The nature of international law cyber norms

Article

Published Version

THE TALLINN PAPERS

A NATO CCD COE Publication on Strategic Cyber Security

MICHAEL N. SCHMITT AND LIIS VIHUL

THE NATURE OF INTERNATIONAL LAW CYBER NORMS

Tallinn Paper No. 5
Special Expanded Issue
2014

Previously in This Series

No. 1 Kenneth Geers "Pandemonium: Nation States, National Security, and the Internet" (2014)

No. 2 Liis Vihul "The Liability of Software Manufacturers for Defective Products" (2014)

No. 3 Hannes Krause "NATO on Its Way Towards a Comfort Zone in Cyber Defence" (2014)

No. 4 Liina Areng "Lilliputian States in Digital Affairs and Cyber Security" (2014)

Roles and Responsibilities in Cyberspace

The theme of the 2014 Tallinn Papers is 'Roles and Responsibilities in Cyberspace'. Strategic developments in cyber security have often been frustrated by role assignment, whether in a domestic or international setting. The difficulty extends well beyond the formal distribution of roles and responsibilities between organisations and agencies. Ascertaining appropriate roles and responsibilities is also a matter of creating an architecture that is responsive to the peculiar challenges of cyberspace and that best effectuates strategies that have been devised to address them.

The 2014 Tallinn Papers address the issue from a variety of perspectives. Some of the articles tackle broad strategic questions like deliberating on the stance NATO should adopt in cyberspace matters, or exploring the role small states can play in this domain. Others touch upon narrower topics, such as the right to privacy in the growingly intrusive national security context and whether software manufacturers should be compelled to bear their burden of cyber security by making them liable for faulty software. The thread running through all the papers, however, is their future-looking approach, one designed to inspire discussion and undergird strategic development.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

The Nature of International Law Cyber Norms

Michael N. Schmitt[1] and Liis Vihul[2]

As with all human activity, that which takes place in cyberspace is shaped by a normative architecture consisting of related, but distinct, regimes. In the contemporary environment, policy norms loom largest, as illustrated by the issuance of national "cyber strategies"[3] and the work of intergovernmental bodies such as the United Nations.[4] Yet, other normative regimes are also beginning to influence the development of said architecture, as demonstrated by the fervent debates in the field of ethics over the proper balance between cyber security and cyber privacy, the ever-growing body of domestic legislation to govern intrastate cyber activities, and the increasing trend in favour of setting common technical standards to foster interoperability.

This article explores the nature, formation and evolution of international legal norms pertaining to cyber activities. At present, it is fair to say that this category of norms operates in the shadow of most others, a situation often attributed to the alleged paucity of international law applicable in cyberspace. After all, very few

1 Senior Fellow and Director, "Tallinn 2.0" Project, NATO Cooperative Cyber Defence Centre of Excellence; Charles H. Stockton Professor and Director, Stockton Center for the Study of International Law, United States Naval War College; Professor of Public International Law, Exeter University; Fellow, Harvard Law School Program on International Law and Armed Conflict. This article draws upon earlier research published as: Michael N. Schmitt & Liis Vihul, 'The Emergence of Legal Norms for Cyber Conflict', in *Binary Bullets: The Ethics of Cyberwarfare* (Fritz Allhoff, Adam Henschke & Bradley Jay Strawser, Oxford University Press, 2015). The views expressed are those of the authors in their personal capacity and do not necessarily reflect those of any institution with which they are affiliated.

2 Researcher and Project Manager, "Tallinn 2.0" Project, NATO Cooperative Cyber Defence Centre of Excellence.

3 See, e.g., White House, International Strategy for Cyberspace, May 11, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. For a compilation of national cyber strategies, see http://www.ccdcoe.org/strategies-policies.html.

4 See, e.g., the summary of work under the auspices of the United Nations at United Nations Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of Information Security, http://www.un.org/disarmament/topics/informationsecurity/. For a catalogue of international organisations' developments in the cyber sphere, see http://www.ccdcoe.org/incyder.html.

express cyber-specific rules of international law exist. However, such assertions display a misunderstanding of the content and operation of international law that this article is, in part, designed to alleviate.

Analysis will begin by introducing and situating the different types of legal norms in the international law framework. The inquiry's foundational premise is that the rules of international law governing cyber activities are identical to those applicable to other types of conduct. Any differences in their explication and application are the product of the unique nature of cyber activities, not a variation in the legal strictures that shape their content and usage.

The article will then briefly discuss certain terminology that has befuddled discussions about international law cyber norms. This brief detour is essential because the divergent language employed by the legal and non-legal communities is a source of much confusion in discourse about the relevant norms. Such dialogue is also often obfuscated by improper reference to various norms that reside in different fields of international law that are not on point in a particular case. Experience has demonstrated that an understanding of the key legal terminology is a precondition to any meaningful interchange between the various normative communities.

With the groundwork laid for substantive analysis of international legal norms, the article turns to how they emerge, are interpreted, and develop through time. Although the analysis applies to international law generally, emphasis will be placed on two bodies of international law: that governing when states may resort to force (the *jus ad bellum*) and that applying during an armed conflict (international humanitarian law). This is because it is in these legal regimes that the law, or at least contemporary understanding of the law, applicable to cyberspace is most developed. This reality is primarily the product of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*[5] that was produced under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) between 2010 and 2013. Comprehension of how other areas of international law apply to cyber activities is far less mature, a situation being addressed by the NATO CCD COE in its ongoing "Tallinn 2.0" project.[6]

Since legal norms reside in treaties or are found in customary international law, the examination will proceed by addressing each source of law separately,

5 *Tallinn Manual on the International Law Applicable to Cyber Warfare* [hereinafter *Tallinn Manual*], gen. ed. Michael N. Schmitt (New York: Cambridge University Press, 2013).

6 On the project, see NATO Cooperative Cyber Defence Centre of Excellence website, http://ccdcoe.org/research.html.

first in the abstract and then in its cyber context. Dividing the discussion of international law in this manner is useful because cyberspace poses different challenges to the formation, identification and application of each of these two sources of international law. General principles of law, which form the third source of international law, are unlikely to significantly inform the contours of international law directly applicable to cyberspace. They will therefore be addressed only briefly, before turning to the authors' final reflections on the subject.

The Nature and Place of International Legal Norms

Any consideration of the international community's legal architecture, including that applicable to activities in cyberspace, necessarily begins with Article 38 of the Statute of the International Court of Justice:

> 1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. international conventions, whether general or particular, establishing rules expressly recognised by the contesting states;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilised nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.[7]

Although situated in the constitutive document of a single international tribunal, the article, which tracks the formulation found in the 1920 statute of its predecessor, the Permanent Court of International Justice,[8] is today universally accepted as accurately setting forth the three forms of international law – treaty law, customary law and general principles of law. Subparagraph (d) delineates the two secondary sources used to elucidate that law: judicial decisions and the work of distinguished scholars.[9] It must be cautioned that secondary sources are not in themselves law. In particular, and unlike the practice in many domestic jurisdictions, the decisions of tribunals are binding only on the parties before the court, a fact codified in Article 59 of the Statute. Nevertheless, such decisions

7 Statute of the International Court of Justice, art. 38, June 26, 1945, 59 Stat. 1055, 33 UNTS 993 [hereinafter ICJ Statute].

8 Statute of the Permanent Court of International Justice art. 38, Dec. 16, 1920, 6 LNTS 379.

9 See, e.g., *Oppenheim's International Law*, I, 24 (Robert Jennings & Arthur Watts eds., 9th ed. 1996).

and scholarly works are highly persuasive in interpreting treaty provisions and identifying customary law. Indeed, considering the lack of cyber-specific customary and treaty law, scholarly works such as the *Tallinn Manual* are proving instrumental in identifying and shaping international legal cyber norms. So too is the case law of international judicial bodies, a fact illustrated by the frequent reference herein to their pronouncements.

International legal norms differ from other inter-state norms regulating cyber behaviour in the sense that in the event of non-compliance, international legal responsibility results.[10] The essence of this responsibility lies in the obligation to stop on-going violations and to provide reparations to the injured states for the harm caused. It is therefore important to carefully distinguish legal norms from non-binding norms. For instance, a "code of conduct", like that proposed by the Shanghai Cooperation Organisation,[11] seldom qualifies as international law because it is aspirational or exhortational in nature, but not compulsory. Codes of conduct or statements of best practice are not binding on states in the same manner as legal norms, and their violation does not involve the same remedies. While the sanctioning of violations of international legal norms is complicated by the general absence of a compulsory enforcement mechanism, states are nevertheless significantly more reluctant to breach legal, as opposed to other, types of norms.

