted by multiple cyber operations, none of which alone rise to the level of an armed attack. May "pinprick attacks" be amalgamated for the purpose of finding an

---

[42] Koh Speech, *supra* note 4, at 7.

[43] *See, e.g.,* Abraham D. Sofaer, *International Law and the Use of Force*, *in* 82 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 420, 422 (1988). Sofaer was at the time the State Department's Legal Adviser.

[44] Tallinn Manual, *supra* note 5, R. 13 cmt. 6, *citing* Nicaragua, s*upra* note 20, para. 191.

[45] *Id*., para. 195.

[46] *Id.*

[47] Oil Platforms, s*upra* note 41, paras. 57, 61.

[48] Tallinn Manual, *supra* note 5, R. 13, para. 6.

[49] Tallinn Manual, *supra* note 5, R. 13, para. 9.

[50] *Id.*

armed attack? The Experts agreed that pursuant to the "accumulation of effects" theory, combining effects to meet the armed attack threshold is appropriate so long as the cyber operations are conducted by the same attacker (or attackers operating in concert), are related in terms of objective, and satisfy the requisite scale and effects threshold.[51]

As reflected in the Koh speech, the US Government maintains that self-defense is permissible in the face of an imminent attack. Most members of the International Group of Experts also took the view that international law allows for "anticipatory self-defense". Accordingly, the *Tallinn Manual* notes that "[t]he right to use force in self-defense arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy."[52] By this approach, a State need not take the first "cyber hit" before acting to defend itself.

The devil is in the details. Some of the Experts who acknowledged the existence of a right of anticipatory self-defense adopted a strict temporal approach, one grounded in Secretary of State Daniel Webster's famed 19th Century assertion during the *Caroline* incident that the right of self-defense only applies when the "necessity of self-defense is instant, overwhelming, leaving no choice of means, and no moment for deliberation."[53] For these Experts, the legality of defensive actions taken anticipatorily is to be gauged by reference to the time that passes between the act in question and the pending armed attack that necessitated it.

However, the majority of the Experts were of the view that "a State may act in anticipatory self-defense against an armed attack, whether cyber or kinetic, once the attacker is clearly committed to launching an armed attack and the victim-State will lose its opportunity to effectively defend itself unless it acts."[54] For them, "[t]he critical question is not the temporal proximity of the anticipatory defensive action to the perspective armed attack, but whether a failure to act at that moment would

---

[51] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 13 cmt. 8. *See also* YORAM DINSTEIN, WAR AGGRESSION, AND SELF-DEFENCE 206 (5th ed., 2011).
[52] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 15. *See also* DEREK W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 188–189 (1958). *But see* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BETWEEN STATES 275–8 (1963); YORAM DINSTEIN, WAR AGGRESSION AND SELF DEFENCE 203–204 (5th ed. 2011). Imminency refers to the defensive measures taken before an armed attack has occurred, while immediacy refers to those taken following an armed attack.
[53] Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 INTERNATIONAL LAW DIGEST 412 (John Bassett Moore ed., 1906).
[54] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 15 cmt. 4.

reasonably be expected to result in that State being unable to defend itself effectively when that attack actually starts."[55]

The International Group of Experts flatly rejected the notion of "preventive" self-defense. An act amounts to preventive self-defense if undertaken when the prospective cyber attacker either lacks the capability to conduct an armed cyber attack or, despite possessing the capability, has not yet formed an intention to carry one out.[56] Since cyber armed attacks are relatively easy to mount, it is the latter requirement that is the most likely to bar the taking of defensive actions.

