DOI 10.5817/MUJLT2019-1-4

THE TALLINN MANUALS AND THE MAKING OF THE INTERNATIONAL LAW ON CYBER OPERATIONS[*]

by

PAPAWADEE TANODOMDEJ[**]

The Tallinn Manuals (the Manuals) attempted to clarify how to apply existing international law to cyber operations. Though the Manuals are non-binding instruments, the Group of International Experts claimed that they reflected the lex lata applicable to cyber operations. However, this claim is questionable due to the dominating role of a few Western states in the drafting process and the linked neglect of the practice of "affected states" in cyber operations. This article examines the quality of the Manuals' drafting process and the composition and impartiality of the experts involved. It focuses on the issue of the prohibition of the use of force. The aim of this examination is not to discuss whether the Manuals provided the right answer to the question of how international law applies to cyber operations. Rather, they function as a case study of how legal scholarship may affect the making of international law. The article concludes that certain rules in the Manuals are marked by NATO influence and overlook the practice of other states engaged in cyber operations. Therefore, the Manuals disregard the generality of state practice, which should be the decisive factor in the formation of customary international law. As far as "political activism" may be involved, the article argues that the role of legal scholars as assistants to the cognition of international law could be compromised.

[*] The author would like to thank the reviewers and the members of *Masaryk University Journal of Law and Technology* for their helpful comments and help preparing this article for publication. In addition, the author would like to thank to *Professor Kinji Akashi* for always inspiring and constant support and *Dr. Lasse Schuldt* for incessant encouragement.

[**] papawadee.tanodomdej@gmail.com, LL.D. student, Kyushu University, Japan; lecturer at Chulalongkorn University, Law Faculty, Bangkok, Thailand.

KEY WORDS
Cyber Attack, Cyber Operation, International Law-making, Legal Scholarship, Tallinn Manual

1. INTRODUCTION

> *"In the 21st Century, bits and bytes can be as threatening as bullets and bombs."*[1]

The statement made by a former US Deputy Secretary of Defense holds true, since the Internet has extended its role from a means of communication to an enabling technology facilitating almost every aspect of human activities. Not only actors in the private sector rely on information technology, but also government agencies and entities managing critical infrastructures utilize cyber technology to discharge their functions. The fact that states increasingly attach their core functions to the interconnectivity of cyberspace exposes them to this new paradigm of threats. For instance, the DDoS attack on Estonia in 2007 disabled the websites of all ministries, two major banks, several political parties and the parliamentary email server, the credit cards and automatic teller machines (ATMs) leading to the whole nation being halted.[2]

The international community is aware of the rise of cyber threats and attempts to extend the existing international law to regulate cyber operations. *The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security (UN GGE)* concluded in its 3rd report in 2013 that international law, in particular the Charter of the United Nations (UN Charter), applies to cyberspace.[3] However, there is no consensus neither from the UN GGE nor the whole international community clarifying how exactly international law is applicable to cyber operations. Against this backdrop, the "Tallinn Manual on the International Law Applicable to Cyber Warfare" and the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" ("Tallinn

[1] Lynn, W. J. (2011) *Remarks on the Department of Defense Cyber Strategy as Delivered by Deputy Secretary of Defense William J. Lynn.* [speech] 14 July. Available from: http://www.defense.gov/speeches/speech.aspx?speechid=1593 [Accessed 12 July 2018].

[2] Tikk, E. Kaska, K. and Vihul, L. (2010) *International Cyber Incidents: Legal Considerations.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 18–24.

[3] (2013) *UN Doc A/68/98.* pp. 6, 8.

Manuals") emerged by the articulation of a group of legal scholars and international lawyers. The Tallinn Manuals are the products of the deliberation of the International Group of Experts invited by the *NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)* on how international law applies to cyber operations, but they are non--binding instruments. The Tallinn Manuals cover both cyber operations in armed conflict and peacetime, while at the same time address the law of state responsibility, sovereignty, human rights, air and aviation law, space law and the law of the sea. The publication of the Manuals has not only attracted the states' attention but has also lead to an academic discussion on cyber operations because of the group's rather bold statement that the rules in the Manuals, made through the consensus of the International Group of Experts, reflects the *lex lata* applicable to cyber operations and avoids articulating *lex ferenda*.[4] If this claim were true, the Manuals would articulate the international law applicable to cyber operations with unprecedented clarity. Accordingly, this article aims to scrutinize the legitimacy of the Tallinn Manuals as products of legal scholarship contributing to the international law-making on cyber operations. In doing so, this article consists of two parts. Firstly, attention is paid to the role of legal scholarship in law-making. Secondly, the legitimacy of experts involved in the drafting of the Tallinn Manuals will be examined. Furthermore, the article assesses the quality of the Manuals' drafting process with regard to the prohibition of the use of force, one of the fundamental principles of the UN Charter since it was the starting point of the debate on the suitability of international law as a normative framework for the regulation of cyber operations. The ultimate goal is not to assess the quality of the Tallinn Manuals, but to demonstrate how legal scholarship can affect the making of international law.