Traditionally, norms of international law were viewed as binding only on states. It was left to individual states to address the conduct of individuals and organisations that fell under their personal jurisdiction when engaged in activities that were within their subject matter competency. Although international law continues to primarily govern international relations between states, in the last century it has increasingly come to address individual conduct. Classic examples include international legal norms that permit universal jurisdiction over certain acts such as war crimes. Nevertheless, to amount to international law, all such norms must be agreed to by multiple states, either through treaty or the development of customary law. In this sense, international law is at its core a body of compulsory norms involving two or more states.

10 Draft Articles on Responsibility of States for Internationally Wrongful Acts, art. 1, Rep. of the Int'l L. Comm'n, 53d Sess., U.N. Doc. A/56/10, GAOR 56th Sess., Supp. No. 10 (2001), reprinted in [2001] *Yearbook of the International Law Commission* 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles on State Responsibility].

11 Letter dated 12 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, Annex, UN Doc. A/66/359 (Sept. 14, 2011).

As noted above, there are three forms of international law – treaty law, customary law and general principles of law. Customary law is unwritten international law that develops over time and is based on state practice. Although unwritten, it binds all states, except those that fall into a very specific and narrow category of "persistent objector". Treaties, by which states expressly agree to be bound in law, may be bilateral (two states) or multinational (more than two parties), and treaty law may be coterminous with customary law in the sense that a treaty's provisions simply reflect customary law, or have come to reflect customary law that has subsequently emerged. However, conceptually it is useful to think of treaty law as consisting of express agreements that either recognise customary norms or create new legal norms that render an act or failure to act unlawful for the parties to the treaty. This latter point is key since the status of the customary law governing cyber activities remains rather unsettled.

A state may even consent by treaty to certain conduct that would otherwise constitute a violation of a customary norm, unless the customary norm is of *jus cogens* character, such as the prohibition on genocide which states may never agree to violate in their relations. For instance, although certain intrusions by a state into another state's cyber infrastructure may amount to a violation of the latter's sovereignty, that state may execute a bilateral or multilateral treaty that permits other states to do so in certain circumstances, such as during joint counter-terrorism operations. Additionally, a state may acquiesce to such a violation on an *ad hoc* basis, as when it has information that its cyber infrastructure is being used for criminal purposes, but lacks the ability to address the situation itself.

International law is typically described as prohibitory in nature: any activity that is not disallowed is generally permitted.[12] But even when law does exist, it may prove lacking when meeting unanticipated circumstances and thus is occasionally breached as part of the process of creating a new norm. Indeed, it is often said that customary law norms are "made in the breach". By way of illustration, it may be that pre-existing human rights law would, if logically applied in the cyber context, prohibit intrusions into certain forms of cyber communications between individuals. However, if states treat this customary norm as inconsistent with their need to ensure, for instance, the security of their cyber systems, they may begin to act contrary to the norm. Over time, their state practice, could, as will be explained, be viewed by states as legal, such that the original human rights norm will have been modified. Given the novelty of cyber activities, they are particularly vulnerable to this dynamic of customary law.

12 *S.S. 'Lotus' (Fr. v. Turk.)*, Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 3, 18 (Sept. 7).

Once the international law boundaries of conduct are demarcated, domestic legal, political (policy), ethical and other norms can operate to further restrict or require particular conduct in cyberspace. For instance, while it is unclear precisely how international human rights norms in the realm of privacy restrict state monitoring of personal cyber communications, monitoring may constitute a violation of domestic constitutional law or be contrary to state policy or the ethical benchmarks that a state has adopted. Thus, international legal norms merely define the space within which states may engage in normative construction. Of course, states may act to transform these non-legal norms into those with legal authority by adopting a treaty incorporating them or engaging in state practice that crystallises over time, as described below, into customary law.

Terminological Precision

To avoid cross-disciplinary confusion in understanding how legal norms are created for, and applied to, cyber activities, it is first necessary to grasp the relevant legal vocabulary. Indeed, perhaps the greatest hindrance to effective conversation between cyber norm communities is terminological in nature. To cite a simple but pervasive example, non-lawyers tend to speak of "cyber war" in a generic sense as encompassing all forms of hostile cyber activities conducted by or against states and use the term "cyber attacks" as referring to any harmful cyber operations. However, as will be seen, these terms do not formally reside in international law. Instead, international law uses a *patois* that employs the same words – attack and war – but has a discrete normative implication.

Of greatest significance in this regard are the legal terms of art populating the *jus ad bellum* and international humanitarian law (IHL). The *jus ad bellum* deals with the prohibition of the use of force found in Article 2(4) of the United Nations Charter and customary law, as well as the law of self-defence set forth in Article 51 and its customary law counterpart.[13] In contrast, IHL deals with how force may be employed by the parties to an armed conflict. IHL, in particular customary international law and the Geneva Conventions with their 1977

13 UN Charter, arts. 2(4) & 51.

Additional Protocols,[14] contains, *inter alia,* the rules governing attacks, delineates protections to which certain persons and objects are entitled, and restricts the kinds of weapons that may be employed in order to conduct hostilities.

With respect to the *jus ad bellum*, the primary terminological obstacle deals with the use of the word "attack". Article 51 of the UN Charter allows states to use force in self-defence in situations amounting to an "armed attack". Not all hostile cyber operations directed at a state rise to this level. As a general matter (the precise threshold is by no means settled), such operations must result in the destruction of property or injury to persons before qualifying as an armed attack that opens the door to a forceful response, whether kinetic or cyber in nature.[15] Thus, for the legal community, the term "cyber attack" in this context refers to a particularly egregious hostile cyber operation that allows for the most robust of state responses. To style operations of lesser consequences as "attacks" often results in the various normative communities talking past each other.

In IHL, there are two consistently pernicious terminological quagmires. The first involves use of the word "war", as in "cyber war". War is a historical term that no longer enjoys the normative meaning associated with it for centuries, when the fact that states were "at war" or had engaged in an "act of war" meant that certain bodies of law, such as the law of war and neutrality law, applied.

Since the mid-twentieth century the term has been obsolete in international law. It was intentionally discarded by the international community in lieu of "armed conflict" in the four 1949 Geneva Conventions.[16] This was done to emphasise that international humanitarian law applies irrespective of a declaration of war or other legalistic formalities. Henceforth, the determination that states were "at war" (involved in an armed conflict) would be factual.

It is clear that when cyber operations accompany kinetic hostilities qualifying

14 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field, August 12, 1949, 75 UNTS 31; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, August 12, 1949, 75 UNTS 85; Convention (III) Relative to the Treatment of Prisoners of War, August 12, 1949, 75 UNTS 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 UST 3516, 75 UNTS 287; 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 UNTS 3; Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 UNTS 609.

15 *Tallinn Manual, supra* note 5, r. 13 and accompanying commentary.

16 Geneva Conventions I – IV, *supra* note 14, arts. 2 & 3.

as armed conflict (as with the conflict between Russia and Georgia in 2008 or that taking place in Syria at the time of writing), IHL applies fully to all the cyber operations that have a nexus to the conflict, whether they are launched by states, non-state groups or individual hackers. For instance, in the same way that IHL prohibits injurious or destructive kinetic attacks against civilians and civilian objects, it likewise prohibits cyber attacks against them having the same effects.[17]

For international lawyers the term "cyber war" is better rendered as "cyber armed conflict". When non-lawyers speak of the norms applicable in cyber war, the lawyer will accordingly insist on examining the attendant circumstances, because only if they qualify as armed conflict will the specific international law norms applicable therein attach. Otherwise, the situation will be subject to those aspects of international law that apply during peacetime, such as the law of state responsibility and human rights law.