A critical issue in light of the ease with which devastating cyber attacks can sometimes be mounted is whether non-State actors, such as terrorist groups, are capable of launching a cyber armed attack as a matter of law. Although the Koh speech did not directly address the issue, the U.S. government had previously taken the position that they were.[57] It is well accepted that the actions of a non-State actor may under limited circumstances be attributed to a State such that the victim-State may respond in self-defense against the State sponsor. The International Court of Justice made this point in the *Nicaragua* judgment when it stated that the notion of armed attack includes "'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (*inter alia*) an actual armed attack conducted by regular forces, 'or its substantial involvement therein'."[58]

The more difficult question is whether a non-State actor's cyber operations that are not attributable to a State can nevertheless qualify as an armed attack justifying a defensive response at the level of a use of force against that non-State actor. The majority of the International Group of Experts were of the view that such attacks can so qualify, assuming the operations are conducted by an organized group (rather than isolated individuals), generate consequences of the requisite scale and effects, and are directed against a State[59] They based their conclusion on the reaction of the international community to major terrorist attacks, especially those of 9/11. States treated the terrorist attacks as armed attacks that could be responded to in self-defense despite the fact that the State support for the terrorists fell well below the

---

[55] *Id.*

[56] Some of the Experts adopted the position that a State that lacks the capability may nevertheless be deemed to possess it at the point when the defending State will not be able to defend itself effectively unless it acts immediately. Even in such cases, the State acquiring the means in question must have decided to use it before the right of self-defense matures.

[57] GGE Report, *supra* note **Error! Bookmark not defined.**, at 36.

[58] Nicaragua, *supra* note **Error! Bookmark not defined.**, para. 195.

[59] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 11 cmt. 5.

Nicaragua threshold, or was non-existent altogether.[60] The Experts rejected the approach adopted by the International Court of Justice in the *Wall* opinion and the *Armed Activities in the Congo* judgment.[61] In those cases, the Court seemingly took the position that some nexus with a State at the *Nicaragua* level is required before the group's actions can be deemed an armed attack.

IV. THE *JUS IN BELLO*

"Must attacks distinguish between military and nonmilitary objectives? Yes. The *jus in bello* principle of distinction applies to computer network attacks undertaken in the context of an armed conflict."

"Must attacks adhere to the principle of proportionality? Yes. The *jus in bello* principle of proportionality applies to computer network attacks undertaken in the context of an armed conflict."

"What do we do about 'dual-use infrastructure' in cyberspace? Unresolved."

"How should States assess their cyber weapons? States should undertake a legal review of weapons, including those that employ a cyber capability."[62]

At the heart of international humanitarian law lies the principle of distinction.[63] Codified in Additional Protocol I, it requires that "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."[64] The applicability of this principal to cyber

---

[60] See discussion of this issue 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, 165–168 (Michael N. Schmitt & Jelena Pejic eds., 2007).
[61] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, para. 139 (July 9); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J.168, paras. 146–147 (Dec. 19). at.
[62] Koh Speech, *supra* note **Error! Bookmark not defined.**, at 5–8.
[63] Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 48. The principle derives from that set forth in the 1868 St. Petersburg Declaration: "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, Nov. 29/Dec. 11, 1868, 18 Martens Nouveau Recueil (ser. 1) 474.
[64] Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 48. That the principle is customary in nature is beyond question. For instance, the International Court of Justice has noted, "States must never make civilians the object of attack and must consequently never use

operations was acknowledged in the Koh speech and confirmed in the *Tallinn Manual*.[65]

International humanitarian law operationalizes the general principle of distinction by prohibiting attacks against specified protected persons and objects, imposing restrictions on how attacks may be conducted, and setting a limit on the extent of incidental harm to civilians and civilian objects that may be caused during an attack.[66] For instance, it is prohibited to attack civilians who are not directly participating in hostilities or civilian objects that have not been transformed into military objectives through either use or purpose.[67] What is of particular importance is that many of the rules governing the conduct of hostilities are framed in terms of "attacks". This term, which must be distinguished from the term "armed attack" in the *jus ad bellum* context, was the focus of great attention during the drafting of the Manual.