2. ROLE OF LEGAL SCHOLARSHIP IN LAW-MAKING

The orthodox doctrine views international law-making in terms of sources.[5] Article 38 of the Statute of the International Court of Justice (ICJ) is the main reference to both the sources of international law and its making. However,

---

[4] *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* p. 19; see also *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* p. 3.

[5] Skouteris, T. (2001) The Force of a Doctrine: Art. 38 of the PCIJ Statute and the Sources of International Law. In: Fleur Johns et al. (eds.). *Events: The Force of International Law.* New York: Routledge, pp. 69–80.

due to the plethora of actors using and speaking of international law, it is undeniable that communicative practices assimilate themselves to the process of international law-making.[6] In particular, legal scholars and international lawyers play a significant role by interpreting the existing international law to solve the novel global challenges. The main question is to what extent legal scholarship contributes to international law-making.

In order to give a precise response, it is imperative to discuss the relationship between the sources doctrine and Article 38 (1) (d) of the ICJ Statute before addressing the variety of contemporary international-law making theories recognizing communicative practices.

2.1 LEGAL SCHOLARSHIP AND ARTICLE 38 (1) (D)

Article 38 (1) (d) of the ICJ Statute stipulates that judicial decisions and the teachings of the most highly qualified publicists are the subsidiary means for the determination of rules of law. This could be read that legal scholarship is the

> *"subsidiary means for the determination of law, not a subsidiary source of law".*[7]

Legal scholarship may thus present evidence of international law through its analysis of collected state practice reflecting certain international legal norms. However, 19th century legal scholars have often referred also to the works of famous men such as *Grotius*, *Pufendorf*, *Westlake* and *Vattel* to validate their arguments.[8] It remains doubtful to what extent legal scholarship can objectively substantiate international practice as evidence of international law. In the joint separate opinion of Judges *Higgins*, *Kooijmans* and *Buergenthal* in the *Congo v. Belgium* case, the Judges discussed the question whether a state is entitled to exercise jurisdiction over persons having no connection with the forum state when the accused is not present in that state. Despite the contribution of legal scholarship on the question, the Joint Separate Opinion rejected scholarly writings asserting that

---

[6] Venzke, I. (2013) Contemporary Theories and International Law-making. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking.* Cheltenham: Edward Elgar, pp. 66–73.

[7] Kammerhofer, J. (2013) Lawmaking by Scholars. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking.* Cheltenham: Edward Elgar, p. 306.

[8] Parry, C. (1965) *The Sources and Evidence of International Law.* Manchester: Manchester University Press, p. 103.

the treaties on crimes and offences are evidence of universality as a ground for the exercise of jurisdiction recognized in international law.[9] The Opinion noted that

> *"[t]he assertion [from the writings of eminent jurists] that certain treaties and court decisions rely on universal jurisdiction, which in fact they do not, does not evidence an international practice recognised as custom. And the policy arguments advanced in some of the writings can certainly suggest why a practice or a court decision should be regarded as desirable, or indeed lawful; but contrary arguments are advanced too, and in any event, these also cannot serve to substantiate an international practice where virtually none exists."*[10]

Although certain scholar writings have been rejected by the ICJ, this does not mean that the role of legal scholars as assistants to the cognition of international is ignored. In the Advisory opinion on *the Construction of a Wall*, the ICJ made reference to and agreed with the views of the editor of *Oppenheim's* international law.[11]

Accordingly, the ICJ holds full discretion to grasp the legal scholarship which it holds to reflect the applicable international law. Moreover, Article 38 (2) of the Statute of the ICJ allows the ICJ to decide the dispute, if the parties agree, on the ground of any norms not contained in Article 38 (1). It appears therefore that the ICJ is endowed with the power to appreciate any evidence that manifests rules of international law, not limited to legal scholarship or judicial decisions. Against this backdrop, legal scholarship does not have any particular intrinsic epistemic power and could, at best, be deemed as "evidence of the law".[12]

2.2 COMMUNICATIVE PRACTICE

While the normative-positivist considers legal scholarship as mere evidence of the law, many contemporary theories on international law-making take

---

[9] *Case Concerning the Arrest Warrant of 11 April 2000* (*Democratic Republic of Congo v. Belgium*). The Joint Separate Opinion of Judge Higgins, Kooijmans and Buergenthal, Judgement of 14 February 2002. ICJ Reports 2002. para. 26.