The second term that causes confusion between the normative communities is, again, "attack". As noted, "armed attack" is a legal term of art in the *jus ad bellum*. Yet, "attack" is also a legal term of art in IHL. The term does not simply refer to military operations directed by one belligerent against another during an armed conflict. Rather, it is defined in Article 49 of Additional Protocol I to the Geneva Conventions as "acts of violence against the adversary, whether in offence or in defence."[18] The *Tallinn Manual* accordingly defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[19]

The definition of an "attack" lies at the core of IHL, because many of its prohibitions are framed in terms of prohibition of attacks, the paradigmatic examples being those on directing attacks against civilians and civilian objects.[20] To the extent that a cyber operation does not qualify as an attack in the IHL regime, the prohibitions are inapplicable. Consequently, when a non-lawyer uses the term "cyber attack", clarification must be sought (in addition to the *jus ad bellum* issue outlined above) not only as to whether the operation occurred during an armed conflict such that IHL applies, but also whether the operation constitutes an attack such that IHL prohibitions and restrictions come into play.

Clearly, terminological indistinctness and imprecision have long hobbled

17 *Tallinn Manual, supra* note 5, rr. 32 & 37.

18 Additional Protocol I, *supra* note 14, art. 49(1).

19 *Tallinn Manual*, *supra* note 5, r. 30.

20 See the various prohibitions set forth in Additional Protocol I, *supra* note 14, part. IV.

interdisciplinary understanding between the legal and non-legal communities; they continue to do so today. A proper grasp of the international law governing cyber operations, and its likely future evolution, demands terminological fastidiousness. It is to that law that we now turn.

General Rules Governing Treaty Law

As noted, international legal norms bearing on cyber activities take two forms, the most commonly recognised by the non-legal community being treaty law. A treaty is an international agreement governed by international law.[21] Such agreements adopt many titles – protocol, agreement, convention, act, etc. So long as the parties to the agreement intended to create legally binding rights and obligations for themselves, the instrument's precise appellation is of no legal significance.[22]

The law that applies to the formation, application, and interpretation of an international agreement is identical irrespective of its subject matter. The law governing treaties is in great part captured in the Vienna Convention on the Law of Treaties.[23] While some states, such as the United States, are not party to the Convention, most of its provisions are viewed as reflective of customary international law, a topic examined below.

Of particular note in the cyber context is the principle that treaties are governed exclusively by international law, except in cases where the agreement itself refers to domestic law. The fact that a state's domestic law or even constitutional law disallows an action required by a treaty – or demands one prohibited by a treaty – does not excuse a state's non-compliance with the terms of the treaty. Indeed, a state may refuse to enforce an international law norm in its courts on the basis of domestic legal concerns, such as constitutional law. In states such as the United States that do not accept the supremacy of international over domestic law, doing so is sometimes domestically required by law. However, the violation by that state of the international legal norm remains a breach of international law attributable to the state.

Once a treaty has been successfully negotiated, states subsequently consent to be bound by it, which may occur through a number of means. Consent may be indicated through signature (but not in every case, since signature sometimes

21 Vienna Convention on the Law of Treaties art. 2(1)(a), May 23, 1969, 1155 UNTS 331.

22 *Id.*, art. 2(1)(a).

23 Vienna Convention on the Law of Treaties, *supra* note 21.

denotes only adoption), exchange of instruments, ratification, accession, or any other means that the parties agree upon.[24] State representatives sometimes sign treaties subject to ratification. In the United States, for instance, treaty-making power is vested in the President, but is subject to the "advice and consent" of the Senate.[25] In such a case, the state only becomes bound once the instrument is ratified. A state may also "accede" to a treaty when it did not participate in the negotiations leading to its adoption. Finally, a treaty usually specifies a particular date of its entry into force or includes a provision requiring a particular number of states to ratify the treaty before it comes into effect.[26]

These procedural requirements are important with respect to the application and evolution of legal norms, because it is not unusual for a treaty to be adopted and ratified by some states long before it comes into force. For instance, the Rome Statute of the International Criminal Court[27] was adopted in 1998, but only came into force when 60 states had ratified it, which did not happen until 2002. Pending a treaty coming into force, states that have signed it or otherwise expressed an intent to eventually be bound by it may not engage in activities that would defeat the treaty's object and purpose, unless they formally provide notification of their decision to not become a party thereto,[28] as was the case with the United States and the International Criminal Court Statute in 2002.[29] Accordingly, the fact that a treaty has not yet come into effect does not preclude it from having some normative significance. For instance, 89 states signed the 2012 International Telecommunication Regulations Treaty[30] at the World Conference on International Telecommunications in Dubai, United Arab Emirates. They must act in accordance with the treaty's object and purpose despite the fact that it will only come into effect on January 1, 2015.

States occasionally issue reservations to multilateral treaties when they consent to be bound by them.[31] Reservations act to exclude or modify treaty provisions

24 *Id.*, arts. 11-15.

25 US Const. art. II, sect. 2, cl. 2.

26 See, e.g., Vienna Convention on the Law of Treaties, *supra* note 21, art. 24.

27 Rome Statute of the International Criminal Court, July 17, 1998, 2187 UNTS 90.

28 Vienna Convention on the Law of Treaties, *supra* note 21, art. 18.

29 Press Statement, U.S. Department of State, Richard Boucher, Spokesman, International Criminal Court: Letter to UN Secretary General Kofi Annan, May 6, 2002, http://2001-2009.state.gov/r/pa/prs/ps/2002/9968.htm.

30 International Telecommunication Regulations, Dec. 9, 1988, S. Treaty Doc. No. 13, 102d Cong., 1st Sess. (1991).

31 Vienna Convention on the Law of Treaties, *supra* note 21, art. 19.

with respect to the state concerned.[32] Some treaties prohibit reservations altogether. Even when allowed, reservations cannot be inconsistent with the object and purpose of the treaty. If a state reserves, and another state accepts the reservation, the exclusion or modification of the provision in question operates with respect to the obligations of both states. Should a party to the treaty object to the reservation, the reservation will not come into effect between the parties concerned. An objecting state may also determine that a reservation is so objectionable that the treaty is not in force at all between it and the reserving state. It should be evident that reservations to a multilateral treaty can create an extremely complex maze of legal relationships.

In addition to reservations, states may issue interpretative declarations that clarify their position with regard to a particular provision of the treaty or to how the treaty will be applied by the states concerned. Declarations have no technical legal effect on the state's rights or obligations. However, states sometimes make interpretative declarations that *de facto* amount to reservations. For example, the United Kingdom has issued a statement concerning the prohibitions on reprisals set forth in Additional Protocol I to the 1949 Geneva Conventions.[33] The declaration arguably denudes certain provisions of their effect. Thus, declarations, like reservations, must always be carefully surveyed when evaluating the actual normative reach of a treaty.

Perhaps the most important aspect of treaty law deals with interpretation, as a treaty's text may be vague or ambiguous. Such ambiguity is often the only way the parties involved were able to achieve sufficient consensus to adopt the instrument. The Vienna Convention on the Law of Treaties provides that treaties "shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose."[34] The term "context" refers to the other text of the treaty, as well as to any agreement between the parties made at the conclusion of the treaty.[35] In addition to context, interpretation of a treaty's provision should take account of any subsequent express agreement between parties as to its meaning, as well as "subsequent practice in its application that establishes the agreement of the parties regarding its interpretation."[36] If the meaning of a provision remains ambiguous, reference may be made to the "preparatory work of the treaty

32 *Id.*, art. 2(1)(d).

33 UK Ministry of Defence, *Manual of the Law of Armed Conflict* 422-23 (2005).

34 Vienna Convention on the Law of Treaties, *supra* note 21, art. 31(1).

35 *Id.*, art. 31(2).

36 *Id.*, art. 31(3).

and the circumstances of its conclusion."[37] In other words, it is appropriate to explore what was in the mind of the parties at the time when the agreement was negotiated and adopted.

Treaty Law in the Cyber Context

Given that cyber activities are relatively new, very few treaties deal directly with them. Prominent contemporary examples include the Convention on Cybercrime,[38] its 2006 Additional Protocol,[39] the Shanghai Cooperation Organisation's International Information Security Agreement,[40] and the ITU Constitution and Convention[41] and International Telecommunication Regulations.[42] The rules regarding treaties apply fully to each of these instruments and others that exist or are to be adopted in the future. Since it is not the purpose here to examine their substantive content, it suffices to recall that when considering the formation, interpretation and application of cyber treaty norms, the key guidance is to be found in the Vienna Convention on the Law of Treaties and in the customary law of treaties.