Additional Protocol I to the 1949 Geneva Conventions defines "attacks" as "acts of violence against the adversary, whether in offence or in defence."[68] The Experts unanimously agreed that although cyber operations are not violent in the sense of releasing kinetic energy, the term attack should logically be interpreted as extending to non-kinetic actions having violent *consequences*, specifically injury to or death of persons or damage to or destruction of objects.[69] However, they were sharply split as to whether the notion of attack included acts having consequences falling below that threshold. After three years of vigorous debate, the majority of the Experts adopted an interpretation that characterizes "interference with functionality" as damage to an object if "restoration of functionality requires replacement of physical components."[70] Most of these Experts would also characterize interference with functionality that necessitates re-installation of the operating system as damage.[71]

Consider the significance of this interpretation; cyber operations directed against civilian computer systems do not violate the prohibition on attacking civilian objects unless they qualify as an attack by virtue of their consequences. The paradigmatic case is a cyber psychological operation (PSYOP) that involves denial of services, but causes no physical damage. Similarly, the incidental effects of a cyber attack against a lawful military objective need not be considered when assessing proportionality

---

weapons that are incapable of distinguishing between civilian and military targets." Nuclear Weapons, *supra* note **Error! Bookmark not defined.**, para. 78.

[65] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 31.

[66] *See, e.g.,* Additional Protocol I, *supra* note **Error! Bookmark not defined.**, pt. IV, sec. I.

[67] *Id.,* arts. 51 & 52; I INTERNATIONAL COMMITTEE OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005), Rs. 1 & 7.

[68] Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 49(1).

[69] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 13 cmt. 3.

[70] *Id.*, R. 30.

[71] Id., R. 30 cmt. 11.

(discussed below) or the requirement to minimize civilian harm if those effects do not include physical damage or interference with functionality.[72]

The Experts also struggled with the importunate controversy over the meaning of the term "military objectives." As discussed, international humanitarian law requires an attacker to distinguish between military objectives and civilian objects; attacks are permissible only against the former. Civilian objects are defined in the negative as objects which do not qualify as military objectives.[73] Military objectives are "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 advantage."[74] For example, a military computer network and a civilian server used to transmit military data are both military objectives.

The United States, unlike most other States, takes the position that the aforementioned definition of military objectives encompasses not only objects that are "war-fighting and war-supporting," but also those that are "war-sustaining," such as oil-production facilities in a country that relies on oil export profits to finance its war effort.[75] Inability to agree on whether the concept of military objectives extends to war-sustaining objects has significant implications with respect to cyber operations because such targets tend to be especially vulnerable to cyber attack. The majority of the International Group of Experts rejected the US position, which was defended by a vocal minority.

---

[72] *See infra* sec. IV on proportionality. The requirement to take precautions in attack is codified for States Party in Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 57. Summarized, that article provides that an attacker must take all feasible measures to avoid collateral damage. Such measures include weapons, tactics, and target selection, as well as taking steps to verify the target and providing warnings when reasonable to do so. *See also* Customary International Humanitarian Law Study, *supra* note 67, Rs. 14–21.

[73] Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 52(1).

[74] *Id.*, art. 52(2).

[75] War-fighting refers to military equipment, such as military cyber attack systems. War-supporting objects are exemplified by a factory that produces war-fighting equipment. War-sustaining generally refers to economic targets, the destruction or neutralization of which would deprive the enemy of funds needed to carry on the war effort effectively. The most current US military international humanitarian law manual, the *Commander's Handbook on the Law of Naval Operations*, substitutes the phrase "war-fighting or war-sustaining capability" for "military action." U.S. NAVY/U.S. MARINE CORPS/U.S. COAST GUARD, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A para. 8.2 (2007).

As noted by Mr. Koh, international humanitarian law's rule of proportionality applies to cyber attacks conducted during an armed conflict.[76] The rule of proportionality is codified in Additional Protocol I.[77] As replicated in the *Tallinn Manual*, it provides that "[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."[78] The rule is extraordinarily difficult to apply in practice because it requires a comparative evaluation of two dissimilar entities: collateral damage and military advantage.