[10] Op. cit., para. 44.

[11] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.* Advisory Opinion of 9 July 2004, para. 57.

[12] Kammerhofer, J. (2013) op. cit., p. 308; see also Triggs, G. (2005) The Public International Lawyer and the Practice of International Law. *Australian Yearbook of International Law,* 24, pp. 202–205.

into account the potential of the use of international law language contributing to its making.[13] This can be seen, for example, in the debates over the meaning of "force" pursuant to, but undefined by, Article 2 (4) of the UN Charter. Also, the authoritative meanings of "combatant" and "civilian" are derived from the practice of interpreting these terms. International law, in the eyes of contemporary theories, is not only made through the conclusion of treaties but also by way of a communicative process of speaking and using international law by the various actors, which are not only states. Therefore, contemporary theories take into account the multiplicity of actors contributing to international law-making by participating in the interpretative process.

First, the *New Haven School*, including *Michael Reisman*, argues that international law emerges from a communicative process among a multiplicity of actors.[14] In particular, aspects of humanitarian concern have been discussed by a wide range of actors in the international political discourse. Even though humanitarianism is construed as social fact, it can be weighed as a point of reference for legal arguments or normative judgments.

The System Theory supports the communicative process as law-making but distinguishes itself from the *New Haven School* in that it holds that interpretation in international law cannot be diminished to the pursuit of values. *Niklas Luhmann* elaborates *Gunther Teubner's* proposition of "Autopoiesis" to describe the self-reproduction of international law whose communication is presented as referring to its own same system.[15] The validation of the legal claims relies upon legal claims.[16] Against this background, *Teubner* argues that

> *"global law will grow mainly from the social peripheries, not from the political centres of nation-states and international institutions"*

and the non-state actors are increasingly important in societal law-making.[17]

---

[13] Venzke, I. (2013), op. cit., p. 66.

[14] Reisman, M. (1981) International Lawmaking: A Process of Communication. *American Society of International Law Proceedings,* 75, pp. 101–120.

[15] Luhmann, N. (1993) *Das Recht der Gesellschaft.* Frankfurt: Suhrkamp, p. 98.

[16] Ibid.

[17] Teubner, G. (1997) Global Bukowina: Legal Pluralism in the World Society. In: *Global Law Without a State.* Hants: Dartmount, pp. 3–28.

The Governance Theory also acknowledges the rise of non-state actors in law-making.[18] However, according to *Slaughter*, the engagements among domestic regulators, the private sector, technicians and academia resulting in the informal international law-making raises the question of accountability. Since

> *"the essence of a network is a process rather than an entity, it cannot be captured or controlled in the ways that typically structure formal legitimacy in a democratic polity."*[19]

The Global Administrative Law (GAL) theory criticizes that, although the sources doctrine ties international law to the consent of states claiming the legitimate order, it does not capture "everything that matters".[20] The GAL theory has been established to respond to the accountability deficiency in the international law-making process by introducing general principles of administrative law such as transparency, procedural participation and review. Under the view of GAL, making international law through interpretation is deemed as an exercise of public authority, provided that the interpreters

> *"have the capacity to establish their own statements about the law as reference points for legal discourse"*

that others could only escape at a cost.[21]

All in all, contemporary theories consider communicative practices, such as interpretation, as part of international law-making. However, legal arguments claiming to establish legal rules may disguise underlying political agendas. This subjectivity could indeed undermine the legitimacy of the communicative law-making process.

---

[18] Pauwelyn, J. (2012) Informal International Lawmaking: Framing the Concept and Research Questions. In: Joost Pauwelyn, Ramses Wessel and Jan Wouters (eds.). *Informal International Lawmaking.* Oxford: Oxford University Press, pp. 15–20.

[19] Slaughter, A.-M. (2000) Agencies on the Loose? Holding Government Networks Accountable. In: George Bermann and Peter Lindseth (eds.). *Transatlantic Regulatory Cooperation, Legal Problems and Political Prospects.* Oxford: Oxford University Press, p. 531.

