LEGAL REGULATION OF CYBER WARFARE: REVIEWING THE CONTRIBUTION OF THE TALLINN MANUAL TO THE ADVANCEMENT OF INTERNATIONAL LAW

MICHAEL SANG

Supervised by

Cathleen Powell & Dr Hannah Woolaver

Thesis presented for the approval of Senate in partial fulfilment of the requirements for the degree of Master of Laws in International Law in the Department of Public Law.

February 2015

Word Count 27,704

LEGAL REGULATION OF CYBER WARFARE: REVIEWING THE CONTRIBUTION OF THE TALLINN MANUAL TO THE ADVANCEMENT OF INTERNATIONAL LAW

Michael Sang

SNGMIC005

Supervised by

Cathleen Powell & Dr Hannah Woolaver

February 2015

I do hereby declare that I have read and understood the regulations governing the submission of a Master of Laws dissertation, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

_____

Michael Sang

ACKNOWLEDGEMENTS

This study would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this thesis.

First and foremost this thesis could not have been written without the assistance of my Supervisor Dr Cathleen Powell who encouraged and challenged me throughout as I embarked on this strenuous journey. She never accepted less than my best efforts and allowed me to exercise my academic freedom in this research. Thank you for your kindness, friendship, support, generosity and encouragement. I am equally indebted to my co-supervisor Dr Hannah Woolaver for her advice as I began working on this thesis that ultimately shaped its final outcome. I thank her also, for her sacrifice in examining the entire draft of this research and giving me valuable feedback for which I am extremely grateful.

I also wish to acknowledge the University of Cape Town as a whole and in particular the School of Advanced Legal Studies for providing a conducive, academic environment which has played a significant role in completion of this thesis. I have spent long nights and days in solitude in the research commons area of the main campus library and in the Bran Van Zyl law library both of which are tremendously equipped with valuable and enormous academic materials that I found in articles or in books that have collectively formed the content of this thesis however, I make no claim to be comprehensive. I thank the library staff if I may mention a few, Mr Malixole Sityana, Ms Zoelfa Jaffer and Chiedza Gwaka for their assistance in helping me access valuable texts.

Gratitude must equally be expressed to my respected lecturers Professor Jan Glazewski, Professor Danwood Chirwa, Dr Hannah Woolaver, Dr Kelly Moult and Ms Michaela Young all of whom taught me during my coursework. I certainly continue to learn a lot from them. I would also like to thank Professor Elrena Van Der Spy who was the first faculty member I met in the Wilfred and Jules Kramer building when I joined the school of law and she gave me some wise tips that I still hold on to. I am grateful for their encouragement and inspiration.

I am also grateful to all my colleagues and my friends, Kato Wambua, John Nkerebuka and David Baraza for their encouragement and moral support throughout the entire period. I am indebted to them.

I am also appreciative to my family with special regard to my respected parents and my good brothers and sisters for their great and abiding influence, for their unflinching support, and for their steadfast encouragement and unwavering confidence in me. I thank my entire family for this.

Above all my unfailing love and appreciation is due to the Most High and who I constantly seek in my moments of doubt. I seek his guidance and direction during my successes and also during my failures. Through his spirit I am humbled for I firmly know that it is only God who makes all things possible. Thank You.

TABLE OF CONTENTS

CONTENTS

Chapter One

Chapter Four

Chapter Five

Treaties

Charter of the United Nations, Adopted in 26 June 1945, entry into force: 24 October 1945.

Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 3.

Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Conflict in the Field, 12 August 1949, 75 UNTS 31.

Geneva Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949, 75 UNTS 85.

Geneva Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949, 75 UNTS 135.

Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 75 UNTS 287.

Hague Convention (IV) Respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat 2277.

Hague Convention (V) Respecting the Rights and Duties of Neutral Powers in Case of War on Land, 36 Stat 2310.

Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, 18 October 1907, 36 Stat 2415.

North Atlantic Treaty (Washington Treaty) 34 UNTS 234.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims in International Armed Conflicts, 8 June 1977, 1125 UNTS 3.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims in Non- International Armed Conflicts, 8 June 1977, 1125 UNTS 609.

Statute of the International Court of Justice, 59 Stat. 1031, U.N.T.S. 993.

Vienna Convention on the Law of Treaties 1155 UNTS 331.

Case Law

Non-treaty Instruments

Declaration of Minimum Humanitarian Standards reprinted in UN Doc E/CN.4/Sub.2/1991/55, revised in 1994, UN Doc E/CN.4/1995/116.

Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, GA Res 25/2625, UN Doc. A/RES/25/2625 (24 October 1970).

Harvard Program on Humanitarian Policy and Conflict Research *Manual on International Law Applicable to Air and Missile Warfare, with Commentary* (2010).

International Law Commission, Responsibility of States for Internationally Wrongful Acts, UNGA Res 56/83 annex, UN Doc A/RES/56/83 (12 December 2001).

International Law Association, *Final Report of the Committee: Statement of Principles Applicable to the Formation of General Customary International Law*, 69 International Law Association Representatives Conference, (2000).

L Doswald-Beck (ed), *San Remo Manual on International Law Applicable to Armed Conflict at Sea* (1995).

MN Schmitt et al (eds) *San Remo Manual on the Law of Non-International Armed Conflict with Commentary* (2006).

MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013).

Statement of Principles Applicable to the Formation of General Customary International Law, in International Law Association (ILA), Report of the Sixty-Ninth Conference (2000).

Military Manuals and Policy Documents

BMZ of Germany, Human Rights in German Development Policy, BMZ Strategy Paper 4, BMZ: (2011).

Canada, Office of the Judge Advocate General, *Law of Armed Conflict at Operational and Tactical Levels*, B-GJ-005-104/FP-021 (2001).

Chairman of the Joint Chiefs of Staff, *The Military Strategy for Cyberspace Operations* (2006).

European Union, *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace* (2013).

German Federal Ministry of Defence, *Manual of Humanitarian Law in Armed Conflicts*, VR II 3, DSK VV207320067, Zdv 15/2 (1992).

Government of Canada, *Canada's Cyber Security Strategy* (2010).

Government of the Netherlands, Response to the AIV/CAVV Report on Cyber Warfare.

HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (2010).

Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (1994) Publication 1-02.

Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, *Joint Terminology for Cyberspace Operations* (2010).

NATO, *Active Defence, Modern Engagement: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (2010).

Russian Federation, *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*, 9 September 2009.

The Commander's Handbook on the Law of Naval Operations (2007).

The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011).

The White House, *National Security Strategy* (2010).

UK Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, JSP 383 (2004).

UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (2004).

US, *National Strategy to Secure Cyberspace* (2003).

US, *National Security Strategy* (2010).

US Department of Defense, *Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934, November 2011.

US Navy/US Marine Corps/US Coast Guard, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M/MCW P 5-12.1/COMDTPUB P5800.7A (2007).

US Department of Defense, *Cyberspace Policy Report* (2011).

US Department of Defense, Office of General Council, *An Assessment of International Legal Issues in Information Operations* (1999).

US Joint Chiefs of Staff, *Joint Terminology for Cyberspace Operations* (2010).

Documents of Treaty Bodies

CESCR, General Comment No. 3: The Nature of State Parties' Obligations, UN Doc. E/1991/23, 14 December 1990.

CRC, General Comment No. 5: General Measures of Implementation of the Convention on the Rights of the Child (Arts. 4, 42 and 44, para 6), UN Doc. CRC/GC/2003/5, 27 November.

Report of the Independent Fact-Finding Mission on the Conflict in Georgia (2009) Vol II, 217-19.

Report of the Human Rights Council's Advisory Committee, Report on Enhancement of International Cooperation in the Field of Human Rights, A/HRC/19/74, 29 February 2012.

Report of the Open-ended Working Group to Consider Options regarding the Elaboration of an Optional Protocol to the ICESCR on its 2 nd Session, UN Doc. E/CN.4/2005/52.

Report of the Secretary General, Progressive Development of the Principles and Norms of International Law Relating to the New International Economic Order, UN Doc. A/39/504/Add. 1/23 October 1984.

List of Abbreviations

AP I	First Additional Protocol to the 1949 Geneva Conventions, relating to the Protection of Victims of International Armed Conflicts (1977)
AP II	Second Additional Protocol to the 1949 Geneva Conventions, relating to the Protection of Victims of Non- International Armed Conflicts (1977)
DDoS	Distributed Denial of Service attacks
ECOSOC	United Nations Economic and Social Council
GC I	First Geneva Convention, for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949)
GC II	Second Geneva Convention, for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (1949)
GC III	Third Geneva Convention, relative to the Treatment of Prisoners of War (1949)
GC IV	Fourth Geneva Convention, relative to the Protection of Civilian Persons in Time of War (1949)
GGE	Group of Governmental Experts
ICJ	International Court of Justice
ICJ Reports	International Court of Justice, Reports of Judgments, Advisory Opinions and Orders
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for the Former Yugoslavia
ILC	International Law Commission
ILM	International Law Materials
ILR	International Law Reports
NATO	North Atlantic Treaty Organization
PCIJ	Permanent Court of International Justice

PCIJ Reports	Reports of the Permanent Court of International Justice
RIAA	Reports of International Arbitral Awards
UK	United Kingdom
UN	United Nations Organization
UN Charter	Charter of the United Nations
UN Doc	United Nations Document
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
US	United States
VCLT	Vienna Convention on the Law of Treaties

Chapter I

CYBER OPERATIONS AS A CONTEMPORARY INTERNATIONAL LEGAL ISSUE: THE LEGAL PROBLEMS AND APPLICABLE LAW

1. INTRODUCTION

The development of modern technology is inevitably bound to change the conduct of warfare.[1] It is also self-evident that the mode, typology and participants in current armed conflicts do not fit within the structures of traditional international law on the use of armed force.[2] Indeed, in some cases the new conflicts pose intractable challenges to the existing law.[3] This is particularly true with regard to the military use of cyber operations either in the context of armed self-defence or in the conduct of hostilities in time of armed conflict.[4] The establishment of the worldwide computer network and the increasing reliance on digital services has brought about a new type of clear and present danger: the threat of cyber attack.[5]

The fact that cyber operations are a relatively novel phenomenon in the history of international law automatically raises some important questions regarding whether the existing rules of international law apply to them.[6] Consider the evidence indicating that there have been Chinese government-backed cyber operations, including espionage, targeting State and corporate computer networks in the United States.[7]

The question that arises in regard to cyber incidents, like the one illustrated above, is whether international law governs them, and if so which specific rules apply, and the circumstances in which they apply. With the aim of clarifying the uncertainty as to the specific rules pertinent to cyber warfare, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* was

---

[1] D Fleck, 'Introduction' in D Fleck (ed), *The Handbook of International Humanitarian Law* (2013).
[2] T Gazzini, *The Changing Rules on the Use of Force in International Law* (2005); Y Dinstein, *War, Aggression and Self-Defence* (2012); N Cox, *Technology and Legal Systems* (2006).
[3] R Arnold & PA Hildebrand, *International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenges* (2005).
[4] M Roscini, *Cyber Operations and the International Law on the Use of Force* (2013).
[5] F Schreier, *On Cyber Warfare* (2014) DCAF Horizon 2015 Working Paper No. 7, 7: "Since information technology and the internet have developed to such an extent that they have become a major element of national power, cyberwar has become the drumbeat of the day as nation-states are arming themselves for the cyber battlespace."
[6] HH Dinniss, *Cyber Warfare and the Laws of War* (2012).
[7] E Nakashima & W Wan, 'China's Denials about Cyber Attacks Undermined by Video Clip' Washington Post, 24 August 2011.

developed by a group of twenty renowned international law scholars and practitioners.[8] It provides a useful basis on which to identify how and evaluate the extent to which international law applies to cyber operations.[9]

This research seeks to critically appraise both the current and prospective contribution of the Tallinn Manual to the advancement of international law. In particular, it focuses on how international law as enunciated in the Tallinn Manual governs cyber operations in general and how it applies to cyber-unique aspects of this form of warfare.

The research then reviews the achievements of the Tallinn Manual as well as its shortfalls in relation to the development of a coherent framework of international law that can be used to govern cyber operations. After this, the research turns to the increasing role of non-binding instruments of international law in the process of international law-making. The case is then made for the possibility of the Tallinn Manual being the basis on which future binding norms may be crafted to provide specific legal regulation for cyber operations.

2. EMERGENCE OF CYBER OPERATIONS AS AN INTERNATIONAL LEGAL ISSUE

2.1 Initial Academic Concern

The questions surrounding the use of cyber operations and their legal implications began to emerge in the later part of the 1990s.[10] In 1999 the United States Naval War College organized a legal conference where legal experts presented papers on various aspects of cyber operations.[11] The proceedings of this conference were subsequently compiled in an edited volume, which has since become an important reference in research on cyber operations.[12]

However, in the years following the 1999 conference at the US Naval War College, cyber warfare and, in particular, its international legal implications received little attention. This was primarily because of subsequent political and international developments, particularly the so-called "war on terror".[13] This attitude would later change in the wake of some cyber incidents, which made clear the fact that the once theoretical and hypothetical spectre of massive cyber

---

[8] MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013).
[9] Roscini (n 4) 30.
[10] M Ignatief, *Virtual War: Kosovo and Beyond* (2000).
[11] BT O'Donnell & JC Kraska, 'Humanitarian Law: Developing International Rules for the Digital Battlefield' (2003) 8 *Journal of Conflict and Security Law* 133.
[12] MN Schmitt & BT O'Donnell (ed), *Computer Network Attack and International Law* (2002).
[13] Tallinn Manual (n 8) 1.

operations causing injury, death or destruction, whether directly or indirectly, was increasingly becoming a reality.

2.2 Cyber Incidents and the Awakening of International Legal Concern

2.2.1 *Cyber Operations against Estonia*

Cyber operations returned to the forefront of international concern in 2007 after the massive computer network attack against Estonia, and particularly the disruption and disabling of government information systems and commercial internet infrastructure.[14] The cyber attacks arose when disgruntled ethnic Russians objected to the Estonian government's decision to relocate a Soviet World War II monument (the statue of the bronze soldier) previously situated in the centre of Tallinn to a military cemetery outside the city.[15]

The objection of the ethnic Russians towards the relocation of the statue resulted in the cyber attacks against Estonia. These consisted of organized and coordinated denial of service and distributed denial of service attacks against critical government websites such as the presidential and ministerial website as well as the parliamentary website.[16] The attacks also targeted commercial interests such as banking information systems and newspapers.[17]

The cyber attacks against Estonia, which began on 27 April 2007, continued over a period of several weeks.[18] They had the general effect of disrupting essential government services and communication systems which had an adverse impact on the country's economy.[19] Moreover, the attacks were attended by "widespread social unrest and rioting, which left 150 people injured and one Russian national dead."[20]

It has never been conclusively determined which State or non-State entity was responsible for the cyber operations against Estonia, but the finger of suspicion has been pointed at Russian

---

[14] MN Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (2011) 56 *Villanova Law Review* 569.
[15] Ibid.
[16] E Tikk, K Kaska & L Vihul, *International Cyber Incidents – Legal Considerations* (2010) 15.
[17] Ibid.
[18] S Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' (2007) 97 *Journal of Criminal Law and Criminology* 379, 384-86; M Landler & J Markoff, 'Digital Fears Emerge after Data Siege in Estonia' New York Times, 29 May 2007, at A1.
[19] N Falliere, LO Murchu & E Chien, 'W32.Stuxnet Dossier', *Symantec Security Response Whitepaper*, Version 1.4, 11 February 2011.
[20] SJ Shackleford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27(1) *Berkley Journal of International Law* 192, 194.

authorities.[21] Specific allegations have been made that the Russian government instructed a Russian cyber crime firm[22] to instigate the attacks against Estonia. For its part, the Russian government has denied any involvement in the attacks. This illustrates the difficulty in attributing legal responsibility for cyber operations under international law.

2.2.2 *Cyber Operations against Georgia*

There have been other cyber incidents involving hostile cyber operations against States and corporate entities after the Estonian attacks. A notable example is the cyber operation mounted against Georgia during its armed conflict with the Russian Federation in 2008.[23] On 7 August 2007, Georgian forces mounted an attack against separatist forces acting within its territory. As a result, Russia launched a military offensive by launching operations in Georgian territory. The physical presence of Russian forces in Georgia was preceded and subsequently accompanied by hostile cyber operations against a large number of Georgian governmental websites, making it among the first cases in which an international political and military conflict was accompanied by a coordinated cyber offensive.[24]

2.2.3 *Cyber Operations against Iran*

Another notable cyber incident is the reported use in 2010 of the Stuxnet worm to disable Iranian nuclear coolers that were critical to the weaponization programme.[25] The factual background of this incident highlights how difficult it can be to accurately characterize a cyber operation, and consequently to determine the applicable international law. In particular, the Stuxnet incident gave rise to serious legal and practical challenges that prevented its definitive classification as an international armed conflict or an armed attack triggering the right to self-defence.

In June 2010, malicious software was identified in affected computers by independent information technology researchers who noted its "unique functions" and "level of sophistication".[26] The computer virus, later named Stuxnet, had a specific attack vector and only

---

[21] C Lotrionte, 'Active Defense for Cyber: A Legal Framework for Covert Countermeasures' in J Carr (ed), *Inside Cyber Warfare* (2012) 282; Klimburg, 'Mobilising Cyber Power' 49-50; I Traynor, 'Russia Accused of Unleashing Cyber War to Disable Estonia', The Guardian, 17 May 2007:
available at www.theguardian.com/world/2007/may/17/topstories3.russia.
[22] Roscini (n 4) 36.
[23] Tallinn Manual (n 8) 2.
[24] Tikk et al (n 16) 4.
[25] Tallinn Manual (n 8) 2.
[26] J Richardson, *Stuxnet as Cyber Warfare: Applying the Law of War to the Virtual Battlefield* (2011) 6.

targeted certain types of computers, and exhibited a high affinity for computers in Iran. It later emerged that Stuxnet was designed to disrupt and shut down the uranium enrichment facility in the city of Nantaz. After successfully infiltrating the Iranian nuclear facility's network, Stuxnet caused the centrifuge rotor components to spin at irregular speeds thereby causing vibrations that would destroy the centrifuges. While Stuxnet significantly disrupted the nuclear enrichment project, it did not destroy the centrifuges completely.[27] The origin of Stuxnet and the actors behind it remain a matter of speculation, but there are numerous reports indicating the complicity of American and Israeli State authorities.[28]

2.3 Cyber Attack as a Threat to National and Regional Security

The cumulative effect of these cyber incidents has brought home the reality that cyber operations pose a critical threat to the national security of States and to the well-being of human life and commercial interests.[29] Accordingly, States began to appreciate the importance of formulating guidelines to tackle the new threat of cyber war. Indeed, some States have already adopted cyber-specific national security policy and strategy documents.

The government of the United States, for example, has explicitly stated in its *2010 National Security Strategy* that cyber threats constitute "one of the most serious national security, public safety, and economic challenges we face as a nation."[30] For its part, the government of the United Kingdom in its *2010 National Security Strategy* cited "cyber attack, including by other States, and by organised crime and terrorists" as one of the top threats to British national security.[31] Other States, including Russia[32] and Canada,[33] have adopted strategy documents specifically dealing with the protection of their respective national security from the threat of cyber attack.

Regional organizations established under multilateral agreements have recognized the significance of the threat posed by cyber attack. An example is the approach of NATO in its

---

[27] Ibid.
[28] DE Sanger, 'Obama Order Sped Up Wave of Cyber Attacks against Iran', The New York Times, 1 June 2012 ; WJ Broad et al, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', The New York Times, 15 January 2011.
[29] P Berkowitz (ed), *Future Challenges in National Security and Law* (2011).
[30] The White House, *National Security Strategy* (2010) 27.
[31] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (2010) 11.
[32] Russian Federation, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space* (2011).
[33] Government of Canada, *Canada's Cyber Security Strategy* (2010).

2010 Strategic Concept[34] which provides suitable illustration for the contemporary relevance of the threat of cyber attack and the need to:

> 'develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations'.[35]

These developments demonstrate the fact that cyber operations have come of age as an important part of international relations that urgently needs to be regulated by international law.

2.4 Enter the *Tallinn Manual*

The cyber attacks against Estonia, a member of NATO, led to the establishment of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) located in Tallinn (the capital of Estonia) and the Cyber Defence Management Agency (CDMA). In recognition of the need to clarify the international law applicable to cyber operations, the CCDCOE set up a group of experts from its member States and it was tasked with drafting the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. This Manual was intended to clarify how and the extent to which international law governed cyber operations. The upshot of this process was the identification of 95 rules of international law, some of which will be discussed in detail in later chapters.

3. FORMULATION OF THE LEGAL PROBLEM

The use in international relations of cyber force whether in the context of self-defence or armed conflict is governed by customary international law. This statement has its basis in the *Nuclear Weapons* Advisory Opinion where the International Court of Justice stated that existing international law applies "to any use of force, regardless of the weapons employed."[36] While this view is not unanimously accepted, it is a rule of reason that the absence of a specific rule does not diminish the obligation to act in accordance with the applicable law, however general it might be. Hence, in the specific case of the conduct of cyber operations, there is a general obligation to comply with the current international law.

---

[34] NATO, *Active Defence, Modern Engagement: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (2010).
[35] Ibid at 16-17.
[36] *Legality of the Threat or Use of Nuclear Weapons* (1996) ICJ Reports 226, para 39.

Yet, it is important to note that cyber operations are an entirely new and unique phenomenon that the provisions of classical international law could not possibly have contemplated. One of the main challenges concerns the manner and extent to which international law applies to cyber operations.[37] The fact that cyber operations are an emergent and evolving form of engagement means that it is conceivable that cyber practice may quickly outpace the current international law. Thus, it becomes important to analyze the contribution of the *Tallinn Manual* to the advancement of international law.