A number of issues as to application of the rule to cyber operations posed challenges for the Experts. In particular, the Experts had to determine the types of harm to civilians and civilian objects that constitutes as collateral damage in the proportionality analysis. They agreed that the standard of harm qualifying a cyber operation as an attack applies equally when identifying collateral damage. For the majority, this means that an attacker need only consider civilian death, injury, damage, or destruction during a cyber attack on a lawful military objective; inconvenience, irritation, stress, or fear do not bear on the proportionality assessment. Moreover, the majority of the Experts agreed that the mere loss of data does not amount to collateral damage unless the loss interferes with the functionality of the civilian object in question. The same logic would hold true with regard to effects on civilians and civilian objects qualifying as damage in the context of the separate requirement to minimize collateral damage during an otherwise lawful attack.[79]

An issue that sometimes arises in discussions of the rule of proportionality is whether an attack's indirect effects count as collateral damage. The issue is especially relevant with regard to cyber operations because the interconnectivity of cyber infrastructure heightens the likelihood that an attack against a military objective might have bleed over effects into civilian systems. The International Group of Experts agreed that collateral damage is not limited to the direct effects of a cyber attack (the effects experienced by the target system). Instead, they adopted a foreseeability test in which

---

[76] Koh Speech, *supra* note **Error! Bookmark not defined.**, at 4.
[77] Additional Protocol I, *supra* note 15, 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; Protocol (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) on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, art. 3(3), Oct. 10, 1980, 1342 U.N.T.S. 168; *Id.* as amended on May 3, 1996, art. 3(8), 2048 U.N.T.S. 133; Customary International Humanitarian Law Study, *supra* note 67, rule 14.
[78] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 51.
[79] *Id.*, Rs. 52–58; Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 57; Customary International Humanitarian Law Study, *supra* note 67, Rs. 15–21.

any foreseeable collateral effects on civilian systems have to be factored into the proportionality calculation.[80]

Mr. Koh highlighted the existence of widespread "dual-use infrastructure" in cyberspace, referring to cyber infrastructure that is shared by military and civilian users. He asserted that shared use raises issues as to the applicability of the proportionality rule and the rule prohibiting the use of civilian objects in order to shield military objectives from attack.[81] By contrast, the International Group of Experts did not find dual-use cyber infrastructure to be uniquely problematic as a matter of law. On the contrary, while the targeting of dual-use infrastructure can be complex, the same is true as to attacks on other dual-use targets like airfields, railheads, electrical networks, and communication systems.[82]

Mr. Koh's reference to shielding merits clarification. The prohibition only applies to civilians and a limited number of specified civilian objects, such as hospitals. [83] It is not expressly prohibited to use civilian objects as such. In any event, civilian cyber infrastructure would, as a practical matter, generally need to be "used" to effectively shield military transmissions. Once that occurs, the shielding issue becomes moot since "[a]n object used for both civilian and military purposes—including computers, computer networks, and cyber infrastructure—is a military objective."[84]

To the extent that civilians or civilian objects (that are not being used for military ends) are harmed during an attack on dual-use cyber infrastructure, the harm factors into the proportionality assessment and the determination of whether precautionary measures have to be taken in order to minimize collateral damage. The International Group of Experts identified two problematic situations in this regard.

---

[80] Their position appears to have been adopted by the United States. U.S. Commander's Handbook, *supra* note 75, para. 8.11.4 (stating in the context of cyber operations that indirect effects of an attack may be one of the factors included when weighing anticipated incidental injury or death to protected persons).
[81] Koh Speech, *supra* note **Error! Bookmark not defined.**, at 8.
[82] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 39.
[83] Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 51(7); Customary International Humanitarian Law Study, *supra* note 67, R. 97. *See also* Statute of the International Criminal Court, art. 8(2)(b)(xxiii), July 17, 1998, 2187 U.N.T.S. 90. As to prohibitions on using particular categories of persons or objects as shields, *see* Convention (III) Relative to the Treatment of Prisoners of War, art. 23, Aug. 12, 1949, 75 U.N.T.S. 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War, art. 28, Aug. 12, 1949, 75 U.N.T.S. 287; Additional Protocol I, *supra* note**Error! Bookmark not defined.**, art. 12(4).
[84] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, R. 39; *see also* Hague IV Regulations, *supra* note 12, art. 27; Additional Protocol I, *supra* note 15, art 52(2); Customary International Humanitarian Law Study, *supra* note 47, at 32.