[20] Kingsbury, B. Krisch, N. and Stewart, R. (2005) The Emergence of Global Administrative Law. *Law and Contemporary Problems,* 68, p. 17.

[21] Venzke, I. (2013), op. cit., p. 85.

3. THE TALLINN MANUALS AND THE COGNITION OF INTERNATIONAL LAW ON CYBER OPERATIONS

In principle, the Tallinn Manuals written under the International Group of Experts' mandate amount to mere legal scholarship serving as a subsidiary means for identifying the sources of international law on cyber operations. The role of these experts can be approximated to the role of the International Law Commission (ILC) and other independent entities where legal experts are assigned to study and clarify international law.

Michael Schmitt, the Director of the International Group of Experts, states in the introduction of the Manuals that

> *"This Manual is meant to be a reflection of law as it existed at the point of the Manual's adoption by the two International Groups of Experts in June 2016. It is not a "best practice" guide, does not represent "progressive development of the law", and is policy and politics-neutral. In other words, Tallinn Manual 2.0 is intended as an objective restatement of the lex lata. Therefore, the Experts involved in both projects assiduously avoided including statement reflecting lex ferenda."*[22]

This statement confirms the self-perception of the International Group of Experts that its task was to not to make law but to articulate the law as it exists. The position of the Group is approximate to the sources doctrine by denying its capacity to make law but accentuating its role as an assistant to the cognition of law. To test the validity of this statement, both the legitimacy of the Group and the use of force rule under the Tallinn Manuals will be discussed.

3.1 LEGITIMACY OF THE INTERNATIONAL GROUP OF EXPERTS

The Group's legitimacy can be discussed from the perspectives of the sources doctrine as well as contemporary theories with a view to the predictability and consistency of international legal rules. The question of objectivity of legal scholars' discourse is intertwined with the legitimacy of the legal scholars themselves.[23] Therefore, both

[22] *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* pp. 2–3.

[23] Schachter, O. (1977) The Invisible College of International Lawyers. *Northwestern University Law Review*, 72, pp. 219–221.

the composition and the authority of the International Group of Experts will be examined.

The International Group of Experts drafting the first version of the Tallinn Manual was composed of 19 experts ranging from international law academics, practitioners, serving or former military officials and technical experts, as well as four observers from the *International Committee of the Red Cross (ICRC)*, NATO and the US Cyber Command who also actively participated in the deliberation.[24] Experts and observers of the Tallinn Manual project came from a few Western countries. Seven experts (including the Director) came from the US. There were no participants from Russia, China, Iran and Israel, all countries which are reportedly involved in cyber operations.[25] The disparity in the experts' countries of origin was criticized for its geographical bias.[26]

When deliberating the Tallinn Manual 2.0, the Group of Experts tried to overturn this critique by emphasizing the appearance of experts from China, Japan, Israel and Thailand.[27] Though the majority of experts still came from Western countries, all experts claimed to participate in their personal capacity,[28] and that their participation in the drafting process did not reflect their affiliation. It has therefore been argued that the lack of experts or participants from certain countries reportedly engaging in cyber operations may not necessarily undermine the authority of the Manuals.[29]

As regards the legitimacy of the individual experts, their selection was based on two factors:

(1) an impersonal validity claim; and
(2) the experience and position of the expert.[30]

---

[24] The International Group of Experts is divided into many functional groups, namely, Editorial Committee, Legal Group Facilitators, Legal Experts, Technical Experts.

[25] See the list of International Group of Experts appeared in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, pp. 6–9.

[26] Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict and Security Law*, 18, p. 331.

[27] There are Professor *Zhixiong Huang* from Wuhan University, Professor *Kazuhiro Nakatani* from University of Tokyo, *Deborah Housen-Couriel* from University of Haifa, and *Kriangsak Kittichaisaree*, a Member of the ILC from Thailand.

[28] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 23; see also *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 2.

[29] Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press, p. 32.

[30] Kessler, O. and Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 26, p. 802.

Firstly, each expert needed to present himself/herself as independent from his/her personal preference and convince the audience that the knowledge he/she produces is validly objective.[31] Secondly, only persons who hold specific skills, knowledge and experience were supposed to be able to satisfy the public trust in producing knowledge.