The legal problem which the proposed research will tackle is two-fold: the critical question of how and if so the extent to which the *Tallinn Manual* has contributed to the clarification of international law pertinent to cyber operations; and the forward-looking question of the possible future role of the *Tallinn Manual* in the development of binding norms of international law governing cyber operations.

4. INTERNATIONAL LAW PERTINENT TO CYBER OPERATIONS AND THE LEGAL ISSUES ARISING

4.1 Applicability of Existing International Law

The emergence of cyber operations as a practical aspect of contemporary warfare raised a critical legal question: how does current international law govern cyber war? It can be argued that current international law applies to cyber operations, but it is important to take note of certain cyber unique circumstances which will require necessary modification. This corresponds with the gap-filling character of the Martens Clause which suggests that the absence of specific rules does not preclude the application of certain general rules of international law that are based on the principle of humanity. In its most recent enunciation, the Martens Clause provides that:

> in cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.[38]

---

[37] R Garnett & P Clarke, 'Cyberterrorism: A New Challenge for International Law' in A Bianchi (ed), *Enforcing International Law Norms Against Terrorism* (2004) 479.

[38] Article 1(2) AP I. The Martens Clause was introduced into the preamble to the 1899 Hague Convention II – Laws and Customs of War on Land. The clause took its name from a declaration read by Fyodor Fyodorovich Martens also known as Friedrich Martens, the Russian delegate at the Hague Peace Conferences 1899, and was based upon his words.

The above provision makes clear that customary international law and other mandatory principles of international law should apply even in cases for which there are no specific rules. This supports the case for the continued application of international law even to new and emerging concepts that are not expressly set forth in treaties.[39] The following sections explain the basis of the applicable international law and highlight the legal issues that arise from the extension of certain norms to the new context of cyberspace.

4.2 *Jus ad Bellum*

Article 2(4) of the UN Charter supplies the treaty-law basis for the prohibition of the threat or use of force against the territorial integrity or political independence of another State. This prohibition also finds a basis in the customary principle of sovereign equality of States, which prohibits the interference by one State in the internal affairs of other States.[40] Certain unique aspects of cyber force require a re-examination of the law on the use of force, and these will be highlighted below.

i) *Qualification of Cyber Force:* Article 2(4) of the UN Charter places an obligation on all Members of the United Nations to refrain in their international relations from the "threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." In light of this, the legal problem arises with regard to whether cyber operations qualify as "force" within meaning of Article 2(4) of the UN Charter.[41] The qualification of force typically entails conduct resulting in death, injury and destruction, or the threat of such conduct.[42] However, in the specific case of cyber operations it is unclear whether non-violent cyber operations qualify as a use of force.

ii) *Non-State Entities and Prohibition of Force:* The wording of Article 2(4) of the UN Charter prohibits the resort by States to force in the specific context of their international relations.[43] This appears to indicate that a use of force is only subject to the prohibition in Article 2(4) if the

---

[39] MM Whiteman, *Digest of International Law* (1963) vol 1, 1.
[40] *Nicaragua* judgment, para 202; *Corfu Channel (United Kingdom v Albania)* 1949 ICJ Reports 4, at 57, 108 and 152; Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, GA Res 25/2625, UN Doc. A/RES/25/2625 (24 October 1970).
[41] MN Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 929.
[42] A Randelzhofer, 'Article 2(4)' in B Simma (ed), *The Charter of the United Nations: A Commentary* (2002) 121.
[43] This provision makes reference to "members of the United Nations" which implies States, and this is supported by Article 4 UN Charter which expressly states that only States can be members of the United Nations.

conduct at issue is performed by authorized State agents or non-State entities whose conduct can be attributed to a State.[44] A legal problem may arise in the case of cyber operations where there is an insufficient link between the wrongful conduct and the non-State entities involved.[45] The question that arises in the particular case of individual "lone-wolf" hackers is whether their cyber operations are prohibited under Article 2(4) of the UN Charter.[46]

iii) ***Distinction between "Force" and "Armed Attack":*** Article 51 of the UN Charter enunciates an exception to or justifiable derogation from the prohibition on the use of force in international relations;[47] it states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations". Although Article 51 of the UN Charter provides a justifiable derogation from the prohibition of the use of force, it indicates there is a discrepancy in the thresholds of "force" within the meaning of Article 2(4) of the UN Charter and "armed attack" within the meaning of Article 51 of UN Charter.[48] The importance of establishing this distinction is relevant in respect of cyber operations because it determines the point at which a cyber incident escalates in scale and effect from a "threat or use of force" to an "armed attack", and the legal consequences that follow.[49]

However, there is little guidance as to the distinction between "force" and "armed attack" in the jurisprudence of the International Court of Justice[50] which, in the *Nicaragua* case, only went as far as finding it necessary to distinguish between the most grave forms of the use of force amounting to an armed attack from other less grave forms.[51] This hardly makes clear where the dividing line lies, an absence of clarity that is particularly unhelpful in the case of cyber operations. This begs the question "whether a cyber attack is an action below the threshold of the use of force, or a use of force, or a use of force amounting to an armed attack".[52]

---

[44] N Melzer, *Cyber Warfare and International Law* (2011) 11.
[45] MN Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed' (2012) 54 *Harvard International Law Journal Online* 24.
[46] Ibid.
[47] Randelzhofer (n 42) 796.
[48] Dinstein (n 2) 174-7.
[49] Schmitt (n 41) 929.
[50] *Oil Platforms (Islamic Republic of Iran v United States of America)* 2003 ICJ Reports 161, para 51.
[51] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* 1984 ICJ Reports 14, para 191.
[52] M Roscini, 'World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 114, 130.

iv) ***Notion of a Cyber "Armed" Attack:*** The concept of "armed attack" under Article 51 of the UN Charter necessarily involves intentional employment of weapons or any other forceful means against a State from across an international border.[53] This invariably raises the question whether cyber means of attack constitute weapons.[54] This issue has, however, been settled in the *Nuclear Weapons* Advisory Opinion where the International Court of Justice explained that Articles 2(4), 42 and 51 of the UN Charter apply in respect of any use of force, irrespective of the weapons used.[55] The position put forth in *Nuclear Weapons* indicates that cyber means can indeed constitute a weapon, provided that they are in fact used intentionally and that they produce harmful and internationally wrongful effects on a significant scale.[56]

Less certain, however, is the issue concerning the specific threshold of gravity and intensity of force required to constitute an "armed attack".[57] That this issue has been very contentious with regard to the use of kinetic weapons points to the challenge that is bound to arise is the case of cyber operations.[58] Indeed, this absence of clarity raises considerable challenges particularly in relation to cyber operations because it becomes difficult to determine when such an operation would amount to an armed attack justifying resort to lawful self-defence measures contemplated in Article 51 of the UN Charter.[59]

v) ***State Responsibility and Attribution:*** It is a generally accepted rule in international law that States bear the international legal responsibility for wrongful conduct that is attributable to

---

[53] *Nicaragua* (n 51) para 195; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004 ICJ 136, para 139; A Randelzhofer, 'Article 51' in B Simma (ed), *The Charter of the United Nations: A Commentary* (2002) 790.

[54] K Zemanek, 'Armed Attack' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (2010) para 21.

[55] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 39

[56] This standard is derived from the *Nicaragua* judgment, para 195. See also Melzer (n 44) 13: "It would thus appear that cyber operations have the qualitative capacity to qualify as an 'armed' attack within the meaning of article 51 of the UN Charter."

[57] Ibid.

[58] Y Dinstein, 'Computer Network Attacks and Self-Defense' in MN Schmitt & B O'Donnell (eds), *Computer Network Attack and International Law* (2002) 105.

[59] MN Schmitt, 'The Koh Speech and the Tallinn Manual Juxtaposed' (2012) 54 *Harvard International Law Journal* 13, 22: "Whether a cyber use of force qualifies as an armed attack depends on its 'scale and effects.' [U]ncertainty as to what those scale and effects are plagued the Tallinn Manual deliberations. The Experts observed, for instance, that the International Court of Justice differentiated a mere 'frontier incident' from an armed attack, but later opined that an attack on a single warship might qualify as an armed attack. Such inexplicable distinctions obfuscated their attempt to identify practical legal thresholds [footnotes omitted]."

them.[60] This rule applies similarly in the case of cyber operations, but its practical application is very problematic because cyber operations often enlist unsuspecting computers from around the world in order to "spin a web of anonymity around the attacker or attackers [thus] making accurate attribution uniquely difficult."[61] The practical difficulty of attributing a cyber attack is exacerbated by the inherent characteristics of cyber space: anonymity, multi-stage actions, and the rapidity with which actions are executed.[62]

It is a general rule that the international wrongful cyber conduct of State organs, even when they act in official capacity but beyond their instructions, is attributable to the State.[63] But this rule is less clear in the case of non-State actors who conduct wrongful cyber operations either on the specific instruction of or with the encouragement of the State. It is also unclear whether "a non-State actor's cyber operations that are not attributable to a State can nevertheless qualify as an armed attack justifying a defensive response at the level of a use of force against that non-State actor."[64]

Some problematic scenarios illustrate the legal problems that arise in the case of cyber operations. Consider the case where the origin of a cyber operation can be traced to cyber infrastructure belonging to State A; does this engage the international responsibility of that State A? Another instance is where cyber means belonging to or provided by State A falls into the hands of insurgents acting against State B, but not under the instruction of State A; does this engage the international responsibility of State A? The Stuxnet Worm incident, concerning a cyber operation against nuclear centrifuges in Iran, is a clear example of the challenges posed by cyber operations with particular regard to attribution.[65]

---

[60] See *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (2001), UNGA Res A/RES/56/83 of 12 December 2001; J Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (2002).
[61] OA Hathaway et al, 'The Law of Cyber Attack' (2012) 100 *California Law Review* 817, 823.
[62] N Tsagourias, 'Cyber Attack, Self-Defence and the Problem of Attribution' (2012) 17(2) *Journal of Conflict & Security Law* 233.
[63] See *Draft Articles of State Responsibility* (n 60) 44-45; *Case Concerning US Diplomatic and Consular Staff in Tehran (US v Iran)*, 1980 ICJ Reports 3, para 74; JP Kesan & CM Hayes, 'Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace' (2011-2012) 25 *Harvard Journal of Law and Technology* 482.
[64] Schmitt (n 59) 24.
[65] Richardson (n 26).

4.3 *Jus in Bello*

Jus in bello consists in the law of armed conflict which is that branch of international law that regulates the conduct of armed hostilities.[66] The following sections highlight some of the practical difficulties that are likely to arise when applying existing international law to the new and unique characteristics of cyber operations.

i) *Classification of Cyber Conflict:* One of the most problematic aspects of cyber operations under the *jus in bello* is their classification; that is, the characterization of the specific type of conflict as international, internal or otherwise.[67] The difficulty of reliably classifying a particular conflict is amplified in the case of cyber operations owing to their uniqueness as non-kinetic capabilities that are launched in cyber space.[68] First, unlike conventional operations involving kinetic weapons, cyber operations are capable of producing massive and widespread disruptive effects on a particular society or its economy without necessarily causing any physical damage that is often associated with combat action.[69]

Secondly, the actors involved in cyber operations may vary from unrelated individuals, insufficiently organized groups or groups that are organized but which exist entirely online.[70] This raises significant challenge in trying to determine affiliations for purposes of according the consequential legal protection and enforcing compliance with international humanitarian law. Thirdly, cyber operations relevant to international law are cross-border and they occur in cyber space,[71] and this, therefore, complicates the classification of conflict relative to the location of the operations.

Moreover, in the specific context of non-international armed conflict, the collective qualification of participants in cyber operations as an organized armed group will present a

---

[66] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (1994) Publication 1-02.
[67] MN Schmitt, 'Classification of Cyber Conflict' (2012) 17(2) *Journal of Conflict and Security Law* 245.
[68] MN Schmitt, 'War, Technology and International Humanitarian Law' HPHPCR, Occasional Paper Series 4 (2005) 43.
[69] WA Owens, KW Dam & HS Lin (eds), *Technology, Policy, Law, and Ethics Regarding US Acquisitions and Use of Cyberattack Capabilities* (2009) 127.
[70] Schmitt (n 67) 256.
[71] MJ Skelrov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1, 62; CC Joyner & C Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 *European Journal of International Law* 825, 865.

particular challenge.[72] Also, there is sharp division concerning whether the requisite test of protracted armed violence[73] would be satisfied, thus bringing into effect the law of non-international armed conflict, in the case of cyber incidents that are not destructive, but which nevertheless have severe consequences.[74]

ii) *Definition of Cyber Attack:* The notion of cyber attack under *jus in bello* is distinct from its counterpart under *jus ad bellum*.[75] Under *jus in bello*, an attack gives rise to prohibitions and restraints premised on the principle of distinction, which requires parties to the conflict to "at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives."[76] Article 49(1) of the 1977 Additional Protocol I to the Geneva Conventions of 1949 defines an "attack" as an act of "violence against the adversary, whether in offence or in defence."

However, it is not clear what "violence" means, a point that is not satisfactorily explained in the ICRC Commentary on the 1977 Additional Protocols.[77] This gives rise to important contentions regarding whether death, injury or destruction are critical components of the foreseeable effects of a cyber "attack".[78] The following questions are suitably illustrative in the above regard: i) does a cyber operation which disrupts, interferes or otherwise manipulates the functionality of an object without causing any physical damage constitute an "attack"?; and ii) does the permanent destruction of banking data files thus causing massive panic among the civilian population amount to an "attack"?[79]

iii) *Distinction:* Article 48 of the 1977 Additional Protocol I enunciates the principle of distinction, one of the cardinal principles of *jus in bello*;[80] it requires parties to an armed conflict to at all times distinguish between the civilian population and combatants and between civilian

---

[72] DE Graham, 'Cyber Threats and the Law of War' (2010) 4 *Journal of National Security Law and Policy* 87, 98.
[73] *Prosecutor v Tadic* (Jurisdiction) ICTY-94-1 (2 October 1995) para 70.
[74] K Dörmann, 'The Applicability of the Additional Protocols to Computer Network Attacks; An ICRC Viewpoint' in K Byström (ed), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law* (2004).
[75] Dinstein (n 2) 193.
[76] Article 48, Additional Protocol I.
[77] Y Sandoz et al, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (1987) para 1679.
[78] Melzer (n 44) 28.
[79] See the factual background of the cyber incident involving massive cyber operations against Estonia.
[80] *Nuclear Weapons* (n 55) para 78.

objects and military objectives, and to direct their operations only against military objectives.[81] Essentially, this principle prohibits direct attack against civilians or civilian objects as well as indiscriminate attacks. Although the principle of distinction may appear straightforward, several questions regarding its practical application remain unresolved.[82] In the particular context of cyber operations, an example is an attack on military cyber infrastructure using malicious computer virus which subsequently spreads to connected civilian systems.[83] The question that will arise is whether cyber operations are capable of discriminate application or whether they are "blind" weapons.[84]

iv) ***Direct Participation in Cyber Hostilities:*** The principle of distinction protects civilians only for as long as they do not take direct part in hostilities, which entails resort to means and methods of killing or injuring the enemy.[85] Consequently, when civilians take direct part in hostilities, they lose their protection against direct attack and become legitimate military targets subject to direct attack.[86] It is noteworthy, however, that the notion of "direct participation in hostilities" is narrower than the notion of "attack". Specifically, the notion of direct participation in hostilities requires the conduct in question to meet three cumulative criteria: i) it must cause death, injury or destruction, or otherwise adversely affect the military operations or military capacity of the opposing party (threshold of harm); ii) it must cause the requisite harm directly (direct causation); and iii) it must be designed in order to support one party to the detriment of the other (belligerent nexus).[87]

It is noteworthy that the concept of direct participation in hostilities is controversial, especially as it relates to the targetability of individuals.[88] The nature of cyber operations will inevitably complicate matters further because it is not clear to establish whether certain conduct

---

[81] *Prosecutor v Kupreškić et al*, IT-95-16 (2000) para 521.
[82] S Haines, 'Weapons, Means and Methods of Warfare' in E Wilmshurst & S Breau (eds), *Perspectives on the ICRC Study on Customary International Humanitarian Law* (2007) 266; DS Rudesill, 'Precision War and Responsibility: Transformational Military Technology and the Duty of Care under the Laws of War' (2007) 32 *Yale Journal of International Law* 517, 541.
[83] WH Boothby, *Weapons and the Law of Armed Conflict* (2009 OUP) 237.
[84] See Dissenting Opinion of Judge Higgins, *Nuclear Weapons* (n 55) 588-89.
[85] Article 51(3) Additional Protocol I.
[86] *Nuclear Weapons* (n 55) para 78; ICRC, *Basic Rules of the Geneva Conventions and their Additional Protocols – Understanding Humanitarian Law* (2009) 36.
[87] ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities* (2009) 995-96; MN Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 *New York University Journal of International Law and Policy* 697.
[88] See Forum: 'Direct Participation in Hostilities: Perspectives on the ICRC Interpretive Guidance' (2010) 42 *New York University Journal of International Law and Policy* 637.

is intended to support one or more of the parties.[89] There is also the possibility that one or more of the cumulative criteria for qualification as direct participation in hostilities may not be satisfied.[90] For instance, would a cyber operation by an individual hacker causing the incapacitation of a dual-use transport system or electrical grid constitute a ground for loss of protected status, regardless of the fact that it does not result in death, injury or destruction?[91] Likewise, would a cyber operation that is merely disruptive of the adversary's communication network amount to direct participation?[92]

5. OBJECTIVE OF THE STUDY

This study aims to explore the key questions that arise from the use of cyber means of warfare within the framework of international law on disputes and the use of force and in light of the *Tallinn Manual*.

6. A NOTE ON THE SCOPE OF THE RESEARCH

This research focuses on the *jus ad bellum* (international law governing the resort by States to the use of armed force) and the *jus in bello* (international law governing the conduct of armed conflict). This is because an examination of other related regimes of international law (e.g telecommunications law, aviation law and space law) will be too broad as to detract from the main aim of the present work: to clarify the legal regulation of cyber operations in the context of warfare and to speculate on the future of international law in that regard.

The main object of this research will be those cyber operations to which either the *jus ad bellum* or the *jus in bello* applies. Accordingly, it only examines legal aspects of military cyber operations to the exclusion of legal questions arising from cyber criminality or cyber terrorism. In particular, the research will not address cyber activities that do not amount to a "use of force" within the meaning of the UN Charter or those which do not meet the threshold of an "armed

---

[89] D Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) *Journal of Conflict and Security Law* 279, 285.
[90] Ibid at 288.
[91] MN Schmitt, HA Harrison-Dinniss & TC Wingfield, 'Computers and War: The Legal Battlespace' Background Paper for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law' (Cambridge 25-27 June 2004).
[92] D Albright, P Brannan & C Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Nantaz Enrichment Plant?* (2010).

conflict" within the meaning of the Geneva Conventions of 1949 and the Additional Protocols of 1977.[93]

7. STRUCTURE OF THE RESEARCH

Chapter One has identified and explained the selected challenges that cyber operations pose for current international law, and these have been supplemented by hypothetical examples that illustrate (by means of analogy to conventional warfare) the problematic nature of cyber operations and the difficulty of legal regulation.

Chapter Two provides a background into the development of the Tallinn Manual and outlines, among others, the following: its scope; its rules and accompanying commentary; the sources and authorities relied upon; the composition of the International Group of Experts; the drafting and peer-review process; and the authority of the *Tallinn Manual*.

Chapter Three adopts an objective approach to the question of how and if so the extent to which the *Tallinn Manual* has contributed to the clarification of international law applicable to cyber operations. This Chapter undertakes a critical appraisal of the merits and demerits of the *Tallinn Manual* with a view to highlighting its positive aspects and to suggesting improvements where it is lacking. The Chapter also appraises, in turn, some of the rules pertinent to *jus ad bellum* and *jus in bello*.

Chapter Four compares the Tallinn Manual, the Naval Warfare Manual and the Turku Declaration on Minimum Humanitarian Standards. By comparing the Tallinn Manual to these non-binding instruments, this Chapter highlights the importance of non-binding instruments in the progressive emergence of binding norms that may prove essential to the effective legal regulation of new forms and methods of warfare. This Chapter also explores how the non-binding rules of the Manual can be transformed into binding norms through State practice.

Chapter Five, the conclusion, provides a succinct summary of the main findings of the research and the suggestions that have been developed in order to enhance the effective legal regulation of cyber operations.

---

[93] Hathaway (n 61) 26: "Nothing was further from the minds of the drafters of the Geneva Convention than attacks carried out over a worldwide computer network."

Chapter II

THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE: AN OVERVIEW

1. INTRODUCTION

The utility of cyberspace as an additional[94] "domain of warfare"[95] presents some challenges to current international law,[96] but it does not necessarily escape from its constraints.[97] The critical question that arises is how cyber warfare can be fully regulated by the existing international law. This question can satisfactorily be answered by analyzing specific traditional norms that were developed for the kinetic context and to assess the extent to which they can be adapted to the cyber context.

The results of the above inquiry can then be used to "identify potential difficulties in their application to different types of cyber operations."[98] This was the primary task that the drafters of the Tallinn Manual who were styled as the "International Group of Experts" had to address. In particular, these Experts were charged with determining how the current rules of international law (*jus ad bellum* and *jus in bello*) applied to cyber operations, and to "identify any cyber-unique aspects thereof."[99]

2. CYBER SECURITY AND THE LEGAL FRAMEWORK OF THE NATO ALLIANCE

2.1 Collective Self-Defense Framework of the NATO Alliance

The North Atlantic Treaty Organization (NATO) was established in 1949 as a collective self-defence organization under the NATO Treaty.[100] Since it was founded in the post-World War II

---

[94] SW Brenner, *Cyberthreats: The Emerging Fault Lines of the State* (2009) 43; Remarks on the Department of Defense Cyber Strategy, As Delivered by Deputy Secretary of Defense, William J Lynn, III, 14 July 2011, available at http://www.defense./gov/speeches/speech.aspx?speechid=1593 : "In the 21st Century, bits and bytes can be as threatening as bullets and bombs".