In light of the paucity of cyber-specific treaties, the threshold question is, of course, whether non-cyber-specific instruments even apply to cyber activities. A number of states, including Russia and China, have previously expressed some reluctance to acknowledge that existing international agreements extend to cyberspace.[43] This disinclination seems to have been partially overcome in

37 *Id.*, art. 32.

38 Convention on Cybercrime, Nov. 23, 2001, 2296 UNTS 167.

39 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Jan. 28, 2003, ETS No. 189.

40 Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, 61st Plenary Meeting, Dec. 2, 2008.

41 Constitution and Convention of the International Telecommunication Union, Dec. 22, 1992, 1825 UNTS 330.

42 International Telecommunication Regulations, Dec. 9, 1988, deposited with the International Telecommunication Union Secretary-General. The International Telecommunication Regulations, as well as the Radio Regulations, are a legal instrument of the ITU (see Constitution of the International Telecommunication Union, art. 4(3)).

43 As an example, Russia has put forward arguments that instead of regulating cyber armed conflict through IHL, it should be outlawed altogether. On this point, as well as for a comprehensive overview of Russia's views on cyber-conflict, see Keir Giles & Andrew Monaghan, *Legality in Cyberspace: An adversary view* 12 (2014), http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1193.

2013 with the publication of the UN Group of Governmental Experts" (GGE) report, which found that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[44] The report also confirmed the appropriateness of the law of sovereignty and of state responsibility in the context of cyber security.[45] Both Russia and China were represented in the group. Interestingly, and unfortunately, a draft provision verbatim endorsing IHL's applicability was removed in order to secure unanimity. However, even beyond the Euro-Atlantic community, many states have publicly confirmed that IHL applies to cyber activities associated with an armed conflict.[46] There appears to be no serious opposition to the notion in academia.[47]

Considering the broad acceptance of the premise that non-cyber-specific treaty law can apply to cyberspace, an array of international agreements that govern state activities in general also constrain cyber activities. As an example, the 1982 Law of the Sea Convention delineates the type of activities that the vessels of one state may engage in while in the territorial sea of another state.[48] Although the vessels have a right of passage though the territorial sea, the passage must be "innocent", that is, not be contrary to the interests of the coastal nation. Conducting cyber operations against the coastal state from aboard naval vessels would consequently violate the innocent passage regime for states party to the Convention, even though that treaty was adopted well before the advent

44 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, U.N. Doc. A/68/98, June 24, 2013, http://undocs.org/A/68/98.

45 *Id.*, paras. 20-23.

46 See, e.g., Information Security Policy Council, Japan, International Strategy on Cybersecurity Cooperation 9 (Oct. 2, 2013), http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf; Australian Department of Defence, White Paper 21 (2013), http://www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf; Republic of Korea, Report to the United Nations Secretary General 1 (2014), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/10/ROK.pdf (welcoming the report of the 3rd UN Group of Governmental Experts, "including the agreement that existing international law is applicable in cyberspace"); Georgia, Report to the United Nations Secretary General 5 (2014), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/Georgia.pdf.

47 The International Committee of the Red Cross has endorsed the same view. ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts 37, Doc. 31IC/11/5.1.2, Oct. 31, 2011.

48 United Nations Convention on the Law of the Sea, arts. 17-19, Dec. 10, 1982, 1833 UNTS 397.

of sea-based cyber operations. Similarly, the 1963 Moon Treaty provides that the Moon and other celestial bodies are to be used for "exclusively peaceful purposes".[49] Therefore, military cyber operations may not be launched from the moon or other celestial bodies, again despite the fact that the treaty predates the technical capability to do so. In Europe, the 1950 European Convention on Human Rights (in effect since 1953) is playing a prominent role in privacy and data protection debates involving cyber communications that its drafters could not have envisaged.[50]

It is, however, in the realm of treaty law dealing with the *jus ad bellum* and IHL that non-cyber-specific treaties are presently playing the most prominent role. This is because of the relative maturity of these bodies of law as compared to certain others that are implicated by cyber operations, such as the law of state responsibility. Additionally, cyber legal issues logically first attracted the attention of lawyers involved in military affairs, as it is primarily the military that plans, develops and executes cyber operations. Since these lawyers' training and experience is in conflict law, the evolutionary development of legal scholarship in conflict law before that in other fields of international law is understandable. Therefore, as of now, the normative regimes of the *jus ad bellum* and IHL offer the most fertile ground for examining how non-cyber-specific treaty law applies in the cyber context. It is certainly with respect to them that the discourse is most mature.

Central among these treaties are the UN Charter with respect to *jus ad bellum*, and the 1949 Geneva Protocols and their 1977 Additional Protocols in IHL. Given the general applicability of these instruments to cyber conflict, the key issue is how their norms are to be *interpreted* in the cyber context. This was the focus of inquiry by the International Group of Experts that prepared the *Tallinn Manual*. Although the *Tallinn Manual* embraces the premise of complete applicability of *jus ad bellum* and IHL norms,[51] it is replete with examples of circumstances in which the experts could not achieve consensus on their precise interpretation with respect to cyber operations. Accordingly, the manual often refers to majority and minority views among them. To ensure comprehensiveness, on

49 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, art. IV, Dec. 5, 1979, 1363 UNTS 3.

50 Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 UNTS 222.

51 *Tallinn Manual, supra* note 5, at 3, 13. The role of human rights law is especially complicated because not all states take the same approach with respect to the extraterritoriality of treaty-based human rights norms. The United States, for instance, has historically taken the position that they do not apply extraterritorially.

numerous occasions the manual even acknowledges the existence of reasonable interpretations not supported by any member of the group.[52]

As became clear during the *Tallinn Manual* drafting process, the object and purpose of treaties enjoys particular significance when interpreting existing treaties in the context of new areas of activity such as cyber conflict. This is particularly so because the activities in question were in most cases beyond the contemplation of those drafting these treaties. Therefore, when applying their provisions to cyber operations, it is necessary to examine the foundational rationale underlining them, both generally and with regard to any individual provision in question.

Four prominent examples illustrate the significance of treaty interpretation, as well as its shortcomings, in the cyber context. The first deals with the meaning of the term "use of force" in the UN Charter's Article 2(4) prohibition thereof. The object and purpose of the provision was self-evidently to limit the circumstances in which states might resort to force to resolve their differences. All of the *Tallinn Manual* experts agreed that a cyber operation by one state against another that causes injury or death to individuals, or damage or destruction to property, qualifies as a use of force. However, no consensus could be reached on the exact threshold at which a cyber activity crosses into the use of force. The International Group of Experts could only offer indicative factors that states are likely to consider when deciding how to legally characterise a cyber operation in this respect.[53] Delineations of factors should prove useful as states estimate how their activities will be seen by other states, as well as when they assess the actions of other states against the norm, but they are not legal criteria *per se*. The object and purpose of Article 2(4) provided a guide to interpretation in the cyber context, but not a fully comprehensive one.

Second, Article 51 of the UN Charter provides that states may use force in response to an "armed attack". Here, the object and purpose was to ensure that states did not remain normatively defenceless should the enforcement regime established in the Charter fail to operate as planned. But the interpretation of this article remains a source of some uncertainty and controversy because it is unclear whether the right of self-defence extends to attacks conducted by non-state actors, or whether states are limited to law enforcement measures in

52 See, e.g., acknowledgement of a view by which the gap between the thresholds of a "use of force" and an "armed attack" is either so narrow as to be insignificant or non-existent, but which was not shared by any member of the International Group of Experts. *Id.*, para. 7 of commentary to r. 11.

53 *Id.*, paras. 8-10 of commentary to r. 11.

responding to such hostile acts. This is an issue that was brought to the forefront of international law debate in the aftermath of the 9/11 attacks against the United States by al Qaeda. It is a central one with respect to cyberspace, because a non-state group's or individual's capability to launch a hostile cyber operation at a state at the armed attack level is much more likely in the cyber context than the kinetic, due to the relative ease of acquiring the expertise and equipment for a cyber armed attack compared to a kinetic one.[54]

Recently, both the United States and the Netherlands have taken the position that defensive use of force in the cyber context is permissible under Article 51 even if a cyber-attack by a non-state actor cannot be attributed to another state.[55] Those states and commentators who take the more restrictive approach in applying Article 51 to terrorist strikes would likely be at least as restrictive when considering cyber operations mounted by non-state actors. This illustrates that difficulties in interpreting treaty law in the non-cyber context are highly likely to resurface in the cyber context.