These two factors seem ambiguous in the International Group of Experts. Regarding the first factor, despite its strong claim to impersonality, the experts cannot escape the criticism as to the dominant position of Western countries. Commentators have therefore not only pointed to the disparity of countries where the experts came from, but also highlighted the sources of evidence used by the experts to justify the existence of *lex lata*.[32] It has been reported that the rules in the Tallinn Manuals are heavily drawn from the military manuals of four countries (Canada, Germany, the United Kingdom, and the United States) with the underlying claim that

> *"the international community generally considers these four manuals to be especially useful during legal research and analysis with respect to conflict issues".*[33]

The word "useful" may have been used to avoid the impression that the military manuals of four NATO states might have served as direct sources of authority. Against this background, it is problematic that the International Group of Experts audaciously asserted that the Tallinn Manuals, which in effect stand for the opinions of a few Western states, represent the international community as a whole.[34]

As *Mégret* has asserted, international humanitarian law today is still attached to the Western image of statehood and the corresponding understanding of international law's nature and function.[35] While most international lawyers support the function of humanitarian law as regulating warfare, the realist or the anti-colonialist might perceive

---

[31] Ibid.

[32] Fleck, D. (2013), op. cit., pp. 331–351; see also Kessler, O. and Werner, W. (2013), op. cit., pp. 793–810.

[33] Fleck, D. (2013), op. cit., p. 335.

[34] Kessler, O. and Werner, W. (2013), op. cit., p. 803.

[35] Mégret, F. (2005) From 'Savage' to 'Unlawful Combatant': A Postcolonial Look at International Humanitarian Law's Other. In: Anne Ordord (ed.). *International Law and Its Others.* Cambridge: Cambridge University Press. Available also from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=918541

the role of the law of armed conflict as a tool to reinforce the "unshakeable grip" of dominant states.[36] However, it would also be unfair to label the Tallinn Manuals as products of neo-colonialism.[37] Nonetheless, the flaws in the drafting process have an inherent potential to undermine their authoritative degree.

The second factor in the selection process was the reputation of the experts. The pertinent element to be examined is the criteria to select the qualified experts to participate in the Tallinn Manuals project. From the start, the Tallinn Manuals were initiated and sponsored by the NATO CCDCOE which confided the task to select the members of the International Group of Experts to the Director, *Michael Schmitt*, Chair of the international law department at the US Naval War College and author of widely quoted articles related to cyber operations.[38] *Schmitt* enjoyed full discretion in composing the group of experts.[39] Neither *Schmitt* nor the Tallinn Manuals explain the selection process. The Tallinn Manuals merely describe the composition with reference to the various personal backgrounds: international law academics, practitioners, serving or former military officials and technical experts. Though there exists no determinative rule under international law how to decide who is a highly qualified publicist or legal expert, the selected experts assume an important status: Their comments were captured in the Tallinn Manuals to which the audience can make a reference. If one compares the role of experts to judges at the International Court of Justice, though they enjoy different competences, one can observe that the Court's judgments enjoy more credibility and authority as they are made by a representatively composed body, rather than by a "like-thinking" group of experts.[40] Therefore, to firmly reject the critique over the bias of experts, the transparency of the selection process of experts is advisable. Only then can the validity of the claim that the Tallinn Manuals reflect *lex lata* be assessed.

---

[36] Ibid.

[37] Kessler, O. and Werner, W. (2013), op. cit., p. 803.

[38] *Michael Schmitt* produces many articles related to cyberwarfare, especially during and after being the Director of the Tallinn Manual and the Tallinn Manual 2.0. But the article before involving in the Tallinn project that triggers the debate on the legal aspects of cyberwar appears in Schmitt, M. (1998–1999) Computer Network Attacks: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 37, pp. 885–935.

[39] The quote is taken from a presentation by *Michael Schmitt* on the Tallinn Manual CyCon 2012 organized by the NATO CCDCOE (see US Naval War College. (2012) *Cycon 2012 Michael Schmitt: Tallinn Manual Part I*. [online video] Available from: http://www.youtube.com/watch?v=wY3uEo-Itso (1:40) [Accessed 20 July 2018].

[40] Schachter, O. (1977), op. cit., p. 222.

3.2 IMPOSITION OF THE CONVENTIONAL USE OF FORCE ON CYBER OPERATIONS

In this section, the focus is shifted to the drafting process of the Tallinn Manuals. To decide whether the Tallinn Manuals secure the status as an instrument objectively providing evidence of international law on cyber operations, one must observe how the rules have been established in the Manuals.