[95] J Healy & K Grindal (eds), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (2013); DE Graham, 'Cyber Threats and the Law of War' (2010) 4 *Journal of National Security Law and Policy* 93.

[96] GJ Rattray & J Healy, Non-State Actors and Cyber Conflict' in KM Lord & T Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age* (2011) 72; R Garnett & P Clarke, 'Cyberterrorism: A New Challenge for International Law' in A Bianchi (ed), *Enforcing International Law Norms Against Terrorism* (2004) 43.

[97] Cox (n 2) 217.

[98] Roscini (n 4) 30.

[99] Tallinn Manual (n 8) 5.

[100] North Atlantic Treaty (Washington Treaty) 34 UNTS 234.

period, the NATO Alliance had as its principal object the organization of effective self-defence capabilities for Western European nations. These capabilities were meant to thwart Soviet aggression and expansionism, which characterized the Cold War period.[101] The NATO Alliance was also established to safeguard the sovereignty of State parties against the increasing calls for secession within their national borders, which in many cases led to violence between the affected State and the militant separatists.

The NATO Treaty was modelled to a large extent on the UN Charter, and this is evident from certain key provisions such as the prohibition of the use of force and the right of self-defence.[102] The very nature of the NATO Treaty, as a multilateral treaty with the main objective of ensuring effective collective self-defence, means that its provision which articulates the right of collective self-defence is critical. Article 5 of the NATO Treaty enunciates the views of the NATO Allies regarding collective self-defence:

> 'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area…'

The practical significance of Article 5 of the NATO Treaty is that it permits the resort by any member State to forceful means in the exercise of its collective right of self-defence, whenever any member State suffers an armed attack. However, it is useful to recall that not all uses of force will trigger the right of self-defence, and thus the initial use of force must rise to the level of an "armed attack" within the meaning of Article 51 of the UN Charter.[103]

This would appear to present a challenge because it limits the use of collective self-defence powers only to cases of such gravity and magnitude as to satisfy the requisite threshold of "armed attack" in Article 51 of the UN Charter.[104] This also suggests that the aim of protecting the collective security of all NATO member nations can only be realized in a very narrow set of

---

[101] MA Smith, *NATO in the First Decade after the Cold War* (2000); T Check, 'Analyzing the Effectiveness of the Tallinn Manual's *Jus ad Bellum* Doctrine on Cyber Conflict: A NATO-centric Approach' 6.
[102] U Haußler, *Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty* (2008) 100.
[103] *Nicaragua* (n 51) paras 191, 195; *Oil Platforms* (n 50) paras 57, 61.
[104] Dinstein (n 2) 210-211; WH Taft, 'Self Defense and the Oil Platforms Decision' (2004) 29 *Yale Journal of International Law* 295, 300.

cases.[105] A cautious approach is appropriate because the NATO Treaty was intended to provide a robust legal basis on which to effectively deal with threats to, and ensure the maintenance of peace and security over, a vast geographical area.[106] Given the expansive nature of its geographical field of application, it is only logical that the right of collective self-defence should be activated by high-threshold uses of force amounting to an armed attack.[107]

However, emerging capabilities require dynamic responses and thus the rigid view that only a high-threshold use of force can activate the right of collective self-defence is unsustainable. Haußler notes that the drafters of the NATO Treaty had the foresight to include in Article 13 a formal mechanism for periodic review of the provisions of the Treaty in light of contemporary developments.[108] This creates an opportunity to make appropriate amendments to the collective security arrangements so as to ensure that the security of member nations is well taken care of. But besides amendment, which has been a rare occurrence,[109] the NATO Alliance has devised a creative means to reinterpret the NATO Treaty without changing its text: strategic concepts.[110]

The utility of NATO Strategic Concepts lies in the fact that they are drafted to reflect its current doctrine as regards the security environment not only in the Transatlantic region, but also in the wider global sphere.[111] Another aspect that lends credibility to NATO Strategic Concepts is the fact that these documents are typically drafted with a view to providing interpretive guidance to member nations as to their legal obligations and policy positions regarding "concrete geopolitical circumstances."[112]

The use of Strategic Concepts has proved most useful in providing the grounds to develop norms dealing with cyber operations and information warfare.[113] In particular, the 2010 NATO Strategic Concept outlined the Alliance's commitment to develop its "ability to prevent, detect, defend against, and recover from cyber attacks".[114] It further sets out the means that it can use to achieve the above objects, including by using the "NATO planning process to enhance and

---

[105] Taft, ibid at 300.
[106] BJ Collins, *NATO: A Guide to the Issues* (2011) 11-22.
[107] A Behnke, *NATO's Security Discourse after the Cold War: Representing the West* (2013) 1-15.
[108] Haußler (n 102) 100.
[109] Ibid at 108.
[110] J Ringmose & S Rynning, *Come Home, NATO! The Atlantic Alliance's New Strategic Concept* (2009) 6.
[111] Ibid.
[112] Ibid. See also *National Security Concept of Georgia*, 2011, 9.
[113] Roscini (n 4) 3; Sean P Knauck, 'Information Warfare: New Challenges for Public International Law' (1996) 37 *Harvard International Law Journal* 272–292 at 284.
[114] NATO (n 34) 16-17.

coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations".[115]

Subsequently, the NATO Alliance began a process that ultimately led to the adoption in 2013 of the Tallinn Manual, a process that was undoubtedly propelled by the fact that some of its member nations had been targeted in cyber incidents.[116] In the following sections, the historical development of the NATO Alliance's interest in cyber capabilities and the move towards a more coherent legal and policy response to the increasing incidents of cyber attacks will be discussed in more detail.

2.2 NATO and Interest in Cyber Capabilities

The self-defence and military capabilities of individual NATO member States vary, but the impact of these differences is diminished because the NATO Treaty establishes a robust framework for collective security and defence.[117] But surprisingly this effective collective security capability has not been apparent in the case of cyber operations either conducted by or against NATO.[118] For a long time the NATO capabilities to effectively defend against all cyber threats in the Transatlantic region were considered woefully inadequate, and this was a point that most commentators found difficult to understand given NATO's role as a collective self-defence organization.[119] For instance, it has been noted that "for an organization tasked with ensuring the defense of the Transatlantic region [NATO] still has difficulties in modernizing and updating its operational capabilities."[120] Even in cases where creditable attempts have been made, their impact has been limited by the use of non-analogous comparisons.[121]

An historical examination of how NATO has responded to cyber incidents provides some insight into the claims of its lacklustre performance.[122] One of the earliest cyber incidents targeting NATO was the 1999 Denial of Service attacks that were mounted against websites

---

[115] Ibid.
[116] *Russia/Georgia Cyber War-Findings and Analysis*, Project Grey Goose: Phase I Report, 17 October 2008; E Tikk et al (n 16) 5; Schreir (n 5) 108.
[117] D Brown, 'The Role of Regional Organizations in Stopping Civil Wars' (1997) 41 *Air Force Law Review* 235.
[118] Lotrionte (n 21) 282; E Tikk et al (n 16) 4, 13.
[119] J Healey & L van Bochoven, *NATO'S Cyber Capabilities: Yesterday, Today and Tomorrow* (2011).
[120] Check (n 101) 10.
[121] N Shachtman & PW Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cyber Security is Misplaced and Counterproductive', Brookings Institution, 15 August 2011.
[122] Dinniss (n 6) 6-7.

belonging to NATO's Supreme Headquarters for the Allied Powers of Europe.[123] This cyber incident occurred during Operation Allied Force, a campaign that entailed aerial bombardment by NATO Allied Forces of Kosovo with a view to defeating military units of the Federal Republic of Yugoslavia.[124]

Although the NATO aerial warfare planners successfully countered this cyber incident, it raised the concern of the NATO Alliance as regards its general cyber capabilities, and particularly "the security of its military information networks".[125] But it was only in 2002 (three years after the event) that NATO came up with a coherent policy response to cyber threats.[126] In 2002, at the Prague Summit, the member nations of the NATO Alliance adopted the Cyber Defence Programme, setting out a strategy to combat cyber threats and to enhance cooperation.[127] This Programme was also intended to be the blueprint for the continuous development, acquisition, and implementation of collective cyber-defence capabilities.[128] However, the Cyber Defence Programme was not fully implemented, and as a consequence there was little progress in updating the NATO Alliance's operational capabilities to effectively defend against cyber threats.[129]

2.3 NATO Cyber Security and Defence Post-Estonia

The 2007 cyber operations against Estonia, a member State of NATO, renewed the interest of NATO in the field of cyber security and defence.[130] The cyber operations against Estonia marked a turning point in the manner in which NATO dealt with the issue of cyber security and defence largely because it was the first time that a member nation came under sustained cyber attack with adverse physical effects and massive economic disruption.

Consequently, in 2008, the Cooperative Cyber-Defence Centre of Excellence (CCD COE) and the Cyber Defense Management Agency (CDMA) were formally established as international

---

[123] Tikk et al (n 16) 63.
[124] Schreier (n 5) 107; N Melzer, *Targeted Killing in International Law* (2008) 130.
[125] Check (n 101) 11.
[126] F Khan, 'States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis' Institute of Strategic Studies Islamabad (ISSI) *available at* http://www.issi.org.pk/publicationfiles/1328592265_43276030.pdf.
[127] RE Overill, 'Reacting to Cyber-intrusions: Technical, Legal and Ethical Dimensions' (2003) 11 *Journal of Financial Crime* 163.
[128] Check (n 101) 11.
[129] Khan (n 126).
[130] See Section 2.2.1.

military organizations under the auspices of NATO. Since the NATO CCD COE forms part of the wider educational "framework supporting NATO Command Arrangements,"[131] it produces non-mandatory documents setting out rules of engagement. Member nations of NATO are required to sign memoranda of understanding before agreeing to be bound by the various mandates or to become part of these operations.[132] At the moment less than half (eleven out of twenty eight) of the NATO member nations participate in the operations of the NATO CCD COE.

In 2009, the NATO CCD COE invited an independent "International Group of Experts" to produce a manual outlining the international law applicable to cyber operations, resulting in the Tallinn Manual.[133] It is also significant to note that in November 2010, NATO adopted a Strategic Concept (a broad outline of its ten-year strategic objectives) that emphasized the critical importance of improving its capabilities for cyber security and defence.[134] It identified a growing trend in the militarization of cyberspace and also noted the relevant security implications: "[c]yber attacks are becoming more frequent, more organized and more costly in the damage that they inflict" and they "can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[135] In this regard, the 2010 Strategic Concept called upon all NATO member nations to develop their collective cyber security capacity in order to further the ability "to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber-protection, and better integrating NATO cyber awareness, warning and response with member nations".[136]

3. CYBER OPERATIONS AND CURRENT INTERNATIONAL LEGAL NORMS

As has been stated above,[137] the drafters of the Tallinn Manual concluded that both the international law on the use of force and the law of armed conflict apply to cyber operations.[138] But the Manual does not provide any detailed explanation as to how this view was arrived at. Yet

---

[131] Tallinn Manual (n 8) 1 at footnote 2.
[132] Check (n 101) 17.
[133] Tallinn Manual (n 8) 1.
[134] NATO (n 34).
[135] NATO (n 34) para 12.
[136] Ibid at 16-17.
[137] See Section 4.1 of Chapter 1.
[138] Tallinn Manual (n 8) 5.

this is important in providing justification for the extension of rules that apply in the kinetic context into the cyber realm. The following section seeks to supply justification for the application of current international law to cyber operations.

3.1 Legal Basis in the Law of Treaties

Article 38 of the ICJ Statute lists treaties as one of the sources of international law and, more importantly, lists it among the two key sources.[139] Treaties are international agreements "concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation".[140] If it is accepted that treaty law applies to cyber operations which rise to the level of a use of force or an armed conflict despite the fact that there is no treaty to this effect, the critical legal question that follows is: what is the legal basis for this view? The specific treaty that deals with the use of force in international relations is the UN Charter, while the law of armed conflict is governed by the 1907 Hague Conventions,[141] the Geneva Conventions of 1949,[142] and the 1977 Additional Protocols to the Geneva Conventions.[143]

An examination of the dates when the above treaties were adopted shows that they all predated the age of cyber warfare and thus provide little specific guidance as to the legal regulation of cyber operations. However, the Vienna Convention on the Law of Treaties (VCLT), whose rules reflect customary international law,[144] offers a solution by allowing progressive interpretation of established treaty provisions in order to take account of current or

---

[139] Article 38(1) Statute of the ICJ; R Gardiner, *Treaty Interpretation* (2008).
[140] Article 2(1)(a) Vienna Convention on the Law of Treaties 1155 UNTS 331.
[141] Hague Convention (IV) Respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat 2277; Hague Convention (V) Respecting the Rights and Duties of Neutral Powers in Case of War on Land, 36 Stat 2310; Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, 18 October 1907, 36 Stat 2415.
[142] Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Conflict in the Field, 12 August 1949, 75 UNTS 31; Geneva Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949, 75 UNTS 85; Geneva Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949, 75 UNTS 135; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 75 UNTS 287.
[143] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims in International Armed Conflicts, 8 June 1977, 1125 UNTS 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims in Non- International Armed Conflicts, 8 June 1977, 1125 UNTS 609.
[144] *Territorial Dispute (Libyan Arab Jamahiriya/Chad),* Judgment, 1994 ICJ Reports 6, para 41.

prospective cases, provided that there is agreement amongst the parties.[145] This concept is implicit in Article 31(3)(b) of the VCLT which provides that treaties shall be interpreted in a manner that takes into account "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation."

Article 31(3)(b) of the VCLT supports the contention that treaties are not static; rather, they are dynamic instruments and thus should be interpreted so as to take account of new and emerging contexts.[146] The necessity of a dynamic approach to treaty interpretation has been endorsed by the ICJ in its *South West Africa* Advisory Opinion, where the Court observed that "an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation".[147] This approach has been reaffirmed in the subsequent case law of the ICJ.[148]

In the context of cyber operations, the dynamic approach postulated in the *South West Africa* Advisory Opinion would require the relevant treaty law (i.e, the UN Charter, the Geneva Conventions etc.) to be interpreted so as to take the increasing prevalence of cyber threats into consideration.[149] Accordingly, the current law should be read with appropriate modification so as to govern cyber operations.[150] This is consistent with the requirement of construing treaty law not in isolation, but in concert with the actual prevailing circumstances and in the appropriate context of application.[151] It has also been regarded as essential to interpret certain treaty provisions in light of the subsequent practice of State parties to the relevant treaties.[152]

---

[145] J Arato, 'Subsequent Practice and Evolutive Interpretation: Techniques of Treaty Interpretation over Time and their Diverse Consequences' (2010) 9 *The Law and Practice of International Courts and Tribunals* 434, 459; Gardiner (n 139) 235.

[146] R Bernhardt, 'Evolutive Treaty Interpretation, Especially of the European Convention on Human Rights' (1999) 42 *German Yearbook of International Law* 15.

[147] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, Advisory Opinion, 21 June 1971, ICJ Reports 1971, para 53.

[148] *Avena and Other Mexican Nationals (Mexico v the United States)*, 2004 ICJ Reports 12, 89-98.

[149] MN Shaw, *International Law* (2002) 839.

[150] H Koh, 'International Law in Cyberspace' (2012) *Harvard International Law Journal* 3.

[151] *Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia v Malaysia)*, 2002 ICJ Reports 625, 645-46; Gardiner, Treaty Interpretation, 235.

[152] *Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v Nigeria)*, 2002 ICJ Reports 303, 407-16; *Maritime Delimitation in the Area between Greenland and Jan Mayen (Denmark v Norway)*, 1993 ICJ Reports 38, 51-52; *Border and Transborder Action: Jurisdiction of the Court and Admissibility Application (Nicaragua v Honduras)*, 1988 ICJ Reports 66, 87-88.

The jurisprudence of the ICJ provides further support for the interpretation of current treaty law so as to effectively extend legal regulation into the cyber realm.[153] In *Dispute Regarding Navigational and Related Rights* the ICJ elaborated the notion of dynamic treaty interpretation, holding that:

> 'Where parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered into for a very long period or is of 'continuing duration', the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning'.[154]

Key concepts that are addressed in the UN Charter and the Geneva Conventions, such as "self-defence" or "civilians", are generic and their continued use is contemplated in the foreseeable future.[155]

It is reasonable to conclude that the drafters of these treaties could not have intended the interpretation of these concepts to be outpaced by future developments; otherwise, the treaties would be redundant.[156] The evolutive capacity of the UN Charter with particular regard to the concept of "self-defence" in Article 51 has been supported in legal doctrine: "the rules on treaty interpretation and on the sources of international law do not exclude the possibility that Art 51 is reinterpreted, including on the basis of subsequent practice."[157] Given that a cyber operation rising to the level of an armed attack would trigger the victim State's right of self-defence, it would defeat the purpose of the UN Charter if cyber operations are excluded from its scope of application.[158]

The application of the treaty law of armed conflict is supported by the Martens Clause. Article 1(2) of Additional Protocol I (AP I), which codifies the Martens Clause, provides that in cases not covered by treaty law, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[159] The Commentary to this

---

[153] Shaw (n 149) 839-841.
[154] *Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)*, Judgment of 13 July 2009, ICJ Reports 2009, para 66.
[155] Shaw (n 149) 841.
[156] *Fisheries Jurisdiction (Spain v Canada)*, 1998 ICJ Reports 432, 461.
[157] A Randelzhofer & G Nolte, 'Article 51' in B Simma et al (eds), *The Charter of the United Nations—A Commentary* (2012) 1400.
[158] G Ress, 'Interpretation' in B Simma (ed), *The Charter of the United Nations – A Commentary, Volume I* (2012) 13-18.
[159] Article 1(2) Additional Protocol I.

provision clarifies that the Martens Clause rebuts the discredited view that acts not expressly prohibited by the relevant treaties are permitted.[160]

More importantly, with specific regard to cyber operations, the Martens Clause reaffirms the view that the treaty law of armed conflict continues to apply "regardless of subsequent developments of types of situation or technology".[161] Indeed, in its *Nuclear Weapons* Advisory Opinion the ICJ concurred that the Martens Clause provides an "effective means of addressing the rapid evolution of military technology".[162] This supports the continued application of the customary law of armed conflict irrespective of modern technological advancements.

Besides the jurisprudence of the ICJ, there is support for the view that current treaty law applies to cyber operations in the practice of States and international organizations.[163] Article 31(3)(b) of the VCLT offers a legal basis for the application of current law in cyber space, but it is vital to look at actual practice in order to ascertain the extent to which the words of this provision have been given effect in the conduct of States and international organizations.[164] Indeed, the International Law Commission acknowledges the importance of examining practice because "it constitutes objective evidence of the understanding of the parties as to the meaning of the treaty".[165]

3.1.1 Affirmative Practice of States

Some States have accepted that the mere absence of specific treaty rules governing cyber operations does not render the existing treaty law norms (some of which have attained customary status) inapplicable.[166] The practice of the United States is illustrative in this regard.[167] In 2011,

---

[160] Sandoz et al (n 77) para 55.
[161] Ibid.
[162] *Nuclear Weapons* (n 55) para 78.
[163] ICRC, IHL and Challenges of Contemporary Armed Conflicts, 36-37; UN Doc/A/68/98, 24 June 2013; UN Doc/A/66/359, 14 September 2011; EU, *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013.
[164] *Kasikili/Sedudu Island (Botswana v Namibia)*, 1999 ICJ Reports 1045, 1075; Gardiner (n 139) 225.
[165] (1966) Vol. II Yearbook of the International Law Commission 221, para 15.
[166] No State is on record as having denied the applicability of existing norms of international law to the emerging context of cyberspace. It is also noteworthy that it was unanimously agreed by the Experts who drafted the Tallinn Manual that the *jus ad bellum* and the *jus in bello* apply to cyber operations. See also US Department of Defence, *Cyberspace Policy Report* (2011) 9: "International legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e. sea, air, land, and space), also apply to the cyberspace domain."
[167] CD Guymon (ed), *Digest of US Practice in International Law* (2012) 594; Roscini (n 4) 21.

the United States adopted its *International Strategy for Cyberspace* in which it took the position that:

> 'The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behaviour – in times of peace and conflict – also apply in cyberspace'.[168]

Apart from the United States, other nations have also expressly acknowledged that certain provisions of current treaty law apply to cyber operations conducted by States.[169] For instance, as early as 2000 the Russian Government had already adopted conceptual views relating to the international legal norms, particularly from the UN charter, that should guide the conduct of Russian forces when undertaking operations in cyberspace.[170] Likewise, the Dutch Government has affirmed that certain aspects of treaty law extend to the cyber realm.[171]

Official pronouncements by States may also provide a useful indicator of the stance adopted by the relevant State as regards a particular issue.[172] Even more convincing as evidence of State practice are official comments or observations presented to organs of the United Nations.[173] In this regard, the views formally submitted by States (on the issue of information security) to the UN Secretary-General also demonstrate that there is a significant level of acceptance of the application of treaty norms in the cyber context. Notable examples of States that have taken this view include: the United Kingdom,[174] Australia,[175] and Cuba.[176]

3.1.2 Affirmative Practice of International Organizations

The International Committee of the Red Cross (ICRC) has consistently maintained that the treaty law of armed conflict (particularly, the Geneva Conventions and the Hague Conventions) governs the conduct of belligerents, regardless of the type of weapons or the technology used.[177] This position has remained essentially unchanged in the case of cyber means and methods of

---

[168] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011).
[169] Roscini (n 4) 21-22.
[170] Russian Federation (n 32) 6.
[171] Dutch Government Response to the AIV/CAVV Report on Cyber Warfare, pp 5-6.
[172] AM Weisburd, 'The International Court of Justice and the Concept of State Practice' (2009) 31(2) *University of Pennsylvania Journal of International Law* 295, 303.
[173] *Nuclear Weapons* (n 55) 254-55; I Brownlie, *Principles of Public International Law* (2008) 6-7.
[174] UN Doc/A/65/154, 20 July 2010, p 15.
[175] UN Doc/A/66/152, 15 July 2011, p. 6.
[176] UN Doc/A/57/166/Add.1, 29 August 2002, p. 3.
[177] Sandoz et al (n 77) para 55.

warfare; it holds that cyber technology, like any other kinetic weapon, is governed by international humanitarian law. This view was articulated in a 2011 analytical report, where the ICRC explained that:

> 'means and methods of warfare which resort to cyber technology are subject to IHL [international humanitarian law] just as any new weapon or delivery system has been so far when used in an armed conflict by or on behalf of a party to such conflict. If a cyber-operation is used against an enemy in an armed conflict in order to cause damage, for example by manipulation of an air traffic control system that results in the crash of a civilian aircraft, it can hardly be disputed that such an attack is in fact a method of warfare and is subject to prohibitions under IHL'.[178]

Similarly, the UN General Assembly has adopted a report which supports the view that current treaty law applies in the context of, and forms the basis for, regulating cyber operations.[179] Indeed the Report of the third[180] Group of Governmental Experts (GGE) established by the UN General Assembly made the key point that international law, and in particular the Charter of the United Nations, is not only applicable but is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible information and communications technologies environment.[181] The fact that this GGE Report was adopted by the UN General Assembly is significant because it reflects the extensive acceptance of this view among member States of the United Nations.