It is also unclear when a cyber operation is severe enough to be regarded as an armed attack in the sense of Article 51. According to the *Tallinn Manual*, operations causing significant damage, destruction, injury or death do qualify. Inclusion of such consequences is consistent with the UN Charter's object and purpose of limiting the use of force in international relations, but consensus among the International Group of Experts stopped there; the group could not agree on any "bright line test" for determining when such harm is sufficiently

54 The ICJ appears to have suggested that the article only applies in situations in which the activities concerned reach the level of intensity required for an armed attack and are either conducted "by or on behalf" of a state or with a state's "substantial involvement". Military and Paramilitary Activities in and against Nicaragua (*Nicar. v. U.S*), 1986 I.C.J. 14, para. 195 (June 27) [hereinafter *Nicaragua*]. However, contemporary state practice, most notably that since the 9/11 terrorist attacks, appears to contradict this position. In particular, the international community unambiguously characterised the Al Qaeda attacks as triggering the United States' inherent right of self-defence. The Security Council adopted numerous resolutions recognising the applicability of the right of self-defence to attacks by non-state actors. *See, e.g.*, U.N. Doc. S/RES/1368, September 12, 2001; U.N. Doc. S/RES/1373, September 28, 2001. International organisations, including NATO, and many individual states took the same approach. *See also* Tallinn Manual, *supra* note 5, at 58.

55 Secretary General, Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/66/152, July 15, 2011, at 18; Netherlands Government Response to the AIV/CAVV Report on Cyber Warfare, http://www.aiv-advies.nl/ContentSuite/template/aiv/adv/collection_single.asp?id=1942&adv_id=3016&page=regeringsreacties&language=UK.

"grave" to cross the armed attack threshold.[56] Some experts took the position that the term should include operations that cause severe non-physical harm, such as cyber operations directed at crippling a state's economy.[57] Others resisted such a broad interpretation on the grounds that it ran counter to the Charter's presumption in favour of non-forceful resolution of international disputes. Again, a reliable interpretation of a treaty provision in the cyber context proved elusive because multiple reasonable interpretations were possible.

The third and fourth examples derive from IHL. The paradigmatic interpretive hurdle in IHL is that cited above, the meaning of the word "attack", which is found in various prohibitions set forth in Additional Protocol I. For instance, pursuant to express provisions of that treaty, it is unlawful to attack civilians, civilian objects, and certain other protected persons and objects.[58] Additionally, states are required to consider expected collateral damage at the attack level when assessing the proportionality of their operations,[59] and must take precautions to minimise such damage whenever they conduct attacks.[60] Interpretation of the term "attack" in the cyber context is essential because, to the extent to which a cyber operation fails to qualify as an attack, these and related IHL provisions do not apply.

Recall the Article 49 of Additional Protocol I definition of attack as an act of violence and the definition of cyber attack found in the *Tallinn Manual* as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." All members of the International Group of Experts agreed that Additional Protocol I's provisions referring to attacks included such cyber operations because they were violent in the sense of Article 49. However, members of the group differed on whether, and if so how far, the notion of violence should be stretched to include operations having non-kinetic effects. Some experts were of the view that the notion is strictly limited to cyber operations that cause physical damage or injury; other operations were not violent and therefore did not qualify as attacks. But a majority of them looked to the object and purpose of the Protocol and its relevant provisions to interpret the term more liberally as applying to a situation in which the functionality of an object is affected by a cyber operation

56 *Tallinn Manual*, *supra* note 5, para. 6 of commentary to Rule 13, para. 8 of commentary to Rule 11.

57 *Id.*, para. 9 of commentary to Rule 13.

58 Additional Protocol I, *supra* note 14 arts. 51-56, 59.

59 *Id.*, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b).

60 Additional Protocol I, *supra* note 14, art. 57.

without physical damage having occurred. Illustrating the difficulties that attend the application of treaty provisions to situations that were not envisaged by the drafters, there were differences of opinion within the majority as to how "functionality" should be interpreted.[61] As this example illustrates, layers of interpretation can exist.

Finally, a similar IHL-based debate is underway as to whether the term "civilian object" extends to data.[62] If so interpreted, a cyber operation designed to destroy civilian data would be prohibited by Article 52 of Additional Protocol I, which bans direct attacks against civilian objects. If not, civilian data is a lawful object of attack, except in those circumstances where its loss might cause physical damage to objects or injury to persons. The critical and unresolved fault line in the debate lies between interpretations that limit the term to entities that are tangible, which is arguably the plain meaning of the term "object", and those based on the argument that in contemporary understanding the ordinary meaning of "object" includes data.[63]

These examples illustrate that even strict application of the rules of treaty interpretation set out above fails to fully suffice in adding the requisite clarity when extant treaty provisions are applied to cyber activities. Such interpretive dilemmas are only likely to be resolved over time. Interpretive clarity will be fostered through the recurrent practice of states in application of the provisions in question, including when those states are acting in their capacity as members of international organisations like the United Nations, European Union and NATO. Also relevant will be state expressions of opinion as to proper interpretation of the terms and provisions in question. Recent examples include those proffered by former US Department of State legal adviser Harold Koh[64] and by the Dutch Government in response to the AIV report, both of which set forth state positions on the meaning of key aspects of relevant treaty law.[65] Judicial interpretation could potentially also shape the meaning of uncertain treaty norms in the cyber context, much as the judgments of the International

61 *Tallinn Manual*, *supra* note 5, paras. 4, 10-12 of commentary accompanying r. 30. On the subject, see Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack', 96 *International Review of the Red Cross* (forthcoming 2014).

62 Michael N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive Precision', 48 *Israel Law Review* (forthcoming 2015).

63 *Tallinn Manual*, *supra* note 5, paras. 5 of commentary accompanying r. 38.

64 Harold H. Koh, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012), 54 *Harvard International Law Journal Online* 1 (2012).

65 Dutch Government Response, *supra* note 55.

Criminal Tribunal for the Former Yugoslavia have added significant granularity to the understanding of IHL in its non-cyber guise. Finally, the work of scholars in the field cannot be understated, in light of the stark paucity of overt state practice and interpretive pronouncements on how treaty law applies to cyber situations. This dynamic is exemplified by the exceptional influence the *Tallinn Manual* is having on the formulation of state policies with regard to the respective treaty norms that bind them.

A persistent question is whether new treaties to address cyber activities are necessary or likely to materialise. Such treaty law would undoubtedly clear much of the normative fog that presently exists, yet new treaties are fairly unlikely for the foreseeable future. Historically, treaty law tends to emerge slowly. For example, despite a millennium of sea travel and commerce, it was not until 1958 that a robust regime governing the law of the sea was codified in treaty form.[66] Similarly, although air warfare is over a century old, no treaty governing these operations exists. In both these examples, the lack of treaty law was addressed through the crystallisation of customary law norms.

In this regard, treaties governing new technologies are often crafted only after the technologies have been used for some time and have revealed lacunae or insufficiencies in the existing law. The paradigmatic examples are the conventions governing weapons such as anti-personnel landmines and cluster munitions, which were concluded decades after the first employment of the weapons and which are still the subject of much controversy.[67]

Although there are exceptions, the classic case being the adoption of space law treaties at the dawn of the space age, it must be remembered that treaties require the express consent of states. This poses numerous hurdles. First, all states are not similarly situated with respect to particular issues and, therefore, finding common ground on which states will agree to be bound can be difficult. This is certainly the case with cyber activities, in which some states are super-empowered while others are novices.

Second, in the early days of a new technology, states will be reluctant to bind themselves to particular rules until they fully understand how those rules may play out as the technology continues to develop. In particular, there is

66 *See, e.g.*, Convention on the Territorial Sea and the Contiguous Zone, Apr. 29, 1958, 516 UNTS 205; Convention on the High Seas, Apr. 29, 1958, 13 UST 2312, 450 UNTS 82.

67 For instance, the United States is not a party to either the Ottawa Convention on anti-personnel mines or the Dublin Treaty on cluster munitions. In both cases, it took the position that the instruments run counter to operational needs.

presently little support for proactively addressing cyber weaponry and cyber military operations. As with all other methods and means of warfare, states are hesitant to restrict the use of weapons that may afford them an advantage on the battlefield until they have sufficient experience to allow them to weigh the costs and benefits of prohibitions and limitations on their use.[68]

Third, to the extent that states wield cyber capabilities that are strategically or operationally useful, they have an incentive to retain the option of employing them. But those same states may be vulnerable to hostile operations by other states using similar capabilities. Therefore, it may be difficult for a state's political and legal organs to agree on how the state should characterise a particular practice, as they may view the state's national interests from different perspectives.