First, it is sometimes impossible to identify the parts of a dual-use network over which military transmissions pass. The Experts concluded that in such cases the entire network qualifies as a military objective, much like a road network in which only certain roads are used by the enemy.[85] Second, the Experts struggled with the use of social networks for military purposes. In recent conflicts, Twitter, Facebook, and other social media have been used to transmit military information. The Experts agreed that such use would transform those facets of the social media networks that are used for military purposes into military objectives. [86] However, the entire networks would not be subject to direct attack. They also emphasized that the rule of proportionality and the requirement to take precautions in attack would provide the social networks a degree of protection. And, of course, the issues of targetability, proportionality, and precautions only arise when the consequences of the cyber operations are such that the operations qualify as attacks.[87]

Although the International Group of Experts disagreed with the assertion that the law governing dual-use cyber infrastructure is unresolved, the Experts concurred with Mr. Koh's view that cyber weapons should be subject to a legal review.[88] This requirement has been codified in Article 36 of Additional Protocol I, which the International Group of Experts, going further than Mr. Koh, believed reflective (in part) of customary international law.[89] For the purposes of the *Tallinn Manual*, the Experts defined cyber weapons as any "cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack."[90]

A unique aspect of cyber weapons is that they are sometimes developed for immediate operational use without going through the standard development, acquisition, and review cycle. For instance, military cyber operators may discover a vulnerability in the enemy's cyber infrastructure and immediately develop malware capable of exploiting it. The Experts took the position that in such cases the lawyer who provides advice to the commander of the unit employing the malware is responsible for conducting the legal review.[91] Similarly, if significant changes are made to a previously reviewed cyber weapon, further legal review by the commander's

---

[85] Tallinn Manual, *supra* note 5, R. 39 cmt. 3.
[86] *Id.*, R. 39 cmt. 4.
[87] *Id.*
[88] Tallinn Manual, *supra* note 5, R. 48(a).
[89] The Experts were only willing to characterize the requirement to review means of warfare (i.e., weapons), not methods of warfare (i.e. tactics), as customary. Consequently, Rule 48(b) of the *Tallinn Manual* applies only to States Party to Additional Protocol I. Tallinn Manual, *supra* note 5, R. 48(b).
[90] Tallinn Manual, *supra* note 5, R. 41 cmt. 2. The reference to cyber attack is to an attack in the jus in bello sense (Rule 30), rather than armed attack as that term as used in the jus ad bellum (Rule 13).
[91] *Id.,* R. 48 cmt. 8.

lawyer is required before it may be employed.[92] However, minor changes that do not significantly alter the operational effect of a cyber weapon do not require a formal legal review.[93]

A legal review of a cyber weapon considers, *inter alia,* whether:

(i) it is, in its normal or intended circumstances of use, of a nature to cause superfluous injury or unnecessary suffering; (ii) it is by nature indiscriminate; (iii) its use is intended or may be expected to breach law of armed conflict rules pertaining to the environment to which the State is Party; and (iv) there is any *ad hoc* provision of treaty or customary international law that directly addresses it.[94]

The process would normally include a review of the technical description of the cyber weapon, as well as consideration of its likely targets, the desired effect on the targets for which it has been designed, the dynamic by which the effects will be achieved, the likely scope of the effects, and the cyber weapon's precision when striking targeted cyber infrastructure.

V. SOVEREIGNTY

"In this analysis, what role does State sovereignty play? . . . States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict."[95]

The Koh speech dealt with a number of issues beyond the *jus ad bellum* and *jus in bello*, including sovereignty and State responsibility. The U.S. Government's position on sovereignty mirrors that of the International Group of Experts, which found that "no State may claim sovereignty over cyberspace *per se*" and that "States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[96] Sovereignty is "the right [within a State's territory] to exercise . . ., to the exclusion of any other State, the functions of a State."[97] Those functions include the right to exercise legal and regulatory control over cyber infrastructure located on its territory. Territorial sovereignty also affords protection to cyber infrastructure under international law irrespective of whether it is owned privately or by the government.