The European Union is also another international organization that has recognized the applicability of existing international treaty law to cyber operations conducted by States.[182] More specifically, the 2013 Cyber Strategy of the European Union emphasizes the critical role played by international treaty law in general, and more specifically the UN Charter, in providing the basis for engagement in cyberspace.[183] As a regional body, the views articulated in the above strategy can safely be taken as a reflection of the views of the constitutive nations that form the

---

[178] ICRC (n 163) 36-37.
[179] Roscini (n 4) 22.
[180] It is useful to note that the first Group was established in 2004, but it did not submit a report to the UN General Assembly. The second Group was established in 2009, and it produced its report in 2010 (UN Doc/A/65/201, 30 July 2010). For its part, the third Group was established in 2012, and it issued its report in 2013 (UN Doc/A/68/98, 24 June 2013).
[181] UN Doc/A/68/98, 24 June 2013, p 8.
[182] Roscini (n 4) 22.
[183] EU, *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace* (2013) 15-16.

European Union. The practice of certain States that are members of the European Union clearly support this view.[184]

3.2 Legal Basis in Customary International Law

Legal obligations arising from treaty law are limited in their effect because they bind only those States that have consented to be so bound.[185] However, in some instances, the binding effect of some treaty norms is enhanced because the norms have attained customary status[186] or reflect a general principle of law.[187] Customary international law, defined as "evidence of a general practice accepted as law",[188] binds all States, with the possible exception of persistent objectors.[189] Customary norms are evidenced by two elements which indicate the formation of a rule of customary international law, namely State practice and *opinio juris*.[190]

3.2.1 State Practice and *Opinio Juris*

The element of practice in the formation of customary international law requires that the relevant conduct, i.e the observation of a certain rule, has been complied with by a representative number of States.[191] It is useful to note that this element is qualitative in nature, placing less emphasis on the number of States and more on the relationship that exists between the States and the norm at issue.[192] Evidence of practice is not limited to the conduct of States, but may be derived from the conduct of other subjects of international law, including international organizations.[193] The following are indicative material sources of the practice of a State:

> 'diplomatic correspondence, policy statements, press releases, the opinions of legal advisors, official manuals on legal questions, e.g. manuals of military law, executive decisions and

---

[184] Notable examples of European States that have endorsed the applicability of the existing rules of international law to the new and developing phenomenon of cyber operations include Denmark, France, Germany, and Italy.
[185] Shaw (n 149) 839.
[186] *Gabčikovo-Nagymaros Project (Hungary v Slovakia)*, 1997 ICJ Reports 7, 38.
[187] Article 38(1)(b) and (c) ICJ Statute; *Land, Island and Maritime Frontier Dispute (El Salvador v Honduras; Nicaragua intervening)*, 1992 ICJ Reports 350, 386-87.
[188] Article 38(1)(c) ICJ Statute.
[189] T Treves, 'Customary International Law' in *Max Planck Encyclopedia of Public International Law* (2012) 940; R Kolb & R Hyde, *An Introduction to the International Law of Armed Conflicts* (2008) 52; M Fitzmaurice & O Elias, *Contemporary Issues in the Law of Treaties* (2005).
[190] *Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v Belgium)*, 2002 ICJ Report 3, 23-24; A Aust, *Modern Treaty Law and Practice* (2013); A Cassese, *International Law* (2005) 156.
[191] *North Sea Continental Shelf*, Judgment of 20 February 1969, ICJ Reports 1969, para 77.
[192] *Nuclear Weapons*, para 64.
[193] *Ahmadou Sadio Diallo (Guinea v Democratic Republic of Congo)*, 46 ILM 712, 732; *Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada v United States)*, 1984 ICJ Reports 246; Roscini, Cyber Operations and the Use of Force, 25.

> practices, orders to naval forces etc., comments by governments produced by International Law Commission, State legislation, international and national judicial decisions, recitals in treaties and other international instruments, a pattern of treaties in the same form, the practice of international organs, and resolutions relating to legal questions in the United Nations General Assembly'.[194]

The element of *opinio juris* denotes the subjective aspect and it requires the relevant conduct of States or other subjects of international law (practice) to occur in "such a way as to show a general recognition that a rule of law or legal obligation is involved."[195] Absent evidence as to a belief in the presence of a prescriptive rule that establishes the basis for observing a particular practice, it may be sufficient to rely on the imperative force of necessity as the basis for that conduct.[196] The material sources that are relied on to demonstrate practice are also evidentiary sources of *opinio juris*; in fact, the International Law Association (ILA) has observed that it is often difficult or even "impossible to disentangle the two elements."[197] Therefore, official statements of States, including national policy statements[198] and manuals of military law, and other representative pronouncements may indicate *opinio juris*.[199]

With specific regard to the question of the regulation of cyber operations, customary international law provides a crucial legal basis for constraining State conduct within the limits of the law. In particular, as a general rule, customary norms applicable to kinetic operations also apply, in more or less the same way, to "cyber operations amounting to a use of force or acts of hostilities."[200] This general rule derives from the logic that norms of a customary nature, especially regarding the use of weapons and technology, cannot be expected to develop selectively.[201] Instead, the better view is that customary norms should develop in a manner that is general enough to govern any type of weapon or technology.[202] Otherwise, there will be a

---

[194] Brownlie (n 173) 6.
[195] *North Sea Continental Shelf*, para 74; *Nicaragua*, para 183; J-M Henckaerts & L Doswald-Beck, *Customary International Humanitarian Law* (2005) Vol I, xxxii.
[196] *Prosecutor v Kupreskic*, Case No IT-95-16-T, Trial Chamber Judgment, 14 January 2000, para 527; A Cassese, *International Law* (2003) 156.
[197] ILA, Statement of Principles Applicable to the Formation of General Customary International Law, in International Law Association (ILA), Report of the Sixty-Ninth Conference (2000) 718.
[198] MC Waxman, 'Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions' (2013) 89 *International Law Studies* 116.
[199] HHG Post, 'Some Curiosities in the Sources of the Law of Armed Conflict Conceived in a General International Law Perspective' in LANM Barnhoorn & KC Wellen (eds), *Diversity in Secondary Rules and the Unity of International Law* (1995) 99-100.
[200] Roscini (n 4) 25.
[201] Y Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' (2013) 89 *International Law Studies* 280.
[202] *Nuclear Weapons* (n 55) para 39.

recurrent duplicity of effort in trying to identify the customary norms relevant to "every concrete weapon employed in armed attack."[203]

An examination of the practice of States and the *opinio juris* indicates a general acceptance of the fact that cyber operations constituting a use of force or the conduct of hostilities are subject to the respective customary norms of the *jus ad bellum* and the *jus in bello*.[204] In light of the scarcity of State cyber practice (drawn from cyber incidents that can clearly be attributed to States),[205] other evidentiary sources such as manuals of military law and operational conduct become instructive. While the actual operational conduct of a State would arguably provide more conclusive evidence as to its practice,[206] national military manuals have the additional advantage of providing an indication of what the State has declared as well as its attitude regarding the existence of a legal rule.[207] It has also been observed that practice is essentially about what States clearly declare as their intent, and not necessarily what they do.[208]

Military manuals are particularly relevant since they constitute both State practice and evidence of *opinio juris*.[209] The utility of such manuals is enhanced in the case of cyber operations because most States that have been linked to recent cyber incidents have either denied involvement or dissimulated their roles,[210] thus making it very difficult to ascertain State cyber practice.[211] This special role of military manuals has been recognized in international jurisprudence; in particular, the Appeals Chamber of the ICTY has held that where information on the actual conduct of States is either unavailable or is being withheld by the parties, recourse can be made to military manuals.[212] Considering that State cyber practice is sparse, an examination of military manuals can offer vital insight into the extent of practice and *opinio juris*.

---

[203] Dinstein (n 201) 280.
[204] HM Government, (n 31) 29-30; Chairman of the Joint Chiefs of Staff, *The Military Strategy for Cyberspace Operations* (2006); E Tikk et al, *Cyber Attacks against Georgia: Legal Lessons Identified* (2008) 5.
[205] Tallinn Manual (n 8) 5; Shackleford (n 20) 219.
[206] *Continental Shelf (Libyan Arab Jamahiriya v Malta)*, 1985 ICJ Reports 13.
[207] C Garraway, 'The Use and Abuse of Military Manuals' (2004) 7 *Yearbook of International Humanitarian Law* 431; Y Dinstein, 'The Creation of Customary International Law' (2006) 322 *Recueil des cours* 272.
[208] C Gray, *International Law and the Use of Force* (2008) 418.
[209] AJK Bailes & A Wetter, 'Security Strategies' in *Max Planck Encyclopedia of Public International Law* (2012) Vol IX, 87.
[210] Schreier (n 5) 113; Brenner (n 18) 402.
[211] *Report of the Independent Fact-Finding Mission on the Conflict in Georgia* (2009) Vol II, 217-19.
[212] *Prosecutor v Tadic*, Case No IT-94-1, Decision of the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para 99.

An example of a military manual that contemplates the regulation of cyber warfare is the United States Commander's Handbook which affirms that the long-established rules that apply to kinetic naval operations also extend to cyber operations.[213] Similarly, the British Manual states that cyber operations are subject to certain key rules of the law of armed conflict.[214] Other States that have a special interest in cyber warfare, e.g., Israel and China, are in the process of updating their military manuals to effectively address cyber operations.[215]

Apart from military manuals, other official pronouncements of States such as policy statements intended to guide operational conduct are also useful evidentiary sources of practice and *opinio juris*.[216] This view is supported by the jurisprudence of the ICJ, which has held that the conduct of any organ of a State, including the conduct of State officials, "must be regarded as an act of that State."[217] An illustrative example can be found in the *International Strategy for Cyberspace* of the United States, which makes clear that the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete."[218]

3.2.2 An Emerging Relaxed Approach

The above discussion on practice and *opinio juris* raises the question as to whether it can be said that cyber-specific customary norms may be in the process of developing. The predominant view is that the dual requirements of State practice and *opinio juris* must be satisfied for the customary status of a particular norm to be established.[219] However, a novel view is emerging that the determination of new rules of custom can be carried out according to less strict criteria than were originally envisaged.[220] This suggests that the strict approach is giving way to a more relaxed approach.

---

[213] *The Commander's Handbook on the Law of Naval Operations* (2007) 8-17.
[214] UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (2004) 118.
[215] L Zhang, 'A Chinese Perspective on Cyber War' (2012) 94 *International Review of the Red Cross* 805; E Benari, 'Israel to Establish Cyber Warfare Administration', Israel National News, 13 January 2012.
[216] M Bothe, 'Comments' in HHG Post (ed), *International Economic Law and Armed Conflict* (1994) 34.
[217] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*, Advisory Opinion, 1999 ICJ Reports 62, 87.
[218] White House (n 168) 9.
[219] Roscini, Cyber Operations and the Use of Force, 30.
[220] *North Sea Continental Shelf*, para 74; R Heinsch, 'Methodology of Law-Making: Customary Law and New Military Technologies' in D Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (2013) 36.

Two key points need to be highlighted in order to illustrate this emerging relaxed approach to the formation of international custom.[221] First, while evidence of practice was initially exclusively derived from actions of States, the current view admits of verbal acts as evidence of the acceptance of certain norms.[222] Indeed, the ICRC Study on Customary International Humanitarian Law includes opinions of official legal advisors, including their verbal statements, as evidence of State practice.[223] Verbal acts have also been expressly considered to be sufficient evidence of State practice by the International Law Association[224] and certain influential legal commentators.[225] Also, the strict requirement that State practice must be "extensive and virtually uniform" has been relaxed such that the practice of few specially affected States would suffice to establish that a "general practice accepted as law" has crystallized.[226] This is supported by the ILA Statement of Principles which emphasizes that the requisite State practice is more of a qualitative nature: "if all major interests ('specially affected States") are represented, it is not essential for a majority of States to have participated".[227]

The second point that shows the emergence of a relaxed approach to the formation of customary international law is the decisive role that *opinio juris* has come to play in recent times.[228] Originally, State practice was considered the objective basis on which to establish the presence of a customary norm, while *opinio juris* was deemed subjective in the sense that it supplemented a conclusion largely premised on practice.[229] However, in new and emerging contexts (such as the use of new technologies) where State practice is either sparse or difficult to

---

[221] *Prosecutor v Kupreskic* (n 81) para 527; *Nicaragua* (n 51) para 218.
[222] Michael Wood, 'State Practice' in *Max Planck Encyclopedia of Public International Law* (2012) Vol IX, 510; JB Bellinger & WJ Haynes, 'A US Government Response to the International Committee of the Red Cross Study on Customary International Humanitarian Law' (2007) 89 *International Review of the Red Cross* 445.
[223] Guymon (n 167) 593.
[224] Statement of Principles Applicable to the Formation of General Customary International Law, in International Law Association (ILA), Report of the Sixty-Ninth Conference (2000) 725.
[225] Gray (n 208) 418; Brownlie (n 173) 6-7.
[226] AT Guzman, 'Saving Customary International Law' (2005-2006) 27 *Michigan Journal of International Law* 151.
[227] ILA, *Statement of Principles*, 737.
[228] G Bartolini, 'Armed Forces and the International Court of Justice: The Relevance of International Humanitarian Law and Human Rights Law to the Conduct of Military Operations' in M Odello & F Seatzu (ed), *Armed Forces and International Jurisdictions* (2013) 51, 61-62.
[229] Gardiner (n 139) 225.

determine, *opinio juris* becomes more determinative.[230] This position is supported by international jurisprudence[231] and international legal doctrine.[232]

What then does the emergence of a relaxed approach to the formation of customary international law hold for cyber-specific norms? The drafters of the Tallinn Manual state that due to the scarcity of State cyber practice and publicly available expressions of *opinio juris*, "it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists."[233] The cautious tenor of the above statement is understandable because the Tallinn Manual was keen to avert any criticism that it was stipulating unsupported norms.[234]

However, the cautious stance taken by the Tallinn Manual does not exclude the possibility that "customary international law rules specific to cyber warfare might be in the process of forming and eventually ripening."[235] This view is persuasive because if it is accepted that current treaty and customary norms extend to the cyber context then it follows that cyber-specific norms are in the process of developing, at least, in respect of certain aspects relating to the conduct of cyber operations by States.[236] Otherwise, given the complete absence of specific treaty law provisions governing cyber operations, the cyber conduct of States would be left unregulated.

3.3 Applicability of Current Norms to Cyber Operations

The preceding discussion has shown that cyber operations that are conducted either in the context of the use of force or an armed conflict are subject to both customary and treaty law. But what is less clear is how and to what extent the treaty law provisions and customary law specific to kinetic operations can be applied in the cyber context. To answer this question, it is necessary to first examine the norms that apply in kinetic operations and identify how these norms can be adapted to the cyber context, with special focus on the unique aspects of cyberspace.

---

[230] R Kolb, 'Selected Problems in the Theory of Customary International Law' (2003) 50(2) *Netherlands International Law Review* 119, 129; Heinsch, (n 220) 25-26.
[231] *Kupreskic* (n 81) para 527; *Nicaragua* (n 51) 218.
[232] MP Scharf, 'Seizing the "Grotian Moment": Accelerated Formation of Customary International Law in Times of Fundamental Change' (2010) 43 *Cornell Journal of International Law* 439, 468; T Meron, 'The Martens Clause, Principles of Humanity, and Dictates of Public Conscience' (2000) 94(1) *American Journal of International Law* 78, 88.
[233] Tallinn Manual (n 8) 5.
[234] Ibid at 5: "[A]ny claim that every assertion in the Manual represents an incontrovertible restatement of international law would be an exaggeration."
[235] Roscini (n 4) 25.
[236] Roscini (n 4) 19; Schmitt (n 41) 921.

This is the approach that was adopted by the drafters of the Tallinn Manual who sought to identify and elaborate how the existing international law applies to cyber operations that rise to the threshold of a use of force or acts of hostilities. This exercise, which was conducted by renowned experts serving in their personal capacities,[237] resulted in the adoption of 95 Rules governing cyber operations. In addition, each of the Rules is accompanied by an extensive Commentary that explains the legal basis of the Rule and outlines any points of contention, whether among the drafters or in the legal doctrine.[238]

4. CONCLUSION

This Chapter has examined the background of the Tallinn Manual, highlighting its origins from the NATO collective self-defence documents to its eventual conclusion as a Manual. The relevant discussion in the Chapter has also outlined the legal basis for extending the current law to cyber operations, demonstrating that this view has a legal basis in treaty and customary international law. Accordingly, it finds that the position taken at the outset by the drafters of the Tallinn Manual is valid and is supported both in law and in practice. The main point highlighted in this Chapter is the need for progressive development of international law because the Manual is not an attempt to present a comprehensive account of the applicable rules.

[237] Tallinn Manual (n 8) 11.
[238] Ibid at 6-7.

Chapter III

A CRITICAL APPRAISAL OF THE CONTRIBUTION OF THE TALLINN MANUAL TO THE CLARIFICATION OF INTERNATIONAL LAW RELATIVE TO CYBER OPERATIONS

1. INTRODUCTION

The potentially adverse consequences of cyber operations that can disrupt and destroy critical aspects of modern societies highlight the crucial need for a coherent legal framework that governs the use of cyber technology in international relations.[239] The Tallinn Manual comes as an attempt to fill the gap of legal regulation of cyber operations in international law, an area that was not specifically codified by traditional international law.[240] In fact, one of the explicitly stated objects of the Tallinn Manual is to supply "some degree of clarity to the complex legal issues surrounding cyber operations, with particular attention [being] paid to those involving the *jus ad bellum* and the *jus in bello*."[241]

The Tallinn Manual sets forth specific Rules that establish a framework for the legal regulation of cyber operations and each of these are accompanied by a Commentary setting out the Rule's legal basis and explaining its interpretation vis-à-vis current norms. The present chapter reviews the extent to which selected Rules of the Tallinn Manual have contributed towards clarifying some of the complex issues of international law surrounding cyber operations.

PART I JUS AD BELLUM

2. A CRITIQUE OF *JUS AD BELLUM* RULES IN THE TALLINN MANUAL

This section analyzes selected *jus ad bellum* Rules by critically discussing their legal basis then assessing their practical utility as regards the novel phenomenon of cyber attacks. The analysis will explore important questions regarding whether a cyber operation may constitute a use of force giving rise to the right of self-defence, within the specific meaning of the UN Charter and customary international law.

---

[239] D Allan & C Brown, 'The *Mavi Marmara* at the Frontlines of Web 2.0' (2010) 40 *Journal of Palestinian Studies* 63.
[240] WJ Lynn, 'Defending a New Domain: The Pentagon's Cyber Strategy' (2010) September/October 97, 101.
[241] Tallinn Manual (n 8) 3-4.