A fourth factor rendering cyber treaties unlikely in the near term is the difficulty of verifying compliance with their terms and effectively enforcing them. To begin with, it is sometimes difficult to even ascertain that harm is the result of a cyber operation. Not only are the technical challenges posed by attribution perplexing, but the law of attribution is complex.[69] In other words, even when the originator of a cyber operation is known, it may be unclear whether his or her actions can be deemed to be those of a state as a matter of law such that the state is in violation of a treaty obligation.

Perhaps the prospect for evolution of cyber treaty norms was best set forth by the United Kingdom in its 2013 submission to the United Nations Secretary General:

> "Experience in concluding these agreements on other subjects shows that they can be meaningful and effective only as the culmination of diplomatic attempts to develop shared understandings and approaches, not as their starting point. The United Kingdom believes that the efforts of the international community should be focused on developing common understandings on international law and norms rather than negotiating binding instruments that would only lead to the partial and premature imposition of an approach to a domain that is currently too immature to support it."[70]

Even if states were to embark on multilateral diplomatic conferences with the

68 As an example, the 1923 Hague Rules of Air Warfare were never implemented in treaty form, in great part out of the uncertainty of states as to the role of air power in future conflicts.

69 On this topic, see, e.g., Michael N. Schmitt & Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution', 1:2 *Fletcher Security Review* 54 (2014).

70 'Developments in the field of information and telecommunications in the context of international security,' 19, UN Doc. A/68/156, July 16, 2013, http://undocs.org/A/68/156.

aim of concluding cyber treaties, any resulting treaty would likely be perforated with individual reservations, thereby degrading its practical effect. While the conclusion of uniform law treaties – those requiring states to harmonise their domestic legislation by adopting the same legal norms – is usually subject to less intense negotiation than, for instance, joint security treaties that impose cyber norms directly, in the cyber context even the former have proven difficult to agree on. As an example, despite determined international promotion, the 2001 Convention on Cybercrime has been signed by only 53 states. Nine of them have yet to ratify the agreement[71] and 22 reservations and 21 declarations have been attached by the states that are party to the Convention thus far. If this track record is illustrative, the prospects for crafting a meaningful legal regime specifically for cyber conflict are grim.

Customary International Law

The second form of international law recognised in Article 38 of the Statute of the ICJ is "general practice accepted as law", or customary international law.[72] It is a genre of norms unique to international law in the sense that it is unwritten. In many fields, such as the law of the sea, the *jus ad bellum* and IHL, customary international law was historically predominant; only in the 20th century did treaty law on these subjects come into its own.[73]

Despite the proliferation of treaties in the last century, customary law retains its significance. In great part, this is because most treaty regimes are not universal. As an example, neither the United States nor Israel are party to the 1977 Additional Protocols, although both states have been involved in numerous conflicts since their adoption. To the extent that non-party states comply with the norms expressed in a treaty, they do so only on the basis that they reflect customary international law. Also note that rules expressed in a treaty sometimes crystallise into customary law, even though they did not mirror a customary norm at the time of adoption. The classic case is that of the Regulations annexed to the 1907

71 For a list of signatories and ratifications, see *Council of Europe* website, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

72 Statute of the International Court of Justice, art. 38(1)(b), June 26, 1945, 59 Stat. 1055, 33 UNTS 993.

73 For instance, significant codification in the field occurred during the Hague Conferences of 1899 and 1907. For a list of treaties, see *International Committee of the Red Cross* website, http://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByDate.xsp.

Hague Convention IV.[74] When a particular point encompassed in the material scope of an agreement is not directly addressed, any existing customary law will govern the matter.[75]

Although unwritten, customary law is as binding on states as treaty law. Such law "crystallises" upon the confluence of two factors: the objective element of state practice (*usus)*, and the subjective element of *opinio juris sive necessitatis.*[76] As noted by the ICJ in the *Asylum* case:

> "The party which relies on custom…must prove that this custom is established in such a manner that it has become binding on the other party…that the rule invoked…is in accordance with a constant and uniform usage, practiced by the States in question, and that this usage is the expression of a right appertaining to the State…and a duty incumbent on [the other State]."[77]

Objectively, this is a high threshold. Subjectively, as this is unwritten law developed through an informal process, it is very difficult to definitively establish when crystallisation has occurred and to delineate its precise contours. For reasons that will be explained, this is particularly so with regard to nascent activities such as cyber operations.

The first prong of the test, state practice, includes both physical and verbal acts of states.[78] To qualify as state practice, the conduct in question must generally occur over an extended period of time. The classic illustration is the 1900 US Supreme Court case, *The Paquete Habana,* in which the court looked into the practice of numerous countries over a period measured in centuries to conclude that fishing vessels were exempt from capture by belligerents during an armed conflict.[79]

74 Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, October 18, 1907, 36 Stat. 2227. This was the finding of the Nuremburg Tribunal. International Military Tribunal at Nuremburg, Case of the Major War Criminals, Judgment, October 1, 1946, I Official Documents 253-54.

75 See generally Yoram Dinstein, 'The Interaction between Customary International Law and Treaties', 322 *Recueil des Cours* 383 (Martinus Nijhoff, 2007).

76 *North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.)*, 1969 ICJ. 3, paras. 71, 77 (Feb. 20); *Continental Shelf case (Libya v. Malta)*, 1985 I.C.J. 13, para. 27 (June 3); *Nicaragua*, *supra* note 54, para. 183.

77 *Asylum Case (Colom. v. Peru)*, 1950 I.C.J. 266, 276-77 (November 20).

78 *See, e.g.*, International Law Association, 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, 13 ff. (2000) [hereinafter ILA Report]; I *Customary International Humanitarian Law*, xxxviii-xxxix (Jean-Marie Henckaerts and Louise Doswald-Beck, eds., 2005).

79 *The Paquete Habana*, 175 U.S. 686-700 (1900).

This temporal condition has deteriorated over time. As an example, in the *North Sea Continental Shelf* case, the ICJ, in dealing with the customary law of the sea, held that "passage of only a short time is not necessarily a bar…[if state practice], including that of states whose interests are specially affected [is] both extensive and virtually uniform."[80] Perhaps the best illustration of the weakening of the requirement of long-term practice is the development of customary space law,[81] an example that suggests that the relative novelty of cyber operations does not necessarily preclude the rapid emergence of cyber-specific customary international law.

The state practice essential to establishing customary law must, even if of limited duration, be consistent. When there are significant deviations from a practice by states, which may include both engaging in an activity and refraining from one, a customary norm cannot materialise. Although minor infrequent inconsistencies do not constitute a bar to such emergence,[82] repeated inconsistencies generally have to be characterised by other states as violations of the norm in question before a customary norm can be said to exist. [83] For instance, it is clear that the prohibition on the use of force set out in Article 2(4) of the UN Charter constitutes a customary norm;[84] yet states have historically engaged in the use of force and continue to do so today. The saving factor is that when they do, their conduct is, absent the justification of self-defence, typically styled by other states as wrongful.

There is no set formula as to the number of states that must engage in a practice before a norm crystallises, although the greater the density of practice, the more convincing the argument that crystallisation has occurred.[85] Of particular importance is the diversity of the states involved on issues such as their geopolitics and legal systems,[86] and the fact that "specially affected states" have engaged in the practice or expressed their view of such practice when engaged

80 *North Sea Continental Shelf*, *supra* note 76, para. 74.

81 For an early, and classic, treatment of the subject, see Myres S. McDougal, 'The Emerging Customary Law of Space', 58 *Northwestern University Law Review* 618 (1963-1964): 618-42.

82 *Fisheries Case (U.K. v. Norway)*, 1951 I.C.J. 116, 131 (December 18).

83 "In order to deduce the existence of customary rules, the Court deems it sufficient that the conduct of states should, in general, be consistent with such rules, and that instances of state conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule." *Nicaragua*, *supra* note 54, para. 186.

84 *Id*, paras. 188-190.

85 *Customary International Humanitarian Law*, *supra* note 78, at xlii-xliv.