Due to the limited space and the large number of rules inscribed in the Tallinn Manuals, it is impossible to analyze the drafting process of each rule. The rules related to the use of force is selected for the analysis because it represents the cornerstone linking the existing international law with the novel threat of cyber operations.

The most vital aspect of the application of the law on the use of force to cyber operations is:

> *"under what conditions cyber operations can constitute the use of force prohibited by Article 2 (4) of the UN Charter and customary international law".*

The International Group of Experts attempts to extend the existing prohibition of the use of force to cover also cyber operations by referring to the ICJ's statement in the *Nicaragua* case that distinguished *"the most grave forms of the use of force from other less grave"*.[41] The Group concludes that, despite the lack of a definition of "use of force", the difference between use of force and an armed attack relies upon "scale and effect".[42] Rule 11 of the first version of the Tallinn Manuals and Rule 69 of the Tallinn Manual 2.0 stipulate that

> *"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."*

According to this assertion, the consequences of cyber operations are a vital factor to distinguish "cyber operations" that qualify as the use of force from those that do not. The Tallinn Manuals also acknowledge

---

[41] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America).* Judgement of 27 June 1986. ICJ Report 1986, para. 191.

[42] Schmitt, M. (2015) The Use of Cyber Force and International Law. In: Marc Weller (ed.). *The Oxford Handbook of the Use of Force in International Law.* Oxford: Oxford University Press, pp. 1111–1114.

the different qualitative level between use of force and an armed attack, whereas only cyber operations reaching the threshold of an armed attack trigger the right to self-defense of the victim state.[43]

However, the adoption of the "scale and effect" threshold leaves much room for interpretation.[44] The Group, therefore, adopted an approach comprising eight factors, to assist states in determining when the international community would likely characterize a cyber operation launched against them, or that they conducted, as a use of force.

(1) *Severity*. A cyber operation causing death or injury of persons is sufficiently severe to qualify as a use of force, while a psychological operation in cyberspace generating irritation or inconvenience would never qualify as such.
(2) *Immediacy*. The negative consequences of a cyber operation shall be immediately visible to be qualified as a use of force. Unlike the less visible and delayed consequences, there will be more opportunities to mitigate those consequences or resolve the situation peacefully.
(3) *Directness*. The causation chain of a cyber operation and its effect shall be examined. The closer the link between a cyber operation as cause and its effect, the more likely that the cyber operation will be characterized as a use of force.
(4) *Invasiveness*. This refers to the conventional concept of use of force where there exists an intrusion into the target state's border. A cyber operation will be more invasive if it intrudes into the secured system of the target state without its consent. For example, the attack on domain names belonging to critical public agencies such as *.gov*, *.mil* is more invasive than the attack directed at non-state specific domain names such as *.com*.
(5) *Measurability of effects*. Typically, the effect of the use of armed force is measurable. However, in cyberspace, the consequences may be less apparent. If the consequences of a cyber operation can be assessed in specific terms such as the percentage of servers disabled and the amount of data corrupted, it is likely to be considered as a use of force.

[43] Rule 69 of *The Tallinn Manual on the International Law Applicable to Cyber Warfare* and Rule 71 of *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.*

[44] Schmitt, M. (2015), op. cit., p. 1114.

(6) *Military character*. A cyber operation that occurs in a military context increases the likelihood to be constituted as a use of force.
(7) *State involvement*. If there is evidence that a state is involved in the cyber operation, the chance that the cyber operation amounts to a use of force will be higher.
(8) *Presumptive legality*. Under international law, it is generally accepted that the application of violence is unlawful, unless authorized – such as in self-defence. Psychological operations and economic coercion are not expressly prohibited. Therefore, the cyber operation holding a similar characteristic as economic pressure or psychological operations is less likely to be equated as a use of force.

Although the "scale and effect" approach embraces the material aspect of violence similar to the implicit notion of force in the conventional use of force, the application of the eight-factor rule on cyber operations is not without problems.

Firstly, the eight-factor rule was based in essence on *Michael Schmitt's* original work written in 1999 in which he gathered these factors based on his observation of what arguments have influenced states in assessing whether or not a use of force has taken place.[45] However, no hard evidence of state practice or *opinio juris* related to the eight-factor rule appears neither in *Schmitt's* original work nor in the Tallinn Manuals. It appears to be based on the author's intuition, disguised as an empirical method.