2.1 Prohibition of Threat or Use of Force

The Tallinn Manual explicitly prohibits the use of cyberspace or the employment of cyber technology in a manner that amounts to a threat or use of force against a State. In particular, Rule 10 stipulates that a "cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[242] This rule is based on both treaty and customary international law.[243]

Rule 10 adopts an expansive approach that recognizes that the prohibition of threats or uses of force contrary to the UN Charter applies to States as well as to non-State actors. This is apparent in the commentary to this Rule, which explains that on the basis of customary law this prohibition extends to non-State actors, subject to a finding of attribution of their unlawful acts to a State.[244] The commentary to Rule 10 also explains, with reference to the preparatory documents of the UN Charter, that the phrase threats or uses of force "in any other manner inconsistent with the Purposes of the United Nations" establishes a presumption of illegality of any conduct inconsistent with the UN Charter, even if it is not directed against the territorial integrity or political independence of a State.[245]

An important issue addressed in Rule 10 is that cyber operations not amounting to a use of force are not necessarily lawful under international law. This is important because it prevents any gap in the legal regulation of cyber operations. By holding that cyber incidents not rising to a use of force may still constitute a violation of the prohibition on intervention, the Rule 10 effectively ensures that even where there is doubt there will be little room to avoid liability.[246]

However, the above explanation in the commentary to Rule 10 is not entirely unproblematic.[247] For one, the UN Charter outlines many purposes and there is the possibility that these may clash; for example, support for the right to self-determination may clash with imperatives of maintaining international peace. Hence, the prohibition expressed in Rule 10 is

---

[242] Tallinn Manual (n 8) 42-43.
[243] *Nicaragua* (n 51) paras 188-90.
[244] Tallinn Manual (n 8) Rule 10, at para 4.
[245] Ibid at para 2.
[246] Tsagourias (n 62) 21.
[247] JC Woltag, Computer Network Operations below the Level of Armed Force' (2011) ESIL Conference Paper no 1/2011, 16-17.

less clear insofar as it does not elaborate whether the use of the phrase "in any manner inconsistent with the purposes of the United Nations" was intended to be an inclusive basis for outlawing invasive cyber operations.[248]

Another challenging issue is defining the threshold of intervention. In answering this question, the Tallinn Manual relies on the *Nicaragua* judgment where the ICJ stated that the determinative element is coercion: "interference pure and simple is not intervention … intervention is wrongful when it uses methods of coercion".[249] The range and nature of cyber operations make it difficult to determine with certainty whether a particular cyber incident constitutes an intervention or whether it constitutes a use of force. This point is acknowledged by the Tallinn Manual which uses the example of the Stuxnet attack and the cracking of passwords to illustrate the scope of intervention. In the final analysis it emphasizes the point that the decisive test is that of coercion.[250]

2.2 Definition of Threat of Force

Rule 12 of the Tallinn Manual states that: "A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force."[251] This rule has its legal basis in Article 2(4) of the UN Charter as elaborated by the ICJ in its *Nuclear Weapons* Advisory Opinion, where the Court distinguished between lawful and unlawful threats of force:

> '[t]he notions of "threat" and "use" of force under Article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal—for whatever reason—the threat to use such force will likewise be illegal'.[252]

Consequently, the ICJ explained that if a specific threat of force "is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the [UN] Charter."[253] Hence, Rule 12 of the Tallinn Manual reflects the generally accepted position that a threatened cyber operation would be lawful if the threatened action would itself be consistent

[248] Tallinn Manual (n 8) Rule 10, para 7.
[249] *Nicaragua* (n 55) para 205.
[250] Tallinn Manual (n 8) Rule 10 at para 10.
[251] Ibid at 52.
[252] *Nuclear Weapons* (n 55) para 47.
[253] Ibid.

with the UN Charter in the event that it is carried out.[254] More specifically, a threatened cyber operation would be lawful if the threatened action, if carried out, would constitute a legitimate exercise of the right of self-defence or an action implementing a UN Security Council resolution pursuant to Chapter VII of the UN Charter.

While the Tallinn Manual's distinction of lawful from unlawful cyber threats of force accords with current international legal doctrine, it nevertheless lends itself to some ambiguity. For one, it is unclear whether a cyber use of force, say for humanitarian intervention, will be lawful if the force used exceeds what is necessary in the short-term but may be justifiable in the longer term.[255] Another ambiguity lies in the fact that it is often difficult to assess the lawfulness of a use of force, including cyber force, if certain requisite elements (i.e, necessity, proportionality, imminence and immediacy) cannot objectively and conclusively be evaluated at the time of the threat.[256]

Rule 12 of the Tallinn Manual, as elaborated in its commentary, takes the view that the aggressive acquisition by a State of cyber capabilities is not in itself an unlawful threat to use force.[257] Rather it is the announcement that the capabilities will be used to conduct cyber operations against another State.[258] This view is not convincing because it fails to take account of several important factors, including the geopolitical alliances that the aggressor State may have. The presumption that mere acquisition will not constitute a threat of force is also not supported by State practice, as illustrated by the 1967 Cuban missile crisis.[259] Accordingly, the rigid and categorical position adopted in the Tallinn Manual is imprudent because it is inadequate in theory and unsupported in practice.

2.3 State Responsibility and Attribution

Rule 10 of the Tallinn Manual explicitly prohibits the threat or use of cyber force against the territorial integrity or political independence of any State. It also proscribes cyber operations that are inconsistent with the purposes of the United Nations. Accordingly, any cyber action

---

[254] *Nuclear Weapons* (n 55) para 47; L Henkin, 'The Reports of the Death of Article 2(4) Are Greatly Exaggerated' (1971) 65 *American Journal of International Law* 544.
[255] *Oil Platforms* (n 50) paras 73-74; *Nicaragua* (n 51) para 176.
[256] *Nuclear Weapons* (n 55) para 48; Tsagourias (n 62) 28.
[257] Tallinn Manual, Rule 12, paras 4-6.
[258] Ibid at para 4.
[259] A Chayes, *The Cuban Missile Crisis: International Crises and the Role of Law* (1974) 103-104.

amounting to a threat or use of force will become an internationally wrongful act, with the consequence that legal responsibility will attach to its author(s). This calls into focus the special rules on legal responsibility for internationally wrongful acts, which have been articulated by the International Law Commission (ILC) in its Articles on State Responsibility.[260] Moreover, the rules applicable to attribution become relevant in cases where the authors of an internationally unlawful cyber operation are not agents of the State, but are nonetheless linked to the State.

Rule 6 of the Tallinn Manual provides that a State will bear "international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[261] This Rule is based on customary law as articulated in the ILC Articles on State Responsibility.[262] Of particular interest is the Commentary to Rule 6 which elaborates the standards for the attribution of international responsibility. It must be borne in mind that there are primarily three different classes of actors that are typically involved in the conduct of cyber operations.[263] First, there are "organs of the State" which include both civilian and military State agents,[264] provided they act in accordance with internal legislation.[265] Secondly, there are civilian militias which consist in more or less organized individuals without the status of State agents under the internal law of the relevant State, but who may act under the direction of that State.[266] Thirdly, there are those independent citizen hackers who operate autonomously or in concert with other hackers.

The rules for attribution in the case of a State organ are fairly straight forward and well settled; that is, the conduct of any State organ is considered to be that of the State, regardless of its function or place in governmental hierarchy.[267] This is the position taken by the Tallinn

---

[260] International Law Commission, Responsibility of States for Internationally Wrongful Acts, UNGA Res 56/83 annex, UN Doc A/RES/56/83 (12 December 2001).
[261] Tallinn Manual (n 8) 29.
[262] Articles 1 and 2, ILC Articles on State Responsibility.
[263] LL Muir, 'The Case Against an International Cyber Warfare Convention' (2011) 2 *Wake Forest Law Review* 5, 8.
[264] There is an increasing number of States that have specialized cyber units within their military or civilian security agencies. Examples include: Estonia (Cyber Unit of the Estonian Defence League); the United States (67th Network Warfare Wing); North Korea (Unit 121); Syria (Syrian Electronic Army); Colombia (Armed Forces Joint Cyber Command). See Roscini (n 4) 10.
[265] Article 4(2), ILC Articles on State Responsibility.
[266] M Milanovic, 'State Responsibility for the Acts of Non-State Actors: A Comment on Griebel and Plücken' (2009) 22 *Leiden Journal of International Law* 315; SD Watts, 'Combatant Status and Computer Network Attack' (2010) 50 *Virginia Journal of International Law* 405, 411.
[267] *Nicaragua* (n 51) paras 110, 393; *Reservations to the Genocide Convention*, 1951 ICJ 15, paras 392-93; Article 4(1), ILC Articles on State Responsibility.

Manual, which recognizes that cyber attacks may be committed by State organs[268] or persons or entities that, while not organs of that State, are specifically empowered by its domestic law to exercise governmental authority.[269] But in the case of completely autonomous or semi-dependent groups of hackers, the rules are less clear.[270] The commentary to Rule 6 elaborates that the acts of such individuals or groups will be attributable to the sponsoring State if they were in fact carried out under the instruction, direction or control of that State, a view that restates article 8 of the Articles of State Responsibility.[271]

However, the threshold of control at which acts of non-State entities can engage the international responsibility of a State is contentious. There is considerable disagreement as to whether the requisite degree of control should be "overall control" in all cases of acts of non-State actors or whether it should be "effective control" in the case of citizen hackers and unorganized cyber volunteers and "overall control" in the case of organized groups.[272] The effective control test was articulated by the ICJ in *Nicaragua*[273] (and later clarified in the *Genocide* judgment)[274] where it was explained that, for responsibility to attach, it must be proved that the State had effective control of an operation which resulted in internationally wrongful acts or that the State's instructions were given in respect of each unlawful action. The *Genocide* judgment specifies that the threshold of effective control requires a State to have exercised control over specific acts and "not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations."[275]

By contrast, the "overall control" test which was adopted in *Tadić* is a less stringent standard; it only requires evidence that a State had a role in facilitating, organizing, coordinating or planning the actions of a non-State entity, "regardless of any specific instructions by the controlling State concerning the commission of each of those acts".[276] Moreover, unlike the effective control standard, the overall control test focuses not so much on "control over the act,

---

[268] Tallinn Manual (n 8) Rule 6, paras 6-7.
[269] Article 4(1) ILC Articles on State Responsibility; Tallinn Manual (n 8) Rule 6, para 8.
[270] A Klimburg (ed), *National Cyber Security Framework Manual* (2012) 49-50; JA Ophardt, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 *Duke Law and Technology Review* para 12-18.
[271] Tallinn Manual, Rule 6, para 9; Article 8, ILC Articles on State Responsibility.
[272] Tallinn Manual, Rule 6, para 10; Tsagourias, 32.
[273] *Nicaragua* judgment, para 115.
[274] *Genocide* judgment, paras 399-401.
[275] *Genocide* judgment, para 400.
[276] *Tadić*, Appeals Chamber judgment, para 137.

but over the actor, an organized and hierarchically structured group, at a general level."[277] According to the present author, the overall control test appears more appropriate for attributing acts of organized groups, while the effective control test would be more fitting in the case of individuals and unorganized groups.[278] The view of the present author is convincing in light of the inherent anonymity of cyber operations and the difficulty of identifying the perpetrators.[279]

Surprisingly, the Tallinn Manual does not state a definite position regarding which standard of attribution is the more appropriate test for determining whether State responsibility attaches.[280] Instead, it merely explains in the commentary to Rule 6 that even if the lower "overall control" test were to be adopted in respect of cyber operations, it would not apply to individuals or unorganized groups.[281] This implicitly supports the adoption of the stringent effective control test in the case of individuals or groups that are not militarily organized and the adoption of the less restrictive overall control standard in the case of organized groups. This notwithstanding, the Tallinn Manual could have been more forthright in order to provide a ruling on the current position in the law of State responsibility.

Rule 7 of the Tallinn Manual provides that: "The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indicator that the State in question is associated with the operation."[282] This Rule supports the view that the standards for attribution may be adopted in appropriate circumstances because it does not exclude that cyber operations launched from State cyber infrastructure can be the basis for attaching international responsibility. Hence, going by the standards of cognizable "unwillingness" or "toleration" by action or selective inaction, unlawful cyber operations can be attributed to a State if there is sufficient evidence to indicate that "the state tolerates such attacks to be launched from its

[277] Milanovic (n 266) 317.
[278] SJ Shackleford & RB Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 *Georgetown Journal of International Law* 971, 987-988; Tsagourias (n 62) 240-41.
[279] DJ Ryan et al, 'International Cyberlaw: A Normative Approach' (2011) 42 *Georgetown Journal of International Law* 1179, 1187.
[280] Tallinn Manual (n 8) Rule 6, para 10.
[281] Ibid.
[282] Ibid.

infrastructure or willingly fails to safeguard its governmental cyber infrastructure."[283] This view is supported in international law and practice.[284]

Despite the fact that the flexible standards of "unwillingness" or "toleration" have been upheld in international practice[285] and endorsed by influential legal writers,[286] the commentary to Rule 7 does not expressly state that this is the correct interpretation, more so in the cyber context.[287] This omission deprives the Tallinn Manual a vital opportunity to encourage States to be vigilant so as to prevent the use of their infrastructure in furtherance of internationally unlawful ends. In light of the UN Charter's provisions and international case law, there is an obligation on all States, in the exercise of sovereignty, not to allow their territory to be used as a launch-pad of unlawful acts.[288] Such conduct may entail international responsibility of the offending State.

Indeed, it is a rule of customary international law that States have a fundamental duty not to "allow knowingly" their territories to be used in a manner that is "contrary to the rights of other States".[289] The effect of this customary rule is to impose a specific obligation on States to take appropriate steps to ensure their territorial integrity so as to protect the rights of others.[290] It is therefore the opinion of the present author that the Tallinn Manual advocates too flexible a standard for the attribution of cyber attacks launched from governmental infrastructure and it is likely to facilitate rather than check unlawful acts.

The commentary to Rule 7 also states that "[i]n and of itself, the Rule does not serve as a legal basis for taking any action against the State involved or otherwise holding it responsible for the acts in question."[291] This explanation is problematic because it fails to recognize the key role that attribution has in determining the bearer of responsibility for unlawful conduct and identifying the legitimate "target of counter force."[292] But it is possible to appreciate the logic of

---

[283] Tsagourias (n 62) 233.
[284] *Congo v Uganda*, paras 147, 301; Simma et al, Commentary, 1418.
[285] *Congo v Uganda*, paras 147, 301; *Congo v Uganda*, Separate Opinions of Judge Kooijimans, paras 26-30 and Judge Simma, paras 7-12.
[286] Simma et al, Commentary, 1418; Tsagourias (n 62) 240-1.
[287] Tallinn Manual (n 8) Rule 7, para 3.
[288] *Trail Smelter (United States v Canada)*, 3 RIAA 1905, 1965 (1941); See also *Corfu Channel (United Kingdom v Albania)*, 1949 ICJ 4, 22.
[289] *Corfu Channel (United Kingdom v Albania)*, 1949 ICJ 4, 22.
[290] *US Diplomatic and Consular Staff in Tehran (US v Iran)*, 1980 ICJ 3, 67-68.
[291] Tallinn Manual (n 8) Rule 7, para 3.
[292] Tsagourias (n 62) 32.

the above statement when it is considered in context. Certain States, particularly the less developed and technologically unsophisticated ones, may be genuinely be unable to prevent non-State entities from taking control of its cyber infrastructure and using it to conduct unlawful acts. It follows that such States would be unfairly prejudiced by a legal standard that attaches responsibility merely because of a failure to prevent, regardless of the circumstances of the case. Hence, the correct standard should take account of the specific facts on a case-by-case basis.

2.4 Self-Defence against Armed Attack

Rule 13 of the Tallinn Manual provides that: "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects." Part of this rule is a restatement of the principle enunciated in Article 51 of the UN Charter which provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." This provision and particularly the use of the words "inherent right" reflect the customary right of self-defence.[293]

Rule 13 thus confirms that the right to employ force in self-defence applies to armed cyber attacks that are of such a scale and whose adverse effects are analogous to those that ordinarily attend kinetic armed attacks.[294] However, it does not provide any further explanation as to which uses of force can trigger the right of self-defence.[295] In fact, the commentary to Rule 13 observes that the ICJ did not clarify how the gravity of an attack can be measured,[296] but it did not attempt to provide any useful guidance that could remedy that omission.[297] Nonetheless, the fact that Rule 13 implies that the requisite scale and effects are those analogous to kinetic attacks suggests that a cyber operation would only amount to an armed attack if it results in death, injury or

[293] See the *Caroline* incident reprinted in RY Jennings, 'The Caroline and McLeod Cases' (1983) *American Journal of International Law* 82, 89.
[294] Tallinn Manual (n 8) Rule 13, para 3-6; *Nicaragua*, paras 191, 193-95, 211, 237; MC Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 *Yale Journal of International Law* 437.
[295] Tsagourias (n 62) 30.
[296] *Nicaragua*, para 195; *Oil Platforms*, paras 46-77; Tallinn Manual (n 8) Rule 13, at para 7.
[297] Tsagourias (n 62) 30.

destruction.[298] It would be sufficient for a finding of an armed attack if these conditions are satisfied disjunctively.

2.4.1 Grave and Less Grave Uses of Cyber Force

There was unanimous consensus amongst the International Group of Experts that some cyber operations may, independently, be sufficiently grave as to constitute an "armed attack" within the meaning of Article 51 of the UN Charter.[299] This position finds support in the *Nuclear Weapons* Advisory Opinion where the ICJ stated that the choice of means of attack, whether kinetic or non-kinetic, has little bearing on the qualification of its consequent employment as an armed attack.[300] This view also accords with State practice.[301]

While the notion of a cyber operation having the capacity to constitute an armed attack thus triggering the right of self-defence secured viable consensus, the issue of the threshold at which a cyber operation qualifies as an armed attack was more contentious. Most commentators insist that in order to meet the requisite threshold of armed attack, the relevant use of force must be on a relatively large scale and with substantial effect.[302] But this view is not uncontested; the position of the United States in this regard is that:

> 'the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response'.[303]

The divergent viewpoints illustrated above result from the finding of the ICJ in *Nicaragua*, which is wholly adopted in Rule 13, that not every use of force amounts to an "armed attack" for purposes of the right of self-defence. Accordingly, the Tallinn Manual upholds the *Nicaragua* categorization of uses of force into grave and less grave ones, with the consequence that the right of self-defence is only exercisable in respect of the former.[304] The raises the problem of how the

---

[298] RA Clarke & RK Knake, *Cyber War – The Next Threat to National Security and What to Do About It* (2010) 6.
[299] Tallinn Manual (n 8) 54.
[300] *Nuclear Weapons*, para 39.
[301] NATO's Glossary of Terms, 2-C-11; Joint Terminology for Cyberspace Operations, 3; Zhang (n 215) 4; White House Cyber Strategy, 10 and 13.
[302] D Fleck, 'Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the Tallinn Manual' (2013) 18(2) *Journal of Conflict of Security Law* 331, 337; Zemanek (n 54) paras 13, 21.
[303] HH Koh, Legal Adviser, US Department of State, 'International Law in Cyberspace', Speech at USCYBERCOM Inter-Agency Legal Conference, 18 September 2012.
[304] Tallinn Manual (n 8) Rule 13, paras 5-6.

"scale and effects" of a cyber operation can be measured and the threshold at which it can be considered as having risen to the level of an "armed attack" warranting self-defence action.[305]

The practical effect of the uncertainty surrounding the distinction between grave and less grave uses of cyber force can be illustrated by reference to actual cyber incidents. An example is the 2007 cyber operation launched against Estonia which was never clearly characterized as an armed attack.[306] Another instance is the 2010 cyber operation that did extensive damage to Iranian centrifuges; unlike the Estonian case, there was sharp division among the drafters of the Tallinn Manual, with some holding that Stuxnet was an armed attack while others seemingly disputing this view.[307]

2.4.2 Differentiated Uses of Cyber Force and "Accumulation of Effects"

The view taken by the International Group of Experts and supported by the *Nicaragua* case[308] that not every use of cyber force amounts to an armed attack is related to another important issue: whether a State may exercise its right of self-defence in response to a series of cyber attacks that would not constitute an armed attack if taken individually.[309] Proceeding from the position that an "armed attack" within the meaning of Article 51 of the UN Charter is distinct from, and requires a higher threshold than, a "use of force" within the meaning of Article 2(4) of the UN Charter, the critical legal question is: can individual cyber uses of force amount to an armed attack if aggregated, thereby giving rise to the right of a victim State to respond forcibly in self-defence?

The commentary to Rule 13 of the Tallinn Manual answers the above question in the affirmative and thus supports the "accumulation of effects" theory, which holds that there may be cases where individual incidents falling below the threshold of armed attack can be considered cumulatively to amount to an armed attack.[310] The specific view adopted by the Tallinn Manual is that: if there is "convincing evidence" indicating that the same "originator (or originators acting in concert) has carried out smaller-scale incidents that are related and that

---

[305] Tsagourias (n 62) 30.
[306] Tallinn Manual (n 8) Rule 13, at para 13.
[307] Ibid; Tsagourias (n 62) 30.
[308] *Nicaragua*, para 191.
[309] *Oil Platforms*, para 64; Tallinn Manual (n 8) 56, at para 8.
[310] Dinstein (n 2) paras 547-549.

taken together have the requisite scale" then the incidents may be treated as a "composite armed attack".[311]

Three problems arise from the position taken above. First, the commentary to Rule 13 of the Tallinn Manual does not set out the legal basis for its adoption of the "accumulation of effects theory", a theory that is contested both in international legal doctrine[312] as well as in practice.[313] It would have been more prudent to set out the basis of this theory in treaty or customary law. In this regard, it is noteworthy that the ICJ has made reference to the "accumulation of effects" theory as one of the means to establish whether there was an armed attack,[314] but it has not expressly relied on it as a conclusive test.[315] This makes the Tallinn Manual's uncritical reliance on this theory questionable. It would have been more satisfactory to explain a clear basis for such reliance.

Secondly, Rule 13 of the Tallinn Manual and its accompanying commentary do not discuss in sufficient detail the issue of the "requisite scale" that is required before a series of individual cyber incidents amount to an armed attack justifying resort to a forceful response. There is a real possibility that the resulting ambiguity may provide a ground for a State to respond with deadly force supposedly in the exercise of its right of self-defence in the event that it is subjected to two or more cyber incidents that may not, in fact, be serious or related.

Thirdly, by enunciating the "accumulation of effects" theory as justification for the use of defensive force, Rule 13 of the Tallinn Manual does not explain the constitutive element of an originator or originators acting in concert. This is surprising given the fact that the commentary to Rule 13 identifies this as a "determinative factor" in establishing whether or not a series of cyber incidents can be treated as a composite armed attack.