---

[92] *Id.*
[93] *Id.,* R. 48 cmt. 9.
[94] *Id.,* R. 48 cmt. 10 (citations omitted).
[95] Koh Speech, *supra* note 4, at 6.
[96] *Id.,* R. 1 cmt. 1.
[97] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

In the exercise of its sovereign prerogatives, a State may shut down access to the Internet, so long as doing so complies with international human rights and telecommunications law. In particular, the Experts observed that "[t]he fact that cyber infrastructure located in a given State's territory is linked to the global telecommunications network cannot be interpreted as a waiver of its sovereign rights over that infrastructure."[98] Although they also agreed that a cyber operation violates a State's sovereignty if physical damage is caused to cyber infrastructure located in its territory, no consensus was reached as to whether the mere placement of malware causing no physical damage (as with malware designed to monitor activity) amounts to a violation.[99]

Sovereignty is the basis for the exercise of jurisdiction (the authority of a State to prescribe, enforce, and adjudicate) in international law. Consistent with general jurisdictional precepts, the *Tallinn Manual* provides that "a State may exercise its jurisdiction: (a) [o]ver persons engaged in cyber activities on its territory; (b) [o]ver cyber infrastructure located on its territory: and (c) [e]xtraterritorially, in accordance with international law."[100]

Two forms of territorial jurisdiction are especially significant in the cyber context—subjective and objective.[101] When a cyber operation has been initiated within a State's territory the state has subjective jurisdiction, irrespective of where the effects occur. Objective territorial jurisdiction grants a State jurisdiction over cyber operations initiated outside its territory mounted against cyber infrastructure within the territory.[102] The Experts recognized certain other potential bases for the exercise of extraterritorial jurisdiction over cyber activities. These, depending on the circumstances, include the nationality of the perpetrator (active personality), the nationality of the victim (passive personality), national security (protective principle), and violation of a universal norm of international law (universal jurisdiction).[103] The confluence of the various grounds for jurisdiction means that multiple States sometimes enjoy jurisdiction over a particular cyber incident.[104]

Sovereignty creates not only rights, but obligations. Accordingly, the *Tallinn Manual* provides that "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[105] This principle is well established in international

---

[98] Tallinn Manual, *supra* note 5, R. 1 cmt. 10.
[99] Tallinn Manual, *supra* note 5, R. 1 cmt. 6.
[100] *Id.,* R. 2.
[101] *Id.,* R. 1 cmt. 6.
[102] *Id.*
[103] *Id.,* R. 1 cmt. 8.
[104] *Id.,* R. 1 cmt. 9.
[105] *Id.,* R. 5.

law. In its very first case, *Corfu Channel*, the International Court of Justice held that a State may not "allow knowingly its territory to be used for acts contrary to the rights of other States."[106] The holding was consistent with that in the celebrated *Trail Smelter* case, in which the arbitral tribunal noted that "under the principles of international law. . . no State has the right to use or permit the use of its territory in… a manner as to cause injury. . . in or to the territory of another or the properties or persons therein, when the case is of serious consequence. . . ."[107]

The obligation unquestionably attaches whenever the cyber operations in question are underway and the State knows of them. For instance, a State would be obligated to take feasible measures to end cyber attacks launched by a terrorist group from its territory against other States. The duty extends to situations in which only private entities, such as Internet service providers, are capable of taking remedial action. In such cases, the State must act to compel those entities to do so. [108] The Experts differed with regard to the principle's application to prospective acts.[109] Whereas some were of the view that a State must take reasonable measures to ensure the harmful cyber activities are not carried out from its territory, others suggested that no such duty exists in international law.

During an international armed conflict, the law of neutrality governs these situations. Drawn in great part from the 1907 Hague Conventions and now customary in character, the law of neutrality balances the rights and obligations of neutral and belligerent States during armed conflicts.[110] Certain of its rules are especially germane to cyber operations.