Secondly, certain criteria from the eight-factor rule allow certain kinds of cyber operations to escape legal regulation as the characteristics of cyber operations are not fully captured. For instance, the "invasiveness" criterion is not compatible with DDoS Attacks, where the targeted computer system or network is not penetrated, but thousands of requests flood the target system to paralyze its function. The "measurability of effects" of cyber operations is notoriously arduous since the effect-based approach does not clarify which standards of proof is valid. There are various standards of proof to choose from: "beyond any doubt"[46], "convincing evidence"[47], "*prima facie* evidence"[48], and "sufficiently convincing"[49] evidence. *D'Aspremont* points out that, due to such a wide choice, the International

[45] For further detail of the eight-factor background see Schmitt, M. (1998–1999), op. cit., p. 921.

Group of Experts may be tempted to maximize the efficacy of evidencing, for instance by lowering the standard of proof.[50] As to "presumptive legality", the logic on what is not prohibited is permitted is obsolete, as noted by Judge *Simma*:

> *"[The fact that] the international legal order might be consciously silent or neutral on a specific fact or act has nothing to do with non liquet, which concerns a judicial institution being unable to pronounce itself on a point of law because it concludes that the law is not clear. The neutrality of international law on a certain point simply suggests that there are areas where international law has not yet come to regulated, or indeed, will never come to regulate."*[51]

Accordingly, there is a possibility that certain acts might be tolerated which does not mean that the act is legal.

It is understandable why the International Group of Experts asserted their authority to identify the current *lex lata* and to avoid articulating *lex ferenda*. Had the experts decided to claim the role of international law legislator, it would have contradicted their own orthodox understanding of international law-making, which relies on the consent of states, and would have undermined their legitimacy. They, thus, chose a modest strategy conceiving of themselves as assistants who merely displayed the current state of international law by ostensibly using the classic legal tools.

---

[46] This is the standard used by the ICJ in the Genocide case in relation to demonstrating the full knowledge of the intent to perpetrate genocide by the leaders of the army of the Republic Srpska for the sake of complicity within the meaning of Article 3 (e) of the Genocide Convention (see *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro).* Judgment of 26 February 2007, ICJ Report 2007, para. 422).

[47] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, op. cit., paras. 24, 29, 62, 109; *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda)*, op. cit., paras. 72, 91, 136.

[48] This is the standard that some scholars have extracted from the WTO panel decision (see Waincymer, J. (2002) *WTO Litigation: Procedural Aspects of Formal Dispute Settlement.* London: Cameron May, p. 568).

[49] Greenwood, C. (1987) International Law and the United States, Air Operations Against Libya. *West Virgina Law Review*, 89, p. 935.

[50] D'Aspremont, J. (2016) Cyber Operations and International Law: An Interventionist Legal Thought. *Journal of Conflict & Security Law*, 21, pp. 581–582.

[51] Declaration of Judge Simma, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, 22 July 2010. ICJ Reports 2010, para. 9.

As long as the criticism regarding the transparency of the expert selection process and the flaws on the articulation of Rules, in particular pertaining to the use of force, are not casted out, the degree of the authority of the Tallinn Manuals as reflecting *lex lata* is questioned. Still, they are the products of a communicative process which will undoubtedly influence the making of international law on cyber operations. If the immobility of the traditional international law-making process – whether in form of universal conventions or judgments from authoritative tribunals indicating customary international law – cannot be overcome, this communicative practice will definitely contribute to future international law-making.

4. CONCLUSION

International law-making at times involves the opinions of legal scholars and international lawyers. The Tallinn Manuals are no different in this respect. However, the claim that the Tallinn Manuals present the existing international law is debatable due to the imbalanced composition of the drafters, their questionable authority and the opaque drafting process. This article addressed the question to what extent legal scholarship plays a role in international law-making. Based on communicative practices, it argues that legal scholarship has a significant influence on the formation and interpretation of international law. The role of legal scholars contributing to the international law-making has been particularly relevant during the absence of concrete and specific international legal rules on cyber operations. The article argues that significant parts of the Tallinn Manuals have been shaped by the intuition of legal scholars, however, without disclosing this fact. As scholars will continue to play a significant role in the making of international law, this article argues that, in this process, issues of legitimacy need to be addressed more thoroughly by future scholarship.

LIST OF REFERENCES

[1] *(2013) UN Doc A/68/98.*

[2] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro).* Judgement of 26 February 2007. ICJ Report 2007.

[3] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America).* Judgement of 27 June 1986. ICJ Report 1986.