The nature of cyber operations makes it difficult to determine the identity of the originators of a cyber incident. Even less easily discernible is whether one or more originators are working

---

[311] Tallinn Manual (n 8) 56, at para 8.
[312] For proponents of this theory, see C Greenwood, 'Self-Defence' in *Max Planck Encyclopedia of Public International Law* (2010) para 13; B Simma et al (eds), *The Charter of the United Nations* (2012) 1409. For opponents of this theory, see N Lubell, *Extraterritorial Use of Force Against Non-State Actors* (2010) 51; T Gazzini, *The Changing Rules on the Use of Force in International Law* (2006) 192.
[313] *Public Committee Against Torture in Israel v the Government of Israel*, para 27; *Oil Platforms* (Dissenting Opinion of Judge Simma), para 14.
[314] *Armed Activities*, paras 146-147; *Oil Platforms*, para 64.
[315] Tsagourias (n 62) 31.

together towards the same objective. Thus, the failure of the Tallinn Manual to provide guidance on how to identify concerted cyber action significantly diminishes its practical utility. In particular, it makes it difficult for States to determine with certainty what the correct approach is. This is a ground for future normative development.

2.4.3 Cyber Operations not resulting in Adverse Physical Consequences

Rule 13 of the Tallinn Manual states that the determining factor on whether or not a specific cyber operation would constitute an armed attack within the meaning of Article 51 of the UN Charter is "its scale and effects."[316] The element of effects raises some problematic issues. Unlike kinetic operations, cyber operations may not result in the physical consequences (injury, death, damage or destruction) that are typically used as indicators of harm in the defensive force analysis. The critical legal question is whether a cyber operation that does not result in physical consequences, but which causes extensive adverse effects would constitute an armed attack for purposes of self-defence.[317]

It is regrettable that the above question of such practical importance was left unanswered by the International Group of Experts. Some of the Experts took the view that harm to persons or physical damage to property is determinative, while others maintained that it is the extent of the "ensuing effects" of an attack and not the injurious or destructive nature of the consequences that matters.[318] It is regrettable that the Tallinn Manual does not comment further on the validity of these divergent positions, consequently leaving the issue unsettled. It is the view of the present author that, given the nature of cyber operations, the extent of the ensuing effects is the better approach.

The negative effect of the Tallinn Manual's failure to provide a definitive answer to the above question can be illustrated by reference to the cyber incident which entailed a three-week Distributed Denial of Service (DDoS) attack against Estonia.[319] Majority of the DDoS attacks targeted government websites, banking data and systems, newspapers, television stations, and other targets.[320] While this attack caused significant economic disruption and communication

---

[316] Tallinn Manual (n 8) 54.
[317] Tsagourias (n 62) 31.
[318] Tallinn Manual (n 8) 56, at para 9.
[319] Roscini (n 4) 6.
[320] Tikk et al (n 16) 18.

breakdown, it did not result in any physical consequences.[321] Hence, the absence of clarity as to the characterization as "armed attack" of the DDoS attacks against Estonia and whether they can give rise to the legitimate use of defensive force is likely to present problems in future cases. This demonstrates the practical import of the Tallinn Manual's dispiriting lack of guidance in the above regard.

2.4.4 Cyber Operations by Non-State Actors

The commentary to Rule 13 affirms that the cyber actions of non-State actors that can be attributed to a State and which meet the requisite scale and effects requirement may constitute an armed attack for self-defence purposes.[322] With explicit reference to *Nicaragua*,[323] the commentary explains that if a single individual or a group of individuals under the direction of "State A undertakes cyber operations directed against State B, and the consequence of those actions reaches the requisite scale and effects, State A will have committed an armed attack."[324]

While there is little doubt that cyber actions by non-State actors which are clearly attributable to a State and which satisfy the scale and effects criteria can amount to an armed attack, the opposite is the case in instances where the conduct of the non-State actors is not directed by a State.[325] The commentary to Rule 13 does not state authoritatively whether acts of non-State actors can constitute an armed attack in the absence of State direction.[326] It nonetheless outlines two competing points of view in this regard. The first point of view, adopted by the majority of the Experts, is that cyber action may qualify as armed attack even absent attribution of such conduct to a State.[327] The second point of view is that State direction and consequent attribution of the cyber action of a non-State actor is determinative.[328]

Although the commentary to Rule 13 leaves does not take a decisive standpoint, the first point of view appears to be consistent with both treaty and customary law.[329] The customary

---

[321] SD Watts, 'Low-Intensity Computer Network Attack and Self-Defense' (2010) 87 *International Law Studies* 70.
[322] Tallinn Manual (n 8) 58, paras 14-15.
[323] *Nicaragua*, para 195.
[324] Tallinn Manual (n 8) 58, para 15.
[325] O de Frouville, 'Attribution: Private Individuals' in J Crawford *et al* (eds), *The Law of International Responsibility* (2010) 257-282.
[326] Tallinn Manual (n 8) Rule 13, paras 15-17.
[327] C Greenwood, 'Self-Defence' in *Max Planck Encyclopedia of Public International Law* (2012) paras 16-17.
[328] *Wall*, para 139; *Congo v Uganda*, para 146-147.
[329] Tsagourias (n 62) 31.

norm of self-defence derived from the *Caroline* case,[330] the "inherent" nature of the right of self-defence articulated in Article 51 of the UN Charter,[331] and Security Council Resolutions[332] all provide support for the view that the right of self-defence can be exercised in response to attacks by non-State actors that rise to the level of an "armed attack" within the meaning of Article 51 of the UN Charter. It is however notable that the majority ICJ *Wall* Opinion took a different view, arguing that Article 51 did not apply in the case because the wall was not built by Israel to defend against attacks attributable to a foreign State.[333] Nonetheless, this aspect of the majority opinion was criticized in the Separate Opinions of Judges Higgins[334] and Kooijimans.[335]

2.5 Necessity and Proportionality

Rule 14 of the Tallinn Manual provides that a "use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate."[336] This rule restates the dual customary criteria for the lawfulness of self-defence actions: necessity and proportionality.[337] Necessity denotes the requirement that a specific use of force is the only effective means of thwarting an imminent attack or defeating one that is already underway.[338]

An important point concerning necessity that is highlighted in the commentary to Rule 14 is that the existence of necessity to resort to forceful means by way of self-defence should be judged from the perspective of a victim State, and this determination must be "reasonable in the attendant circumstances."[339] This position is particularly relevant in the context of cyber operations because it is possible that a State which has been the victim of a cyber armed attack may not know that the attacker has desisted from the attacks.[340] Thus by preserving the continued existence of the right of self-defence, Rule 14 protects a victim State and, importantly, discourages unlawful uses of force. However, it is noteworthy that this does not supply a *carte*

---

[330] Jennings (n 293).
[331] Dinstein (n 2) 210-211.
[332] SC Res 1368; SC Res 1373.
[333] *Wall* Opinion, para 139.
[334] Separate Opinion of Judge Higgins, para 33.
[335] Separate Opinion of Judge Kooijimans, para 35.
[336] Tallinn Manual (n 8) 61.
[337] *Nicaragua*, para 176, 194; *Nuclear Weapons* Advisory Opinion, para 41, *Oil Platforms*, paras 43, 73-4, 76.
[338] E Wilmshurst, 'The Chatham House Principles of International Law on the Use of Force in Self-Defence' (2008) 55(4) *International and Comparative Law Quarterly* 963, 967.
[339] Tallinn Manual (n 8) Rule 14, para 4.
[340] Ibid.

blanche right of self-defence; inherent in the concept of necessity is the strict and objective limitation of measures taken avowedly in self-defence, thereby "leaving no room for any measure of discretion."[341]

Proportionality concerns itself with the quantity of force, including cyber force, by way of self-defence that is permissible once the necessity requirement is satisfied.[342] The standard of proportionality of defensive force is that the scale, scope and duration of force used should not be excessive in relation to the aim sought to be achieved, that is, effective repulsion of an armed attack or defeating one that is imminent.[343] It is noteworthy that the Tallinn Manual adopts a flexible approach to the proportionality analysis by recognizing that the amount of force required to successfully mount a defence against a cyber armed attack is "context-dependant".[344] However, it is notable that this view is stated in the commentary without any further elaboration specific to the cyber context, thus making it doubtful how the unique aspects of proportionality in cyber space should be determined.

Nonetheless, the commentary to Rule 14 makes a notable statement to the effect that there is no requirement that the defensive force be of the same nature as that constituting an armed attack.[345] This makes clear that a victim State's right of self-defence in general and the proportionality of its response in particular need not be restricted to the original unlawful use of force against it. Accordingly, it explains that "a cyber use of force may be resorted to in response to a kinetic attack, and vice versa."[346] It further clarifies that while forceful kinetic operations by way of self-defence may be permitted, they must be strictly restricted to the objective of repelling or defeating an armed cyber attack.[347]

2.6 Imminence and Immediacy

Rule 15 of the Tallinn Manual sets out the temporal parameters for the lawful resort to forceful measures, which seeks to supply an answer to the question concerning the precise moment at which a cyber armed attack may trigger the right of self-defence. The rule provides that: "The

---

[341] *Oil Platforms*, para 73.
[342] *Nicaragua*, para 176; *Nuclear Weapons* Advisory Opinion, para 41.
[343] Tallinn Manual (n 8) Rule 14, at para 5.
[344] Ibid.
[345] Ibid.
[346] Ibid.
[347] Ibid.

right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy."[348]

This rule, which is based on Article 51 of the UN Charter and customary international law as expressed in the *Caroline* test, indicates that a State may resort to self-defence if the necessity of that self-defence is "instant, overwhelming, leaving no choice of means and no moment of deliberation".[349] It thus permits self-defence in anticipation of a cyber armed attack.[350] Rule 15 also takes into account the view that self-defence applies only in respect of cases where an armed attack has already occurred[351] or is still incipient.[352] Rule 15 therefore fails to reconcile the competing views as to the permissibility or prohibition of anticipatory action. Moreover, the approach adopted in the Tallinn Manual implicitly reinforces the accepted position that a factual determination of imminence must be made in good faith by the relevant State, and on evidentiary grounds that are capable of objective assessment.[353]

While it is an arguable rule of custom that self-defence action may be resorted to in respect of an imminent armed attack, the more difficult question concerns the temporal interpretation of the word "imminent" in the context of armed cyber operations.[354] Two approaches emerged in this regard: a "strict temporal" approach which limits the scope of anticipatory action to instances where a cyber armed attack is about to be conducted; and a "last feasible window of opportunity" approach which permits self-defence where the victim State will lose its opportunity to effectively defend itself when the attack starts unless it acts promptly.[355] The majority of the Experts supported the later interpretation of imminence, an outcome that indicates they took significant account of the unique nature of cyber operations.

While this view may be criticized as opening the possibility for some States to act unlawfully in supposed self-defence, the commentary to Rule 15 elaborates that the "potential victim State must first reasonably conclude that the hostility has matured into an actual decision to attack."[356]

---

[348] Ibid.
[349] Letter from Daniel Webster to Lord Ashburton (6 Aug 1842), reprinted in JB Moore (ed), *International Law Digest* (2nd ed, 1906) 412.
[350] Tallinn Manual (n 8) Rule 15, at para 2.
[351] Ibid at para 3.
[352] Ibid at para 3; Dinstein (n 2) 203-4.
[353] E Wilmshurst (n 338) 968.
[354] Tsagourias (n 62) 35.
[355] Tallinn Manual (n 8) Rule 15, at para 4.
[356] Ibid at para 7.

This accords with treaty and customary law in force, but it is less clear how the determination of the inference of a decision to attack should be made. This is particularly problematic in the context of cyber operations where evidence of conduct is usually surreptitious and hard to determine.[357]

In recognition of this, Rule 15, as elaborated in its commentary, adopts the position that the "lawfulness of any defensive response will be determined by the reasonableness of the victim State's assessment of the situation."[358] This is realistic because it affords a potential victim State the opportunity to respond effectively to an armed cyber attack. However, it must be insisted that any such determination must be objective, and the standard of objectiveness should be assessed on a case-by-case basis taking into account all the relevant contextual factors.

PART II JUS IN BELLO

3. A CRITIQUE OF *JUS IN BELLO* RULES IN THE TALLINN MANUAL

This section examines selected *jus in bello* Rules of the Tallinn Manual that relate to the application of international humanitarian law to cyber operations. It examines: the extent to which the rules of international humanitarian law apply to cyber operations; the characterization of cyber conflicts; the definition of cyber attack; and doubt as to the status of individuals or objects.

3.1 Applicability of the Law of Armed Conflict

Rule 20 of the Tallinn Manual affirms the applicability of the law of armed conflict to the cyber conduct of belligerents during an armed conflict; it specifically states that "[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict."[359] This view has been explained by the ICJ in its *Nuclear Weapons* Opinion, where it observed that the established principles and rules of humanitarian law applicable in armed conflicts "applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[360] The applicability of the existing norms of the law of armed conflict to cyber

[357] Tsagourias (n 62) 36.
[358] Tallinn Manual (n 8) Rule 15, at para 6.
[359] Ibid at 75.
[360] *Nuclear Weapons*, para 39.

operations conducted in the context of an armed conflict also appears to be supported in State practice.

For instance, during the 2012 Operation Pillar of Defense, Israel's chief information officer stated that "[t]he war is taking place on three fronts. The first is physical, the second is on the world of social networks and the third is cyber".[361] The practice of the United States also supports the view that cyber operations are subject to the current framework of the law of armed conflict; the United States Department of Defence has stated that "[i]nternational legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e. sea, air, land, and space), also apply to the cyberspace domain."[362]

An important point that is captured in the commentary to Rule 20 is that while it is generally accepted that the law of armed conflict applies to cyber operations undertaken in the context of an armed conflict, the application of this law is contingent on a nexus existing between the cyber activity and the armed conflict.[363] However, the nature of the requisite nexus was a point of contention. There are those Experts who held that nexus can only be established if a cyber activity is conducted by a party to an armed conflict (or on its behalf) against its opponent, while others held that the cyber activity must have been used to contribute to the originator's military effort.[364] The following example is cited in the commentary to Rule 20 to illustrate the different viewpoints:

> Consider a cyber operation conducted by State A's Ministry of Trade against a private corporation in enemy State B in order to acquire commercial secrets during an armed conflict. According to the first view, the law of armed conflict would govern that operation because it is being conducted by a party to the armed conflict against a corporation of the enemy State. Those Experts adopting the second view considered that the law of armed conflict does not apply because the link between the activity and the hostilities is insufficient.[365]

According to the later school of thought (nexus turning on its advancement of a party's military effort), the law of armed conflict would not apply because of an insufficient nexus

---

[361] Roscini (n 4) 8.
[362] US Department of Defense, *Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934, November 2011, p 9.
[363] Tallinn Manual (n 8) Rule 20, at para 5.
[364] Ibid.
[365] Ibid.

between the cyber activity and the hostilities. Yet the former school of thought found the law of armed conflict to apply.[366] This illustrates disagreements on fundamental issues of the law of armed conflict, which is likely to have implications on the future development of the legal regulation of cyber operations.

The divergence of views as to the existence of a cyber armed conflict and the scope of the applicable international humanitarian law points to a fundamental problem: the legal regulation of hard-to-define and frequently changing conflicts.[367] In this regard, paragraph 9 of the commentary to Rule 20 notes that the application of the law of armed conflict to cyber operations can prove problematic.[368] It further explains that it "is often difficult to identify the existence of a cyber operation, its originator, its intended object of attack, and its precise effects."[369] Importantly, however, it takes the view that these uncertainties of fact do not preclude the application of the law of armed conflict.

This view is substantiated by reliance on the Martens Clause which states that in cases that do not appear to be clearly covered by any specific rule of the law of armed conflict, the applicable law remains to be derived from "the principles of law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of public conscience."[370] This clarifies that even when the nature, actors, effects and objects of a cyber operation are unclear or altogether unknown, such conduct does not occur in a legal limbo.

Hence, the Tallinn Manual adopts the convincing position that to the extent that cyber activities are conducted in the course of an armed conflict, the Martens Clause, which constitutes customary international law, functions to ensures that such activities are not conducted in a legal vacuum.[371]

3.2 Characterization of Armed Conflict

The rules regarding the characterization of a cyber armed conflict either as international or non-international are is set forth in Rules 22 and 23 respectively. Rule 22 stipulates that an international armed conflict "exists whenever there are hostilities, which may include or be

---

[366] Ibid.
[367] Roscini (n 4) 1.
[368] Tallinn Manual (n 8) Rule 20, at para 9.
[369] Ibid at 77.
[370] Preamble, Hague Convention IV.
[371] Tallinn (n 8) 78.

limited to cyber operations, occurring between two or more States."[372] For its part, Rule 23 provides that:

> A non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organization.[373]

A contentious question that arises regarding the characterization of international armed conflict is whether such a conflict can arise between a State and a non-State actor which operates across international borders. The Experts failed to agree on this issue, thus leaving the question unresolved.[374] While it is acknowledged that this question has not been conclusively resolved even in the practice regarding purely kinetic operations, it was a lost opportunity for the Tallinn Manual to advocate a progressive interpretation.

The characterization as non-international armed conflict of cyber operations also raised sharp disagreement with particular regard to the requisite elements of intensity and organization. Specifically, the Experts could not agree whether non-destructive cyber operations conducted during civil disturbances could tip the scale and raise the violence to the level of armed conflict.[375]

3.3 Definition of Cyber Attack

Rule 30 of the Tallinn Manual defines a "cyber attack" in the following terms: "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[376] The notion of "attack" provides a basis for several provisions that constitute the law of armed conflict and is central to the rules of targeting and the regulation of means and methods of warfare. Rule 30 is modelled, in large part, after Article 49(1) Additional Protocol I which defines "attack" as "acts of violence whether in offense or in defence". However, neither Article 49(1) nor its Commentary describes what the notion of "violence" entails.

---

[372] Ibid at 79.
[373] Tallinn Manual (n 8) 84.
[374] Ibid, Rule 22, para 9.
[375] Ibid, Rule 23, at para 10.
[376] Ibid at 106.

By contrast Rule 30 implicitly elaborates the notion of violence by requiring that the consequence of a cyber operation be injury or death to individuals or destruction to objects. These criteria are useful when viewed from the perspective of cyber operations. For instance, at what point can the destruction of data constitute an attack? The Tallinn Manual takes a purposive view that although data constitutes non-physical entities, the threshold of "armed attack" will be satisfied when an attack on data results in death of individuals or damage and destruction to physical objects.[377]

The problem with this interpretation is that it fails to take account of the unique aspects of cyber operations; for instance, while a cyber operation that deletes all the social security data of adult citizens before an election thereby causing deep anxiety would not amount to an attack, the physical destruction of a polling centre would do so. This reveals a fundamental inadequacy of Rule 30, which reflects the fact that current international humanitarian law has not systematically taken account of the value of digital assets.[378]

3.4 Doubt as to Status of Persons and Objects

Rule 33 of the Tallinn Manual provides that: "In case of doubt as to whether a person is a civilian, that person shall be considered a civilian."[379] This rule restates the general rule of presumption of civilian status in cases of doubt which is codified in Article 50(1) AP I, and which reflects customary international law.

The commentary to Rule 33 provides an instructive discussion on the varying standards for determining the threshold at which the presumption of civilian status applies, thus bringing this Rule into operation.[380] This discussion is particularly useful because it relates to another important aspect of the rule on presumption of civilian status: the burden of disproving civilian status in cases of doubt. In this regard, the Tallinn Manual convincingly adopts the view that since the attacker has a duty to take active precautions it would not be appropriate to shoulder the burden of proving that a targeted individual is actually a legitimate target.[381] In some cases, the defender must take passive precautions such as unambiguously demonstrating that they are civilians.

---

[377] Tallinn Manual (n 8) Rule 30, at para 6.
[378] Schmitt (n 14) 96.
[379] Tallinn Manual (n 8) 114.
[380] Ibid at 114-15, paras 3 and 4.
[381] Ibid, Rule 33, para 2.

The above view taken by the Independent Group of Experts is enunciated in Rule 40 of the Tallinn Manual which states that: "In case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, a determination that it is so being used may only be made following a careful assessment."[382]

4. SUMMARY OF THE MERITS AND DEMERITS OF THE TALLINN MANUAL

This section undertakes a critical appraisal of the merits and demerits of the *Tallinn Manual* with a view to highlighting its positive aspects and to suggest improvements where it is lacking. This section is important since it summarizes how the International Group of Experts addressed some of the contested questions of international law and critiques selected Rules that emerged as a result.

4.1 General Applicability of Current Norms to Cyber Operations

A notable feature and perhaps the most significant contribution of the Tallinn Manual is its emphasis on the fact that international law applies to cyber warfare, an unprecedented domain in the modern conduct of hostilities with challenging possibilities. By identifying and outlining specific Rules derived from existing international legal norms that apply to cyber warfare, the Tallinn Manual underscores the view that international humanitarian law 'applies to new weaponry and to the employment in warfare of new technological developments'.[383]

4.2 Specific Applicability of International Humanitarian Law

The divergence of views regarding the existence of a cyber armed conflict and the scope of the applicable international humanitarian law points to a fundamental problem: the legal regulation of hard-to-define and frequently changing conflicts. In this regard, paragraph 9 of the Commentary to Rule 20 specifically notes that the application of the law of armed conflict to cyber operations can prove problematic. It further explains that it 'is often difficult to identify the existence of a cyber operation, its originator, its intended object of attack, and its precise effects.'[384] Importantly, however, it takes the view that these uncertainties of fact do not preclude the application of the law of armed conflict.

---

[382] Tallinn Manual (n 8) 157.
[383] ICRC (n 163) 36.
[384] Tallinn (n 8) 77.