86 *Id*., xliv.

in by other states.[87] A specially affected state is one upon which the norm will operate with particular resonance. As an example, the International Committee of the Red Cross (ICRC) has opined that "specially affected states" with respect to the legality of weapons include "those identified as having been in the process of developing such weapons."[88] In cyberspace, the United States would qualify as a "specially affected state" in light of its centrality to cyber activities and its development of military capacity in the field.

The term "*opinio juris*" refers to the requirement that a state engage in a practice, or refrain from it, out of a sense of legal obligation.[89] In other words, the state must believe that its actions are required or prohibited by international law. It is often the case that a state's behaviour is motivated by other factors, such as policy, security, operational, economic and even moral considerations. For instance, Estonia actively seeks to maintain a clean cyber environment. It does so, not because it believes that the international legal requirement of "due diligence" requires such measures, but rather for cyber security reasons such as to prevent the establishment and use of botnets in the country. Such practices have no bearing on the creation of a customary law norm.

The fact that various norms converge to govern state conduct makes it necessary to deconstruct state practice to determine whether a state is acting out of a sense of legal obligation or is instead motivated by ethical or policy concerns. Obviously, it is often difficult to ascertain the rationale underlying a particular practice; care must be taken in drawing inferences as to *opinio juris* based solely on the existence of state practice.[90] For instance, the ICRC cited many military manuals as evidence of *opinio juris* in its 2005 Customary International Humanitarian Law study.[91] In response, the United States objected that the provisions found in military manuals were often as much the product of operational and policy choice as legal obligation.[92] A similar criticism frequently attends the citation of

87 *North Sea Continental Shelf*, *supra* note 76, para. 74; ILA Report, *supra* note 78, 25-26.

88 *Customary International Humanitarian Law*, *supra* note 78, at xliv.

89 *S.S. Lotus*, *supra* note 12, at 28; *North Sea Continental Shelf*, *supra* note 76, para. 77; *Nicaragua*, *supra* note 54, para. 185 (citing).

90 *North Sea Continental Shelf*, *supra* note 76, paras. 76-77.

91 *Customary International Humanitarian Law*, *supra* note 78, at xxxviii. See also *Prosecutor v. Tadić*, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, para. 99 (Int'l Crim. Trib. for the former Yugoslavia October 2, 1995).

92 Letter to Jakob Kellinberger, ICRC, from John B. Bellinger, III & William J. Haynes II, U.S. Department of State and U.S. Department of Defense, respectively, U.S. Initial Reactions to ICRC Study on Customary International Law, November 3, 2006, http://2001-2009.state.gov/s/l/rls/82630.htm.

UN General Assembly resolutions as support for the existence of a customary norm, because states can vote in favour of such legally non-binding instruments for purely political reasons. The point is that when the basis for a practice or assertion is unclear, it does not comprise the requisite *opinio juris*.

Despite this difficulty, states do engage in conduct and issue statements that clearly indicate their characterisation of certain practices as required (or not) by customary international law. As an example, although the United States is a party to neither the Law of the Sea Convention nor Additional Protocol I, it often confirms that it views certain provisions of those instruments as reflective of customary international law.[93]

Once a customary norm has emerged, it is applicable to all states, including those that did not participate in the practice that led to its crystallisation. Such norms are even binding on states that are created after the customary norm has developed.[94] However, there are a number of exceptions to this general principle. In particular, a state may "persistently object" to the norm's formation as it is emerging. If the norm nevertheless emerges, the persistent objector is arguably not bound by it.[95] In this regard, the role of "specially affected states" is paramount.[96] It would be very unlikely that a customary norm could emerge over the objection of such a state. For example, given the military wherewithal of the United States, and its frequent involvement in armed conflicts, it would be difficult for an IHL cyber norm to materialise in the face of a US objection thereto. Fortunately, assertions of persistent objection are infrequent; rather, disagreement regarding customary norms typically surrounds the scope of a rule, not its existence.

In certain limited circumstances, a customary norm may be regional or even local in character. To illustrate, in the *Asylum* case, the ICJ found that a regional customary norm applied in Latin America,[97] whereas in the *Rights of Passage* it determined that another existed between two states with respect to passage

93 Department of the Navy and Department of Homeland Security, The Commander's Handbook on the Law of Naval Operations, para. 1-2, NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, 2007; The United States Army Judge Advocate General's Legal Center and School, Law of Armed Conflict Documentary Supplement 232-33 (2013), http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Documentary-Supplement-2013.pdf.

94 ILA Report, *supra* note 78, at 24-25.

95 *Id.* at 27-29. The doctrine of persistent objection is not universally accepted. *Customary International Humanitarian Law*, *supra* note 78, at xlv.

96 *North Sea Continental Shelf*, *supra* note 76, para. 74.

97 *Asylum Case*, *supra* note 77, at 276-77.

across India to Portuguese enclaves in that state.[98] It is foreseeable that regional norms might develop for cyber activities, particularly where states of a region are similarly situated in that regard, as in the case of Europe.

Customary International Law in the Cyber Context

Many obstacles lie in the path of customary norm emergence *vis-à-vis* cyberspace. The requirement of practice over time hinders this process to an extent, but is not fatal because contemporary customary international law appears to countenance relatively rapid crystallisation. A much greater impediment is the visibility of cyber activities. It is difficult to "see" what goes on in cyberspace. Instead, the effects of cyber operations are often all that is publicly observed; in fact, sometimes even the effects are not apparent to the general public. Therefore, it can be difficult to point to a particular state's cyber practice to support an argument that a norm has emerged. States, including victim states, may be reticent in revealing their knowledge of a cyber operation, because doing so may disclose capabilities that they deem essential to their security. Undisclosed acts cannot, as a practical matter, amount to state practice contributing to the emergence of customary international law.[99]

Similarly, states will frequently hesitate to offer opinions regarding the legality of state practice in cyberspace. For instance, a state may be unwilling to definitively articulate a threshold for "armed attack".[100] This could be because it does not want its opponents to discern when it is likely to respond on the basis of the right of self-defence, or because it prefers not to clarify the "use of force" threshold as doing so might limit its own options in the future. In other words, it may view strategic ambiguity as in its national interest. From an international security perspective, normative clarity is not always helpful.

Two recent examples are illustrative. The relative silence of states in reaction to the 2010 Stuxnet operation against Iranian nuclear enrichment centrifuges does not necessarily indicate that states believe that the operation was lawful (assuming for the sake of analysis that it was launched by other states, since only

98 *Case Concerning Right of Passage Over Indian Territory (Port. v. India)*, 1960 I.C.J. 6, p. 37 (April 12).

99 *Customary International Humanitarian Law*, *supra* note 78, at xl; ILA Report, *supra* note 78, 15.

100 As an example, at the 2014 NATO Summit in Wales, the Alliance's Heads of State and Government decided that "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis." – Wales Summit Declaration, Sept. 5, 2014, pt. 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

states can violate the prohibition on the use of force set forth in Article 2(4) of the UN Charter). On the contrary, they may have concluded that the attack violated the prohibition on the use of force because it was not in response to an Iranian armed attack pursuant to the treaty and customary law of self-defence. Yet those states may logically have decided that the operation was nevertheless a sensible means of avoiding a pre-emptive and destabilising kinetic attack against the facilities by Israel. Similarly, the 2012 Shamoon virus targeting Saudi Arabia's national oil company's computers may also have been considered a violation of the prohibition of the use of force, if it was conducted, as has been speculated, by Iran.[101] Despite this possibility, the relative downplaying by states of the legal aspects in particular, as well as the entire incident in general, may be attributable to concerns regarding the economic consequences of publicly discussing the grave consequences or the perpetrator of the operation.

It is also common for states to support or condemn a cyber activity in their international rhetoric, but not be specific as to whether the condemnation is based on customary international law or on other considerations, such as moral principles or political concerns. The PRISM surveillance programme serves as an example on point. While many states, including Germany and France, criticised the surveillance programme, with the former stating that these practices were "completely unacceptable"[102] and the latter that they "cannot accept this kind of behaviour from partners and allies,"[103] the comments do not necessarily confirm their position on the legality of the programme.