First, "[t]he exercise of belligerent rights by cyber means in neutral territory is prohibited."[111] The prohibition on actions by parties to a conflict would encompass both conducting cyber operations from neutral territory and taking remote control of cyber infrastructure located in that territory and using it to conduct belligerent cyber operations.[112] Second, "[a] neutral State may not knowingly allow the exercise of belligerent rights by the parties to the conflict from cyber infrastructure located in its

---

[106] Corfu Channel Case (U.K v. Alb.) 1949 I.C.J. 4, 22.
[107] Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941).
[108] Tallinn Manual, *supra* note 5, R. 5 cmt. 9.
[109] Id., R. 5 cmt. 7.
[110] *See generally* 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 Hague Convention V]; Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415.
[111] Tallinn Manual, *supra* note 5, rule 92. This rule is based on Hague Convention V, *supra* note 109, arts. 2 & 3, and Hague Convention XIII, *supra* note 84, arts. 2 & 5.
[112] Tallinn Manual, *supra* note 5, R. 92 cmt. 2.

territory or under its exclusive control."[113] The Experts agreed that an exception to this rule applies in the case of "public, internationally and openly accessible networks, such as the internet."[114] Should a neutral State decide to impose restrictions on the use of such a network, it must do so impartially.[115] Third, "[i]f 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."[116] Before a belligerent may act pursuant to this rule, the violation of neutral territory involved must be "serious."[117]

VI. STATE RESPONSIBILITY

"Are States responsible when cyber acts are undertaken through proxies? . . . Yes. States are legally responsible for activities undertaken through 'proxy actors,' who act on the State's instructions or under its direction or control."

"How do we address the problem of attribution in cyberspace?" Unresolved.[118]

The *Tallinn Manual* includes a number of rules drawn from the law of State responsibility, which the U.S. Government and the International Group of Experts agreed applies in cyberspace. In great part, they reflect relevant aspects of the International Law Commission's Articles on State Responsibility.[119] Although the Articles are not hard law, the document, which the General Assembly adopted in 2001, was considered by the Experts to accurately capture the customary international law of state responsibility.[120]

---

[113] Tallinn Manual, *supra* note 5, R. 93 (based on Hague Convention V, *supra* note 109, art. 5).
[114] *Id.,* R. 93 cmt. 3.
[115] *Id.,* R. 93 cmt. 3 (citing Hague Convention V, *supra* note 84, art. 9).
[116] *Id.,* R. 94.
[117] *Id.,* R. 94 cmt. 3; *see also* INTERNATIONAL INSTITUTE OF HUMANITARIAN LAW, SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995), *available at http://www.icrc.org/ihl.nsf/FULL/560?OpenDocument*, R. 22. For a belligerent to act, the conduct must also "represent an immediate threat to the security of the aggrieved party and there must be no feasible and timely alternative to taking action on neutral territory." Tallinn Manual, *supra* note 5, R. 94 cmt. 4.
[118] Koh Speech, *supra* note 4, at 6, 8.
[119] International Law Commission, Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, U.N. Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter Articles of State Responsibility].
[120] A three-year research project sponsored by the NATO Cooperative Cyber Defence Centre of Excellence will examine the subject of State responsibility for cyber operations in much greater depth. The author will serve as director of the project.

Under international law, "[a] State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[121] The obligation may derive from either treaty or customary international law, and its breach can consist of an omission or commission.[122]

Certain acts are self-evidently attributable to a State. Any wrongful act or omission undertaken by organs of the State, including *ultra vires* acts performed in an apparently official capacity, are automatically attributable to that State.[123] Similarly, acts or omissions of persons or entities authorized to act with governmental authority are attributable to the State granting that authority.[124] In the cyber context, the most common example is that of private Computer Emergency Response Teams authorized to defend government cyber infrastructure and networks.[125]

The Koh speech narrowed in on attribution of the cyber activities of non-State actors. According to the Articles on State Responsibility, "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[126] The International Group of Experts noted the lack of agreement as to the precise level of control necessary for attribution of a non-State actor's cyber operations to a State.[127] Although acknowledging that an "overall control" test finds some support in the International Criminal Tribunal for the Former Yugoslavia's Appeals Chamber judgment in *Tadić*,[128] the majority of the Experts, drawing on International Court of Justice jurisprudence, took the position that a State must have "effective control" over non-State actors for attribution to occur.[129] To reach the higher threshold, the State "needs to have issued specific instructions or directed or controlled a particular operation. . . .