This view is substantiated by reliance on the Martens Clause which states that in cases that do not appear to be clearly covered by any specific rule of the law of armed conflict, the applicable law remains to be derived from 'the laws of humanity, and the dictates of public conscience.'[385] This clarifies that even when the nature, actors, effects and objects of a cyber operation are unclear or altogether unknown, such conduct does not occur in a legal vacuum. Accordingly, the Tallinn Manual convincingly adopts the position that to the extent that cyber activities are conducted in the course of an armed conflict, the Martens Clause, which constitutes customary international law, functions to ensures that such activities are not conducted in a legal vacuum.[386]

4.3 Cyber Operation not constituting an "Attack"

The Tallinn Manual provides detailed guidance regarding the legal regulation of cyber operations amounting to an "attack" within the meaning of Article 48 of Additional Protocol I. Article 48 Additional Protocol I restates the customary principle of distinction, stating that parties to a conflict "shall direct their operations only against military objectives". However, the Manual provides little guidance and consequently limited protection in instances where the pertinent operations do not amount to an attack. In particular, the Manual does not discuss in detail how the existing rules of international law, including the customary rule of distinction, protect in cases where the effects of cyber operations do not satisfy the minimum threshold of harm, requiring injury or death to persons or damage or destruction to objects.[387] This is further complicated by the commentary to Rule 30 which provides that minimal damage or destruction does not meet the threshold of harm required in cyber attack.[388]

The position apparently taken in the Tallinn Manual which suggests that the rules of the law of armed conflict may not cover cyber incidents not constituting an "attack" is problematic because it creates gaps in legal regulation. This runs contrary to the stated mission of the International Group of Experts, as expressed by the Project Director of the Tallinn Manual, who

[385] Preamble, Hague Convention IV.
[386] Tallinn Manual (n 8) 78.
[387] Ibid at 106.
[388] Ibid at 107.

explains that the project sought to bring some degree of clarity to complex legal issues on cyber operations, including the law of armed conflict.[389]

4.4 Sparse Regulation of Low-threshold Cyber Incidents

The introduction to the Tallinn Manual specifically states that it does not address cyber activities that occur below the level of a "use of force" within the meaning of Articles 2(4) and 51 of the UN Charter. It also does not set out any prohibitions on specific cyber actions falling below the "armed conflict" threshold that is necessary for the application of international humanitarian law. This indicates that the Tallinn Manual excludes low-threshold actions which are neither regulated by the *jus ad bellum* nor the *jus in bello*. But it is important to note that the Manual does not foreclose the applicability of other international legal standards relative to cyber operations.[390]

Indeed, the Tallinn Manual is without prejudice to other applicable fields of international law, such as international human rights or telecommunication law.[391] An illustrative example of the extent of the Tallinn Manual's accommodativeness is its treatment of cyber espionage in the context of defining the use of force (Commentary to Rule 11)[392] and in the context of armed conflict (Rule 66).[393] In spite of this, the overall reach of the Tallinn Manual is woefully limited, thus giving little operational guidance in cases where cyber activities are employed but it is unclear whether the threshold of applicability of *jus in bello* or *jus ad bellum* has been attained.

4.5 Critical Legal Issues not Sufficiently Addressed

An objective examination of the Tallinn Manual reveals that certain critical legal issues are either insufficiently addressed or ignored altogether. While the Manual deals with some important issues providing welcome clarity, it would be difficult for any satisfactory critique to fail to show some of its notable weaknesses. In the following sub-sections, selected legal issues of critical importance will be highlighted.

4.5.1 Jurisdictional Bases in Cyberspace

---

[389] Ibid at 3.
[390] Tallinn Manual (n 8) 4-5.
[391] Ibid at 4.
[392] Ibid at 50.
[393] Ibid at 192-93.

Part 1 of the Tallinn Manual, entitled "International cyber security law", indicates that its aim is to provide operational clarity as regards those aspects of international law that are pertinent to the "hostile use of cyberspace, but are not formally an aspect of the *jus in bello*."[394] Having expressly excluded the *jus in bello*, the Manual specifies that its primary focus is on aspects of *jus ad bellum*, including jurisdiction. A crucial point to note is that the drafters of the Manual explicitly rejected the view that owing to its relative novelty, "international law is silent on cyberspace in the sense that it is a new domain subject".[395] Instead, unanimity was achieved in support of the contrary view.[396]

The rule of the Tallinn Manual which specifically addresses the *jus ad bellum* aspect of sovereignty is consistent with the view that the general principles of international law are not excluded from the regulation of cyberspace. In particular, Rule 2 states that:

> Without prejudice to applicable international obligations, a State may exercise its jurisdictions:
>
> (a) over persons engaged in cyber activities on its territories;
> (b) over cyber infrastructure located on its territory; and
> (c) extraterritorially, in accordance with international law.[397]

Paragraph 1 of the commentary to Rule 2 confirms that the jurisdictional authority to prescribe, enforce and adjudicate extends to all matters, including those of a "civil, criminal or administrative" nature.[398] The commentary further explains that all the jurisdictional bases that are recognized in international law apply in a more or less similar manner to cyberspace, albeit with appropriate restrictions.[399]

However, the specific issues regarding the application of the internationally recognized jurisdictional bases authorizing lawful State action are not discussed in any satisfactory detail.[400] This leaves room for significant doubt concerning important legal issues that have practical significance in concrete operations. For instance, a reading of Rule 2 of the Tallinn Manual does not make clear: i) whether this Rule applies to objects owned by a State and used specifically for

---

[394] Ibid at 13, para 1.
[395] Tallinn Manual (n 8) 13.
[396] Ibid at 13.
[397] Ibid at 18.
[398] Ibid at Rule 2, para 1.
[399] Ibid at Rule 2, para 8.
[400] Fleck (n 302) 348.

commercial purposes;[401] ii) precisely how a State may exercise jurisdiction over persons or objects that are, at the relevant time, properly within the jurisdiction of two or more States;[402] and iii) the basis on which civilians or non-State entities not clearly affiliated to a State but apparently performing State functions are subject to the relevant State's jurisdiction.[403]

Another weakness is the fact that despite the affirmation of the Tallinn Manual's drafters that the general principles of international law apply in cyberspace, an examination of Rules 2 – 4 does not sufficiently explain whether the content of the Rules set forth "evidences a general principle of public international law".[404]

4.5.2 Limits to Security Council Action

Section 3 of Chapter 2 (The use of force) of the Tallinn Manual, entitled "Actions of international governmental organizations", discusses the role of both international and regional organizations in discharging their respective mandates when dealing with threats to international peace.[405] The organizations referred to in Section 3 (Rules 18 and 19) are those that are established under the UN Charter. Specifically, while the collective security mandate of the UN Security Council has its legal basis in Article 39 UN Charter, that of regional organizations is founded on Article 52(1) UN Charter which empowers the respective regional entities to develop systems of collective security that are "appropriate for regional action".[406]

Rule 18 contemplates the resort, in the first instance, to non-forceful cyber operations in response to a threat to the peace, breach of the peace, or an act of aggression within the meaning of Article 39 UN Charter. Also, it contemplates the authorization of forceful cyber operations if non-forceful measures are not effective.[407] For its part, Rule 19 recognizes the capacity of regional organizations to "conduct enforcement actions, involving or in response to cyber operations, pursuant to a mandate from, or authorization by, the United Nations Security Council."[408] What is most commendable about these rules is that they are well-anchored on

---

[401] Tallinn Manual (n 8) Rule 2, para 6.
[402] Ibid at para 9.
[403] Tallinn Manual (n 8) Rule 2, at para 10.
[404] Fleck (n 302) 348.
[405] Tallinn Manual (n 8) 69-72.
[406] Ibid at Rule 19, para 2.
[407] Ibid at Rule 18; Tsagourias (n 62) 37.
[408] Tallinn Manual (n 8) 71-72.

primary sources of international law,[409] namely statutory provisions, resolutions of international [410] and (inter)national jurisprudence.[411]

4.5.3 Possible limits on UN Security Council enforcement action

Rule 18 of the Tallinn Manual sets out the scope of the UN Security Council's powers deriving from its enforcement mandate established under Articles 39, 41 and 42 UN Charter. More specifically, Rule 18 sets out the extent to which the UN Security Council may deal with escalating and new threats.[412] While it is welcome that Rule 18 adapts the provisions of Article 39 UN Charter to the novel situations that may arise with regard to cyber operations, a notable defect of this Rule is the fact that it does not explain important aspects of the scope of the Security Council's enforcement mandate in sufficient detail. For instance, the commentary to Rule 18 concedes that: "It is uncertain whether other rules of international law limit the authority of the Security Council to authorize or mandate action."[413]

The illustration used in connection with the above view poses the critical legal question as to whether a specific Security Council authorization to conduct cyber attacks against civilians would override a related prohibition. However, it fails to answer this question. Hence, it does not provide any meaningful guidance on how to proceed in the event that there is a conflict of legal obligations. It, however, states that in any event the Security Council's decision to resolving this problem and consequently violate "rules of international law" exercise its enforcement mandate "should not be taken lightly".[414] It also states categorically that under no circumstances may the Security Council deviate from rules of a *jus cogens* nature."[415]

The main problem is that the solution offered by the Tallinn Manual to the critical legal issue of a conflict of legal obligations and the view it adopts regarding the supposed primacy of *jus cogens* norms vis-à-vis the Security Council's powers does not provide an objective analysis of relevant authorities and evidence in support of its position. Instead, paragraph 8 of the commentary to Rule 18 uncritically adopts a rigid view, while there exists authority and evidence

---

[409] Brownlie (n 173) 6.
[410] Rule 18 is based on UNSC Resolution 1373 (2001); UNSC Resolution 1378 (2001); and UNSC Resolution 1540 (2004). For its part, Rule 19 is based on Articles 52 and 53 UN Charter.
[411] See *Al Jedda v UK*; *Nada v. Switzerland*.
[412] Tsagourias (n 62) 37.
[413] Tallinn Manual (n 8) Rule 18, para 8.
[414] Ibid; Tsagourias (n 62) 38.
[415] Ibid.

to suggest the contrary.[416] For instance, the position adopted above makes it unclear how other customary international obligations upon the Security Council may be reconciled with *jus cogens* norms in the context of cyber operations.

4.6 Geographical and Institutional Bias

The Tallinn Manual had the institutional backing of the NATO Cooperative Cyber Defence Centre of Excellence. Thus, it is understandable and indeed is to be expected that the majority of the legal experts involved in the writing of the Manual would be drawn from NATO States. An examination of the list of the International Group of Experts and Participants and their respective affiliations confirms this geographical and institutional bias;[417] it constitutes individuals who are legal experts from predominantly Western European, North American and Australasian backgrounds.[418] On the face of it this smacks of Western political and strategic positioning, a fact that is likely to impact negatively on the legitimacy of the Manual.[419]

Even more surprising is the fact that Estonia, a one-time victim of cyber operations and the host State in which the Tallinn Manual was drafted and adopted, only had one legal expert representing its interests. This fact adds more force to the criticism that the Tallinn Manual is under-representative and therefore should not be taken as a conclusive representation of international law applicable to cyber warfare. Hence, the legitimacy of the Tallinn Manual can easily be called to question by other non-participating but militarily significant States such as China, Russia, Iran and North Korea, which are incidentally key players in the field of cyber warfare.

However, the fact that the Tallinn Manual is not the product of broader geographical and institutional consultation does not necessarily preclude its usefulness in its entirety. The Tallinn Manual does not purport to be an exercise in treaty law-making. Instead, it clearly states that its content is only meant to identify and restate current international law and to clarify how such law applies in relation to the unique aspects of cyber warfare.[420] Therefore, the content of the Tallinn

---

[416] Tsagourias (n 62) 38.
[417] Tallinn Manual (n 8) x-xiii.
[418] R Liivoja & TH McCormack, 'Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello' (2012) 15 *Yearbook of International Humanitarian Law* +4.
[419] O Kessler & W Werner, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' (2013) 26(4) *Leiden Journal of International Law* 793, 803.
[420] Tallinn Manual (n 8) 5.

Manual may arguably be considered objective despite the participation of some of other states with particular interest and experience in the question of cyber warfare such as China, Russia and North Korea.

5. CONCLUDING OBSERVATIONS

The Tallinn Manual identifies and explains the rules and principles of international law applicable to cyber operations, but it is not comprehensive. Indeed, it has some gaps in legal regulation and should be considered a work in progress. Nonetheless, a critically important contribution of the Tallinn Manual is its emphasis that current international legal norms apply to cyber operations, thereby demonstrating that existing international law is not "silent on new technological developments."[421] This will no doubt lend support to the view that despite the little definitive guidance on the subject of legal regulation of cyber operations, States are not consequently relieved of their obligation to comply with applicable international law.[422]

The review in this chapter has revealed a number of merits as well as a few weaknesses of the Tallinn Manual. However, the flaws of the Manual detract little from the general value and importance of the Tallinn Manual. In particular, the Manual provides a fairly detailed, well-researched and clearly presented guideline on the operational rules that are applicable in cyber warfare. This is further complemented by the accessible writing style which makes clarity and accessibility of its presentation.

The most important point to note is that the Tallinn Manual had the challenging task of introducing clarity to the legal rules that ought to govern the relatively new domain of cyber operations with all its complexities and uncertainties. Insofar as the Manual prudently admits to its limitations, it is critical to note that it is a crucial first step in the progressive process of developing the international legal framework that should regulate cyber operations. That this chapter has highlighted selected legal gaps in regulation, limited protection in certain instances and some notable absence of clarity regarding some issues provides support for the fact there is indeed a need for continued work towards developing comprehensive rules on the international law applicable to cyber operations. This is the task that the next chapter will seek to address.

---

[421] Fleck (n 302) 349.
[422] Tallinn Manual (n 8) 3.

Chapter IV

THE TALLINN MANUAL AND THE FUTURE OF LEGAL REGULATION OF CYBER OPERATIONS UNDER INTERNATIONAL LAW

1. INTRODUCTION

It is generally recognized that existing international law applies to cyber operations. What is less clear, however, is how certain unique aspects of cyberspace can fit into the current framework of international law. While the current framework is applicable in principle, there may be some daunting challenges regarding its practical application. For example, it has been observed that "the use of computer technology to wage war necessitates a re-evaluation of the definition of the term 'weapon'."[423] Another point that illustrates the insufficiency of the existing framework is the special role played by non-State actors in cyberspace operations. Typically, when faced with threats, including cyber threats, from non-State actors there is a tendency on the part of States to respond in ways that overstep legal boundaries.[424] This highlights the need for cyber-specific norms to constrain State conduct within the limits of long-established rules of international law.

This Chapter focuses on the special role that non-binding instruments can play in the emergence of binding norms to govern new and emerging contexts. In particular, it undertakes a comparative analysis of the Tallinn Manual and other non-binding instruments of international law. The primary object of this process is to suggest, with reference to the experience of earlier instruments, how best binding cyber-specific norms can be developed.

2. NON-CONVENTIONAL SOURCES OF INTERNATIONAL LAW

The Statute of the International Court of Justice (ICJ Statute) outlines the sources of international law.[425] In particular, Article 38(1) of the ICJ Statute provides that:

> '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 recognized by the contesting states;

[423] D Brown, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harvard International Law Journal* 179, 184.
[424] LR Blank, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 *International Law Studies* 437.
[425] Statute of the International Court of Justice, 59 Stat. 1031, U.N.T.S. 993.

b) international custom, as evidence of a general practice accepted as law;
c) the general principles of law recognized by civilized nations;
d) subject to provisions of Article 59, judicial decisions and teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law'.

Of particular interest to this section are two non-conventional sources of international law: custom and general principles of law.[426] The text of Article 38(1) of the ICJ Statute makes clear that custom and general principles of law are equivalent to international conventions.[427] But unlike conventional law which derives its legal force from the consent of the parties thereto, customary norms and general principles of law draw their binding force from extensive and uniform practice.[428] More specifically,

> 'Given the rudimentary character of international law, and the lack of both a central law-making body and a central judicial institution endowed with compulsory jurisdiction, in practice many decisions of the most authoritative courts (and in particular the ICJ) are bound to have crucial importance in establishing the existence of customary rules'.[429]

It is noteworthy that domestic judicial interpretations of the content of judgments issued by international courts also constitute important indicators of the recognition of certain rules as an emanation of a general principle of law.[430]

Non-binding instruments may also qualify as sources of international law. These instruments may include, among others, declarations, codes of conduct, manuals drafted by independent experts, and reports by non-governmental organizations. The utility of such instruments lies in the fact that they elaborate general rules and express general expectations of the conduct of States. But the normative value of such instruments may be erroneously discounted on the basis that Article 38(1) of the ICJ Statute does not explicitly recognize them as sources of international law.

Although non-binding instruments are not listed as sources of law in Article 38(1) of the ICJ Statute, they nevertheless articulate established norms and are often drafted with a view to respond effectively to contemporary developments. Hence, these instruments can be taken as evidence of "subsequent practice" under Article 31(3)(b) of the VCLT when interpreting a

---

[426] LF Damrosch et al, *International Law: Cases and Materials* (2001) 134-35.
[427] S Rosenne, *The Law and Practice of the International Court* (2006) 645.
[428] International Law Association, *Final Report of the Committee: Statement of Principles Applicable to the Formation of General Customary International Law*, 69 International Law Association Representatives Conference, (2000) 712, 719 (2000).
[429] A Cassese, *International Law* (2001) 159.
[430] ML Movsesian, 'Judging International Judgments' (2007) 48 *Virginia Journal of International Law* 65, 88-89.

particular binding treaty norm. Consequently, they may be relied upon when interpreting existing treaties. Non-binding instruments may also provide an instructive indicator as to the attitudes of certain States regarding particular conduct by looking, for instance, at relevant State participation in the adoption of that instrument. This is particularly pertinent in the case of instruments adopted by consensus and adopted by governments.

A more distinct role of non-binding instruments that will be the focus of this Chapter is their special role as a means to build consensus as to the acceptance of certain norms before their eventual transformation into binding norms.[431] Recent developments in international law point towards the increasing utility of non-binding instruments as a critical precursor to the emergence of binding norms. The following section will briefly examine this trend with a view to suggesting the way forward in developing binding norms to govern State conduct in cyberspace.

3. NON-BINDING INSTRUMENTS

International law is primarily made, applied and enforced by States, and its binding force derives from the fact of consent among contracting parties to international treaties to be bound by the rules set forth therein.[432] But the process of codifying such rules in the form of treaties is long and often encumbered by politics.[433] This poses considerable challenges when seeking to codify timely international rules to govern emergent fields that are sparsely regulated by existing international law. With particular regard to the area of international humanitarian law, this reality has seen the emergence of pragmatic alternatives to the State-centric process of international legislation.

3.1 Emerging Trends in the Adoption of Non-Binding Instruments

A notable feature of the past twenty years in the legislative history of international humanitarian law has been the growing role of non-State, expert-driven initiatives to clarify the international law applicable to under-codified forms of warfare. In contrast to the State-centric process of international law-making which produces binding rules, the alternative non-State process entails the production by international groups of experts of non-binding instruments. These instruments

[431] D Thurer, 'Soft Law' in R Bernhardt (ed), *Encyclopedia of Public International Law* (1993) 449.
[432] Kessler & Werner (n 419) 805.
[433] Ibid.

are subsequently adopted under the auspices of non-governmental forums, and some of them are eventually incorporated into the military manuals of States.

Examples of non-binding instruments dealing with specific aspects of international law applicable to different types of warfare include: (i) the San Remo Manual on International Law Applicable to Armed Conflicts at Sea[434] (Naval Warfare Manual) adopted by the International Humanitarian Law Institute; (ii) the San Remo Manual on the Law of Non-International Armed Conflict[435] (Non-International Armed Conflict Manual) adopted by the International Humanitarian Law Institute; and (iii) the Manual on International Law Applicable to Air and Missile Warfare[436] (Air and Missile Warfare Manual) adopted by the Harvard Program on Humanitarian Policy and Conflict Research.

3.2 Common Aspects of Non-Binding Instruments

The similarities between these manuals are readily apparent; not only are they all non-binding instruments adopted under the auspices of non-governmental entities, but they are also the product of an expert-driven process whereby legal experts comprising scholars and practitioners set forth the applicable law. Another important similarity, which is also reflected in the Tallinn Manual, is that the legal experts participated in the drafting process and endorsed its final outcome not in their official or institutional capacities, but as independent experts acting solely in their personal capacity.

3.3 The Naval Warfare Manual and the Tallinn Manual Compared

The Naval Warfare Manual provides instructive insight when compared with the Tallinn Manual because it was adopted earlier than the other instruments and also because it has been more widely accepted. This Manual shares certain significant similarities with the Tallinn Manual. First, the title of the Tallinn Manual derives its inspiration from the Naval Warfare Manual; both of them set out as the aim of the respective documents the elaboration of the rules of international law applicable to specific subject-matter. Secondly, both the Tallinn Manual and the Naval Warfare Manual were prepared by a group of experts, acting in their personal

---

[434] L Doswald-Beck (ed) *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (1995).
[435] MN Schmitt et al (eds) *San Remo Manual on the Law of Non-International Armed Conflict with Commentary* (2006).
[436] Harvard Program on Humanitarian Policy and Conflict Research *Manual on International Law Applicable to Air and Missile Warfare, with Commentary* (2010).

capacities, who have recognized expertise and deep knowledge of the relevant subject-matter. Moreover, both the final texts of the Tallinn Manual and the Naval Warfare Manual were adopted under the auspices of institutions, namely the NATO CCD-COE and the San Remo Institute for International Law.