Other requirements that will often be difficult to meet in regard to cyber state practice are consistency and density. For instance, Brazil argued at the UN General Assembly in 2013 that the interception of communications represents "a case of disrespect to the [country's] national sovereignty,"[104] presumably suggesting that it breaches the international law principle of sovereignty. It is unlikely that a sufficient number of other states, in particular specially affected states, will embrace the same position to the extent that the criteria of a

101 Nicole Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back', *New York Times,* Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

102 'Merkel Calls Obama about 'US Spying on Her Phone", BBC, Oct. 23, 2013, http://www.bbc.com/news/world-us-canada-24647268.

103 'Hollande: Bugging Allegations Threaten EU-US Trade Pact', BBC, July 1, 2013, http://www.bbc.com/news/world-us-canada-23125451.

104 Statement by Brazilian President H. E. Dilma Rousseff on September 24, 2013 at the Opening of the General Debate of the 68th session of the United Nations General Assembly. Translated reprint at 2, http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

customary norm will be satisfied.

Indeed, as noted above with regard to treaties, states may be conflicted regarding what legal position to take on cyber customary norms. As a result, they may take no position on the legality of a particular cyber practice until they fully understand the position's costs and benefits. And, of course, states will want to avoid being criticised for adopting a "do as I say, not as I do" approach. The United States, rightly or wrongly, has been the subject of such accusations with regard to its condemnation of Chinese cyber operations against United States businesses.[105]

Finally, state comments regarding their own or other states' activities tend to be drafted by non-lawyers. The legal dimension of the activities is accordingly often neglected. The paradigmatic examples were the US public statements regarding possible operations against Iraq in late 2002 and early 2003, which focused on Iraq's alleged involvement in transnational terrorism and its development of weapons of mass destruction capability.[106] By the time the US finally set out its formal legal justification – a very nuanced interpretation of ceasefire law[107] – it had been rendered inaudible against the on-going geopolitical brouhaha that was underway. As this example demonstrates, international security matters generally take on policy and strategic hues, rather than legal ones. The same is proving to be true as states engage in and react to cyber activities.

Considered in concert, these factors render improbable the rapid crystallisation of new customary norms to govern cyberspace. Therefore, the normative impact of customary law on cyber conflict is most likely to take place in the guise of interpretation of existing customary norms, and if so, interpretive dilemmas similar to those affecting treaty interpretation will surface. In fact, the obstacles will be greater with respect to customary international law, because not only are the rules themselves not expressly articulated, but there are also no explicit rules regarding their interpretation such as those found in the Vienna Convention on the Law of Treaties.

105 *See, e.g.*, 'China Denounces US Cyber-theft Charges', BBC, May 20, 2014, http://www.bbc.com/news/world-us-canada-27477601.

106 Address of President George W. Bush, March 19, 2003, http://georgewbush-whitehouse.archives.gov/news/releases/2003/03/20030319-17.html.

107 Letter dated 20 March 2003 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2003/351, March 21, 2003.

General Principles of Law in the Cyber Context

The third formal source of international legal norms cited in Article 38 of the International Court of Justice's Statute is general principles of law. A complicating factor with respect to this source is that its nature is the subject of some controversy.[108] Generally, the term is said to refer to a number of types of legal principles that are: common across domestic legal systems, such as the use of circumstantial evidence;[109] evident from the nature of law itself, for instance *res judicata* (final judgments of a court are conclusive);[110] derive from the nature of international law, such as *pacta sunt sevanda* ("agreements must be kept");[111] and based on fairness, prominent examples being equity[112] and estoppel.[113]

General principles are most likely to become relevant when disputes between states over cyber matters arise. As an example, in the celebrated *Chorzow Factory* case, the Permanent Court of International Justice held that the breach of an obligation in international law necessarily gives rise to the obligation to make reparations,[114] a principle echoed in the International Law Commission's Articles of State Responsibility.[115] Thus, if a state's cyber operations violate the sovereignty of another state and cause harm, the former will be obligated to make reparations to the latter. Similarly, courts may decide cases in part based on equitable considerations. Such a decision might be appropriate, for instance, in the case of cyber infrastructure which is shared by states.

However, at times a general principle of law may reflect a substantive obligation. The classic example is the International Court of Justice's identification of the principle that every State shoulders an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[116] This

108 Malcolm N. Shaw, *International Law* 98 (6th ed. 2008); Oscar Schachter, *International Law in Theory and Practice* 50–55 (1991).

109 *Corfu Channel* (*U.K. v. Alb.*), 1949 ICJ. 4, at 18 (Apr. 9).

110 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. and Montenegro)*, 2007 ICJ. 43, para. 113 (Feb. 26).

111 Vienna Convention on the Law of Treaties, *supra* note 21, art. 26; AMCO v. Republic of Indonesia, 89 Int'l L. Rep. 366, 495-97 (1992).

112 *North Sea Continental Shelf*, *supra* note 76, paras. 98-99; *Barcelona Traction, Light & Power Co. Ltd. (Belg. v. Spain)*, 1970 ICJ. 3, para. 94 (Feb. 5); *Frontier Dispute (Burkino Faso v. Mali)*, 1986 ICJ 554, para. 149 (Dec. 22).

113 *Temple case*, 1962 ICJ 6, 23, 31; *Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria)*, 2002 ICJ. 275, para. 57 (Oct. 10).

114 *Chorzow Factory Case*, 1928 PCIJ., (ser. A) No. 13, at 28.

115 Articles on State Responsibility, *supra* note 10, part 2, ch. II.

116 *Corfu Channel*, *supra* note 109, at 22.

pronouncement, which is now universally accepted, was the basis for *Tallinn Manual* Rule 5: "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."[117]

Conclusion

Legal norms are but one facet of the normative environment in which cyber operations exist. To suggest that they alone suffice would be folly. After all, there is a scarcity of cyber-specific treaty law and a near total void of cyber-specific customary law on the subject. As a result, recourse must be had to general international law and the interpretation thereof in the cyber context. Of course, any interpretive endeavour is plagued with uncertainty and ambiguity, especially when engaged in with respect to novel activities such as cyber operations. This lack of legal normative clarity invites states to take differing interpretive positions. A state's objective view of the law may drive the legal position it adopts; however, it would be naïve to deny that policy and ethical influences have an effect on such determinations.

Controversy and inexactitude will surely characterise this process, which will be neither linear nor logical. The weakening of the early Russian and Chinese objections to the application of extant international law to cyberspace is a milestone in this regard. Yet, while both states have backed away from their opening stance on the issue, it remains unclear where they stand today. Other states such as the United States and the Netherlands are beginning to show a willingness to articulate their positions on how current international law applies in cyberspace. Nonetheless, the public pronouncements to date have been vague, probably intentionally so.

Despite the attention that cyber activities have drawn in the past decade, the conclusion of new treaties or the crystallisation of new customary law norms to govern them is doubtful. Opposition from western states is particularly marked to the former, at least.[118] Instead, the application and interpretative evolution of

117 *Tallinn Manual, supra* note 5, r. 5.

118 See, e.g., President of the United States, International Strategy for Cyberspace, May 15, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 15, Doc. JOIN (2013) 1 final, February 7, 2013.

existing international law is the most likely near-term prospect. As to customary law, although it may sometimes develop rapidly, "usually customary law is too slow a means of adapting the law to fast-changing circumstances."[119]

Consequently, the work of scholars such as the International Group of Experts who prepared the *Tallinn Manual*, and those who are engaged in the follow-on "Tallinn 2.0" project, is likely to prove especially influential. This dynamic is appropriate since, as noted in Article 38 of the International Court of Justice's Statute, the work of scholars is a secondary source of law that informs identification and application of primary sources. But this reality is certainly less than optimal, because states, and only states, enjoy the formal authority to make international law. Unless they wish to surrender their interpretive prerogative to academia, it is incumbent upon them to engage with cyber issues more openly and more aggressively.

In this patchwork and nebulous environment, the role of other normative regimes looms large. Only in exceptional circumstances may their dictates cross the international law border. However, where those boundaries are indistinct, common policy or ethical norms may operate to define the outer boundaries of acceptable conduct in cyber space. Because cyber activities are a relatively new phenomenon, policy and ethical norms may serve to carve out more restrictive boundaries than international laws which are designed to constrain the other activities of states. Over time, these non-legal norms may mature through codification into treaty law or crystallise into customary law, such that they formally define the limits of cyber activities. In the meantime, cyberspace will remain an environment of fervent, and often multi-directional, normative development.

119 *Oppenheim's International Law*, *supra* note 9, at 30.