---

[121] Tallinn Manual, *supra* note 5, R. 6. *See also* Articles of State Responsibility, *supra* note 118, art. 2.
[122] Tallinn Manual, *supra* note 5, R. 6 cmt. 8.
[123] Articles of State Responsibility, *supra* note 94, art. 4(1)–(2). On *ultra vires* acts, see *id.,* commentary accompanying art. 4. *Accord* Tallinn Manual, *supra* note 5, R. 6 cmt. 6.
[124] Articles of State Responsibility, *supra* note 92, art. 5. *Accord* Tallinn Manual, *supra* note 5, R. 6 cmt. 8.
[125] Tallinn Manual, *supra* note 5, R. 6 cmt. 8.
[126] Articles of State Responsibility, *supra* note 118, art. 8.
[127] Tallinn Manual, *supra* note 5, R. 6 cmt. 10.
[128] Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment ¶¶ 131, 145 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
[129] Nicaragua, *supra* note 18, ¶ 115; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro.), 2007 I.C.J. 43¶¶ 399–405. The Experts noted that the Tadić decision bore on the issue of whether an international armed conflict was underway, rather than State responsibility *per se*. *See* Tallinn Manual, *supra* note 5, R. 6 cmt. 11.

Merely encouraging or otherwise expressing support for the independent acts of non-State actors does not meet the…threshold."[130] As an example, State A would bear State responsibility for cyber operations conducted by a non-State group against State B if A provided cyber target data and the malware necessary to carry out the operations.

In his speech, Mr. Koh pointed to the "ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution." There are two facets to this issue. First, although the ability of an advanced cyber power to accurately identify the originator of a cyber operation is significantly greater than realized by the general public,[131] in certain cases tracing an operation to a State may be problematic. Second, it can sometimes be difficult to link a State to cyber operations conducted by a non-State actor. Cognizant of these challenges, the International Group of Experts offered guidelines designed to inform the process of determining whether an act or omission may be attributed to a State as a matter of law. In their view, "[t]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation."[132]Moreover, "[t]he fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State."[133] However, as noted by Mr. Koh, the hurdles tend to be technical or policy-oriented in nature, rather than legal.

VII. CONCLUDING OBSERVATIONS

It is hardly a jurisprudential epiphany to assert that international law applies fully formed to activities in cyberspace. This is particularly so once it is grasped that cyber activities involve individuals using tangible objects in physical domains that have long been subject to international law's normative architecture. It is quite remarkable, therefore, that it has taken States so long to state the obvious, and that the international legal community seemed to struggle so mightily with a rather straightforward issue.

In fact, the International Group of Experts who drafted the *Tallinn Manual* found no relevant body of law that was inapplicable to cyber activities. Be that as it may, the

---

[130] Tallinn Manual, *supra* note 5, R. 6 cmt. 11.
[131] "Potential [cyber] aggressors should be aware that the United States has the capacity to locate them and hold them accountable…." Armed Forces Press Service, *Panetta Spells Out DOD Roles in Cyberdefense* (Oct. 11, 2012), http://www.defense.gov//News/NewsArticle.aspx?ID=118187 (quoting Leon Panetta).
[132] Tallinn Manual, *supra* note 5, R. 7.
[133] *Id.*, R. 8.

unique nature of cyber activities, in particular the fact that they may have devastating results without causing physical injury or damage, can lead to interpretive uncertainty. The Koh speech and the *Tallinn Manual* are but initial forays into the demanding process of exploring how the extant norms of international law will apply in cyberspace. But the long overdue journey has at least finally begun.