[4] *Case Concerning the Arrest Warrant of 11 April 2000* (*Democratic Republic of Congo v. Belgium*). The Joint Separate Opinion of Judge Higgins, Kooijmans and Buergenthal, Judgement of 14 February 2002. ICJ Reports 2002.

[5] D'Aspremont, J. (2016) Cyber Operations and International Law: An Interventionist Legal Thought. *Journal of Conflict & Security Law,* 21.

[6] Declaration of Judge Simma, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo,* Advisory Opinion, 22 July 2010. ICJ Reports 2010.

[7] Fleck, D. (2013) Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict and Security Law,* 18.

[8] Greenwood, C. (1987) International Law and the United States, Air Operations Against Libya. *West Virgina Law Review,* 89.

[9] Kammerhofer, J. (2013) Lawmaking by Scholars. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking.* Cheltenham: Edward Elgar.

[10] Kessler, O. and Werner, W. (2013) Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law,* 26.

[11] Kingsbury, B. Krisch, N. and Stewart, R. (2005) The Emergence of Global Administrative Law. *Law and Contemporary Problems,* 68.

[12] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.* Advisory Opinion of 9 July 2004, ICJ Reports 2004.

[13] Luhmann, N. (1993) *Das Recht der Gesellschaft.* Frankfurt: Suhrkamp.

[14] Lynn, W. J. (2011) *Remarks on the Department of Defense Cyber Strategy as Delivered by Deputy Secretary of Defense William J. Lynn.* [speech] 14 July. Available from: http://www.defense.gov/speeches/speech.aspx?speechid=1593 [Accessed 12 July 2018].

[15] Mégret, F. (2005) From 'Savage' to 'Unlawful Combatant': A Postcolonial Look at International Humanitarian Law's Other. In: Anne Ordord (ed.). *International Law and Its Others.* Cambridge: Cambridge University Press.

[16] Parry, C. (1965) *The Sources and Evidence of International Law.* Manchester: Manchester University Press.

[17] Pauwelyn, J. (2012) Informal International Lawmaking: Framing the Concept and Research Questions. In: Joost Pauwelyn, Ramses Wessel and Jan Wouters (eds.). *Informal International Lawmaking.* Oxford: Oxford University Press.

[18] Reisman, M. (1981) International Lawmaking: A Process of Communication. *American Society of International Law Proceedings,* 75.

[19] Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press.

[20] Schachter, O. (1977) The Invisible College of International Lawyers. *Northwestern University Law Review,* 72.

[21] Schmitt, M. (1998–1999) Computer Network Attacks: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law,* 37.

[22] Schmitt, M. (2015) The Use of Cyber Force and International Law. In: Marc Weller (ed.). *The Oxford Handbook of the Use of Force in International Law.* Oxford: Oxford University Press.

[23] Skouteris, T. (2001) The Force of a Doctrine: Art. 38 of the PCIJ Statute and the Sources of International Law. In: Fleur Johns et al. (eds.). *Events: The Force of International Law.* New York: Routledge.

[24] Slaughter, A.-M. (2000) Agencies on the Loose? Holding Government Networks Accountable. In: George Bermann and Peter Lindseth (eds.). *Transatlantic Regulatory Cooperation, Legal Problems and Political Prospects.* Oxford: Oxford University Press.

[25] Teubner, G. (1997) Global Bukowina: Legal Pluralism in the World Society. In: *Global Law Without a State.* Hants: Dartmount.

[26] *The Tallinn Manual on the International Law Applicable to Cyber Warfare.*

[27] *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation.*

[28] Tikk, E. Kaska, K. and Vihul, L. (2010) *International Cyber Incidents: Legal Considerations.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

[29] Triggs, G. (2005) The Public International Lawyer and the Practice of International Law. *Australian Yearbook of International Law,* 24.

[30] US Naval War College. (2012) *Cycon 2012 Michael Schmitt: Tallinn Manual Part I.* [online video] Available from: http://www.youtube.com/watch?v=wY3uEo-Itso (1:40) [Accessed 20 July 2018].

[31] Venzke, I. (2013) Contemporary Theories and International Law-making. In: Brölmann Catherine and Radi Yannick (eds.). *Research Handbook on the Theory and Practice of International Lawmaking.* Cheltenham: Edward Elgar.

[32] Waincymer, J. (2002) *WTO Litigation: Procedural Aspects of Formal Dispute Settlement*. London: Cameron May.