As regards the substantive content of the Naval Warfare Manual and the Tallinn Manual, both Manuals set out specific rules and also provide a useful elaborations and explanations. The Naval Warfare Manual refers to this as the "Explanation" while the Tallinn Manual employs the term "Commentary", but both terms denote one and the same thing. This serves the purpose of setting forth the basis of the particular rule in treaty and customary international law, and it also explains the manner in which the drafters interpreted the applicable norms in the respective contexts.

4. BETWEEN A CONVENTION AND A NON-BINDING INSTRUMENT

4.1 Sources of International Law Recalled

Article 38(1) of the ICJ Statute outlines three main sources of international law, namely conventions, custom, and general principles of law. The text of this provision contains nothing to suggest that there is any hierarchy between the above sources of law, or that any one of them is less important than the other. Hence, it can be stated that custom and general principles of law are equal, in normative terms, to conventions insofar as their status as sources of international law is concerned. An important difference, however, lies in the fact that conventions are based on the consent of States, as contracting parties to international agreements, to accept certain duties and to recognize certain entitlements arising from that agreement. Accordingly, a rule of treaty law takes effect after the terms of convention have been agreed to by the parties, and this can occur immediately.

By contrast, customary law evolves through the general and consistent practice of States coupled with the belief that the practice is based on a legal obligation. But this does not exclude that a rule of customary law can develop quickly, even spontaneously, in response to a new situation.[437] Another difference between customary law and treaty law is that the former evolves through the recognition that the observance of a particular rule is required by law. Rules of treaty

[437] ILA, Statement of Principles, 731.

law, on the other hand, are developed to cover both specific rules and more general provisions that regulate the relevant conduct, and they draw their binding force from the contractual undertaking of the parties thereto.

General principles of law evolve by means of the recognition as an emanation of a general principle of law of certain general maxims of law. Accordingly, it differs from the development of rules of custom which focus on particular rules. Moreover, unlike the rules of custom which are premised on the practice of States and international bodies, these general principles of law are drawn primarily from the extensive recognition of the relevant rules in domestic law and jurisprudence. It is thus from national forums that general principles of law derive their binding force.

Apart from custom and general principles of law, certain non-binding instruments of international law may be useful in the development of legal norms. Although, as has been stated above,[438] these non-binding instruments are not enumerated as formal sources of international law in Article 38(1) of the ICJ Statute, it is possible to find a legal basis for their reliance.[439] The following sections explore certain non-binding instruments that have been important in the advancement of international law and in the articulation of subsequent practice of States. The examination of these instruments and the extent of the eventual adoption of their norms will provide key insights regarding the future of legal regulation of cyber operations.

4.2 The Progressive Codification of Minimum Humanitarian Norms

The Turku Declaration of Minimum Humanitarian Standards[440] was adopted in 1990 in response to the inadequacy of existing norms of international humanitarian law and human rights law in cases of internal crisis.[441] The Turku Declaration was drafted by a group of experts under the auspices of the Institute for Human Rights at Åbo Akademi University in Turku, Finland. The Turku Declaration outlined 18 Articles setting forth minimum humanitarian guarantees that should apply at all times, in all circumstances and to all actors in situations of violence.

---

[438] See Part 2 (Non-Conventional Sources of International Law).
[439] Hillgenberg, Fresh Look at Soft Law, 513.
[440] Declaration of Minimum Humanitarian Standards reprinted in UN Doc E/CN.4/Sub.2/1991/55, revised in 1994, UN Doc E/CN.4/1995/116.
[441] D Petrasek, 'Moving Forward on the Development of Minimum Humanitarian Standards' (1998) 92 *American Journal of International Law* 557, 558.

Despite the important contribution of the Turku Declaration, its legal effect was not significant, ostensibly because of its unofficial and non-binding nature.[442] Thus in 1991, in a bid to give it official and binding status, the Declaration was presented to the UN for examination and possible adoption. This was an initial step towards codifying the minimum humanitarian norms outlined in the Declaration. In 1994 the Declaration was transmitted to the Commission on Human Rights for detailed analysis and revision with a view to adopting the revised version as a UN document. Subsequently, the Declaration was shelved by the Commission which opted instead to initiate formal negotiations on a proposed convention on minimum humanitarian norms to be adopted under the aegis of the UN.

The Commission therefore requested governments, intergovernmental organisations and non-governmental organisations to provide their views on the norms set forth in the Turku Declaration. In 1996 a meeting was subsequently held in Cape Town, where the participants discussed the Declaration and presented their suggestions for improvement to the Commission. In 1997 the Commission requested the Secretary-General of the UN, in conjunction with the ICRC, to prepare an analytical report of minimum humanitarian standards that would form the basis of consultations with States and non-State entities.

The resulting consultations saw the submission of several comments, observations and analytical reports for consideration. However, the current status of a future treaty on minimum humanitarian norms can best be described as dormant. In fact, it has even been observed that the Turku Declaration "seems to have reached an impasse, with no apparent movement being made on progressing the document to the stage of an official declaration."[443] Therefore, in terms of advancing norms that can bind the conduct of State and non-State actors, the performance of the codification approach has been dismal.

4.3 The Successful Evolution of Norms regarding Armed Conflict at Sea

The Naval Warfare Manual, a non-binding instrument that was adopted in June 1994 by a group of experts, sought to update the international law applicable to armed conflicts at sea. This Manual is a good example of a success story in terms of developing new norms of international law. The Naval Warfare Manual, like the Turku Declaration, was the product of a long-term

---

[442] Ibid.

[443] E Crawford 'Road to Nowhere? The Future for a Declaration on Fundamental Standards of Humanity' (2012) 3(1) *Journal of International Humanitarian Legal Studies* 43, 48-49.

expert-driven project. But it differs from the Declaration in an important respect; it was never transmitted to the UN treaty-making system and thus could not claim any official status.

And yet, currently the Naval Warfare Manual is generally regarded as "the most comprehensive … enunciation of the international law applicable at sea."[444] The rules set out in the Manual have been adopted in the national military manuals of several States, and they are considered to be an accurate restatement of customary norms applicable to naval warfare.[445] Examples of nations that have incorporated the content of the Naval Warfare Manual into their military manuals include Germany,[446] Canada,[447] the United Kingdom,[448] and the United States.[449]

A crucial aspect of the approach taken by the drafters of the Naval Warfare Manual that may have been the key to its comparative success in the evolution of international norms on armed conflict at sea is the decision to keep it as a non-binding instrument.[450] Doswald-Beck, the editor of the Manual, explains the key rationale behind that decision:

> 'In view of uncertainty in the law, the participants decided that it was premature to think in terms of a draft treaty, and that a type of successor to the Oxford Manual of 1913 would be more appropriate and should in itself promote comprehension of contemporary law'.[451]

4.4 Comparative Observations

The evolution of new norms to govern the conduct of armed conflict at sea by way of an independent, expert-driven process is certainly admirable. But what is more remarkable is the fact that binding norms have since developed as evidenced by State practice, which has been uniform and representative. The success of the Naval Warfare Manual in this regard contrasts sharply with the convoluted and ultimately unproductive road taken by the UN process towards the codification of minimum humanitarian norms in the form of an international convention.

---

[444] JA Roach, 'The Law of Naval Warfare at the Turn of Two Centuries' (2000) 94 *American Journal of International Law* (2000) 64, 67.
[445] Ibid at 67.
[446] German Federal Ministry of Defence, *Manual of Humanitarian Law in Armed Conflicts*, VR II 3, DSK VV207320067, Zdv 15/2 (1992) at 97-112.
[447] Canada, Office of the Judge Advocate General, *Law of Armed Conflict at Operational and Tactical Levels*, B-GJ-005-104/FP-021 (2001).
[448] UK Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, JSP 383 (2004).
[449] US Navy/US Marine Corps/US Coast Guard, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M/MCW P 5-12.1/COMDTPUB P5800.7A (2007).
[450] L Doswald-Beck, 'The San Remo Manual on International Law Applicable to Armed Conflicts at Sea' (1995) 89 *American Journal of International Law* 192, 194.
[451] Ibid at 208.

Indeed, while the UN treaty-making process has taken more than twenty years with little to show in terms of norm advancement, the rules set forth in the Naval Warfare Manual only took seven years to be adopted in a national military manual. Moreover, unlike the UN treaty-making process, the drafting of the Naval Warfare Manual was more systematic and efficient.

The fact that the non-binding rules set forth in the Naval Warfare Manual have since been adopted in the operational manuals of some militarily significant States further reinforces its legal effect, demonstrating the potential of non-binding instruments.[452] Therefore, the comparative success of the Naval Warfare Manual (an expert-driven, non-binding instrument that was not submitted to the UN) shows that the eventual evolution of norms is not determined by whether or not they derive from the UN machinery, but by the actual practice of States.

In light of the above, the adoption of the Tallinn Manual should be seen as a first step in the process of developing cyber-specific norms. However, it must be emphasized that it is crucial for States and other subjects of international law, such as international organizations, to express their acceptance of these norms in order for them to acquire binding force. Cyber-specific norms should therefore be allowed to develop over time so as to sediment into either rules of customary law or to be recognized as an emanation of general principles of law.

A promising suggestion for the development of cyber-specific norms is the requirement of justification for every course of action at the operational level.[453] Legal writers have argued that new norms may evolve through the implementation of processes requiring commanders and other superiors to consider the legal implications of a cyber operation.[454] Once the parameters of the respective rights, responsibilities and remedies of various international actors is sufficiently clarified by practice, then the ultimate objective of codification in the form of a treaty can be meaningfully pursued.

---

[452] Crawford (n 443) 68.
[453] JTG Kelsey, 'Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 *Michigan Law Review* 1427, 1450.
[454] O'Donnell & Kraska (n 11) 149.

5. LEGAL AND POLICY CRITIQUES OF A PROPOSED CONVENTION

There is general consensus that the use of cyber operations in international relations are subject to the constraints of international law.[455] Moreover, there is general agreement that certain norms that are cyber-specific should be identified in order to effectively regulate certain aspects that are unique to cyber operations.[456] However, there is little guidance on how, when, and the extent to which these operations are subject to existing norms.[457] The question of the appropriate method to resolve the insufficient legal regulation of cyber operations is contentious; there are two schools of thought.

First, there are those who advocate the adoption of a convention to govern the rights, duties, and remedies related to the conduct of cyber operations.[458] Secondly, there are those who reject the utility or viability of a convention, arguing instead for the need to allow cyber-specific norms to develop and be shaped via practice, ultimately leading to codification.[459] Both of these standpoints have some merit and thus deserve to be objectively examined in order to determine the best way forward as regards the future legal regulation of cyber operations.

5.1 Conventional Limitation of Not-yet-Known Capabilities

The introduction of cyber operations into the arena of war-fighting is still a relatively novel phenomenon.[460] Consequently, its disruptive and destructive capacity has yet to be fully understood because operational practice is sparse, a view that has been acknowledged by some legal writers:

> 'Visible or readily discernible state practice is still scarce. The military potential of computer network attacks is now only starting to be fully explored, and it is difficult to assess how realistic

---

[455] ET Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford Journal of International Law* 207; RD Scott, 'Legal Aspects of Information Warfare: Military Disruption of Telecommunications' (1998) 45 *Naval Law Review* 57, 59.

[456] Department of Defense, Office of General Council, *An Assessment of International Legal Issues in Information Operations* (1999) 11: "There are novel features of information warfare that will require expansion and interpretation of established principles of the law of war."

[457] See K Dörmann, *Computer Network Attack and International Humanitarian Law*, International Committee of the Red Cross, 19 May 2001, para 29.

[458] DB Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 *Lewis and Clarke Law Review* 1023; AJ Schaap, 'Cyberwarfare Operations: Development and Use under International Law' (2009) 64 *Air Force Law Review* 121.

[459] Kelsey (n 453) 1450.

[460] Roscini (n 4) 41.

> or likely the theoretical worst-case scenarios that are contemplated in the literature—e.g. the manipulation of a nuclear power plant via cyberspace—really are'.[461]

Given the limited information relating to the military utility of cyber operations, it would seem unwise to seek to restrict the ability to use potentially advantageous cyber capabilities by means of an international convention.[462] This view finds support in the historical reluctance with which certain States accepted the restrictions of nuclear non-proliferation treaties. The unlikelihood of States yielding to the strictures of treaty law is also supported by the unique character of cyber operations which allows States to "defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military … legal and illegal."[463]

But on the other hand, some States may find it expedient to accept the restrictions imposed by a multilateral convention on cyber warfare.[464] This is particularly true for developed nations such as the United States which possesses the strongest cyber warfare capabilities and at the same time is predisposed to a high level of vulnerability to cyber attack due to its significantly heavy reliance on technology.[465] One legal writer explains the rationale for this: "when operational vulnerabilities outweigh the expected technical advantage, it would be more prudent to advocate an outright ban or strict controls on the cyber weapons."[466]

However convincing the above proportionality rationale may be, its persuasive effect pales in comparison to the unique attributes of cyber capabilities and their operational significance.[467] An economy of force analysis coupled with the notorious anonymity of cyber operations will recommend such operations to States for two reasons. First, it will afford States the opportunity to expend the least possible time, casualties, and material resources. Secondly, it will shield the State from taking responsibility for its acts because of the difficulty in attributing the offending conduct to the concerned State.[468] These are powerful incentives for States not to accept any

---

[461] R Geib, 'The Conduct of Hostilities in and via Cyberspace', War and Law in Cyberspace Panel, *American Law in Society Proceedings*, 2010, p. 372.
[462] BW Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?* (2001) 14.
[463] O'Donnell & Kraska (n 11) 148.
[464] Kelsey (n 453) 1449.
[465] Muir (n 263) 11.
[466] Ellis (n 462) 14.
[467] Roscini (n 4) 41; Kelsey (n 453) 1449.
[468] S Kirchener, 'Distributed Denial-of-Service Attacks under Public International Law: State Responsibility in Cyber War' (2009) 8 *The IUP Journal of Cyber Law* 14.

form of limitation of the use of cyber weapons by means of treaty law because that would foreclose vital military advantage. But there is also the possibility that States may negotiate a weak treaty, sign it then subsequently ignore it.

Even assuming that some States may welcome the restriction of State cyber conduct by means of treaty law, the prospect of regulating a phenomenon whose capacity to kill, injure or destroy is not yet fully known will be problematic. Indeed, it is unlikely that a law can sufficiently address practical aspects of a new and developing form of warfare that has rarely been deployed and whose possible effects have not been fully understood. In light of the numerous and under-explored capabilities of cyber weapons it is doubtful whether States would agree to limit, by means of an international convention, "the use of a new weapon when so little is known about its full capabilities."[469]

Nonetheless, it must be emphasized that the adoption of an international convention on cyber warfare should not be considered an exercise in futility. But while it cannot be categorically excluded that the conclusion of an international treaty on cyber warfare may improve its effective legal regulation,[470] absent any indication that the cyber rights and responsibilities of various concerned subjects of international law have been fully understood such a move would certainly be premature.

5.2 Asymmetry Concerns

A related concern that is likely to impede efforts to conclude a meaningful convention to govern cyber operations under international law is the relative asymmetry between the capabilities and vulnerabilities of individual nations.[471] This can be illustrated by taking two hypothetical States, A and B, and considering their asymmetrical positioning. State A has preeminent cyber capabilities and its well-developed economy is highly dependent on information technologies. For its part, State B is less developed but highly militarized and has acquired significant cyber warfare capabilities. Consider then a scenario where the two nations are involved in a dispute in which recourse is made to cyber operations.

---

[469] Kelsey (n 453) 1449.
[470] Shackleford & Andres (n 278) 971.
[471] Muir (n 263) 7.

State B conducts a cyber operation targeting the commercial capital of State A, shutting down its power grid, disrupting all aerial and railway communications, and in the process causing death, injury and destruction of property. This would be disastrous for State A since its highly networked and technology-dependent economy is at the same time its most dangerous vulnerability.[472] However, if State A conducts a similar operation against State B, its net effect would be comparatively insignificant.

In light of the above, the critical issue to be considered is whether State B is likely to bind itself to a treaty that bans or restricts the use of cyber warfare capabilities. The answer to this is, in all probability, negative because the absence of any treaty prohibition of cyber weapons offers State B strategic military advantage by availing a tool that "cannot similarly be effectively deployed against it."[473] This rationale also finds support in the fact that less developed States will not willingly foreclose "an opportunity to achieve a measure of parity with wealthy states through the development of cyber weapons."[474] Indeed, cyber technologies are relatively cheap and easy to acquire, thereby allowing weaker States and non-State actors to "potentially cause considerable damage to countries with superior conventional military power."[475] This is an advantage that will very unlikely be given up by many nations.[476]

It may well be in the strategic interest of some nations to agree to treaty norms which restrict the range of permissible cyber conduct that they can engage in. This will entail the acceptance of norms prescribing that certain conduct is prohibited, with the consequence of attaching State responsibility. Yet State engagement in some prohibited cyber conduct may actually be beneficial. Indeed, it has been observed that "some prohibited uses of cyber weapons offer states the possibility of dealing blows to an enemy with a low cost in human life and possibly little physical damage to civilian objects."[477]

5.3 False and Fallible Analogies

The relative novelty of military operations conducted in cyberspace and the absence of specific provisions to guide this phenomenon invariably leads those seeking to identify applicable rules

---

[472] Ellis (n 462) 14.
[473] Muir (n 263) 8.
[474] Kelsey (n 453) 1449.
[475] Roscini (n 4) 2.
[476] Muir (n 263) 8.
[477] Kelsey (n 453) 1447.

to draw analogies from the existing law.[478] Cyber operations challenge these analogies fundamentally.[479] When existing rules and principles are sought to be extended to new contexts little account is often taken of the uniqueness of the new scenario. The resulting rules will thus prove to be too general.[480] In the case of cyberspace, many of the traditional international law concepts that were developed to regulate the physical domain may not offer the most insightful of analogies.

Consider the case of cyber operations and the concepts of territorial sovereignty and jurisdiction. It is undeniable that these concepts certainly extend to the cyber realm, but what is less clear is whether an attempt to identify cyber-specific rules by way of analogy will be productive.[481] Unlike the physical domain of war-fighting, cyberspace consists of a physical and a non-physical element.[482] The physical element of cyberspace denotes the "physical infrastructure through which the data travel wired or wireless, including servers, routers, satellites, cables, wires, and the computers, while the [non-physical element] includes the protocols that allow data to be routed and understood, as well as the software used and the data."[483]

In light of the sophisticated inter-connectivity of cyberspace, analogy with the notion of territory is bound to be problematic. Although the effects-based identification of a target State is fairly uncontroversial,[484] the difficulty lies in ascertaining the origin of the attack.[485] The structure of the internet impedes detection and attribution, thus making certain analogies with the physical domain unconvincing. Lessons from actual cyber incidents indicate that some analogies can be inaccurate at best and misleading at worst: "[c]overing one's fingerprints and footprints online is relatively simple, compared to getting rid of physical evidence. IP addresses can be

---

[478] DJ Betz & T Stevens, 'Analogical Reasoning and Cyber Security' (2013) 44 *Security Dialogue* 151.
[479] Muir (n 263) 6.
[480] Roscini (n 4) 23.
[481] WH von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *International Law Studies* 126.
[482] Betz & T Stevens (n 478) 151.
[483] Roscini (n 4) 24.
[484] Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, *Joint Terminology for Cyberspace Operations* (2010) 14.
[485] J Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 *European Journal of International Law* 133.

spoofed, an attack that appears to come from one place, may actually originate somewhere else."[486]

Attempts to draw general analogies between kinetic warfare and cyber warfare with a view to deriving binding norms is also likely to be hampered by the fact that different interests dictate varying approaches. For instance, there is likely to be sharp difference of opinion over the proper classification of cyber conduct as ordinary crime or violations of the *jus ad bellum* and the *jus in bello*. The consequences of categorizing cyber attacks as violations of the latter are so severe compared to criminal law violations "that an impasse in selecting the appropriate choice of laws could derail the entire negotiation."[487] Further dispute will likely arise between nations that will seek to avoid classification of certain conduct as hostile acts rendering them targetable and nations that may not be opposed to treaty regulation, in principle, but which may "wish to reserve the ability to address cyber attacks with a military response."[488]

5.4 Attribution and Inconclusive Evidentiary Standards

The fundamental challenge posed by attribution to the effective operation of the rules of international law has been acknowledged by the ICJ in its *Nicaragua* Judgment, where the problem was identified as being not in the legal process of imputing the conduct to a particular State, but rather in "the prior process of tracing material proof of the identity of the perpetrator".[489] The problem of attribution becomes all the more apparent in cyber operations, where identifying the author of a particular attack is impeded by significant technical problems.[490]

More specifically, authors of cyber attacks can conduct surreptitious operations and effectively deploy their expertise to dissimulate their identities and avoid detection.[491] A good example that illustrates the challenge of identifying the perpetrator or origin of a cyber attack is the Stuxnet incident, where Iranian nuclear centrifuges were targeted.[492] Studies by several cyber security experts have not definitively pinpointed the nation responsible for the attack or even

---

[486] C Farivar, *Cyberwar I: What the Attacks on Estonia Have Taught Us About Online Combat*, Slate, May 22, 2007, http://www.slate.com/id/2166749/; Kelsey, Hacking Into IHL, 1446.
[487] Muir (n 263) 7.
[488] Ibid.
[489] *Nicaragua*, para 57.
[490] Roscini (n 4) 33.
[491] Schackleford (n 20) 204; Muir (n 263) 9.
[492] See Chapter I, section 2.2.3; Muir (n 263) 9.

identified the target. This indicates that the element of identification presents a technical challenge in the cyber context, but it does not suggest that it is impossible to identify authors of hostile cyber actions.[493]

Rather, the technical difficulty of identifying cyber attackers in cyberspace, like the case in other comparable scenarios, reflects the challenge of extending existing rules to new contexts.[494] It therefore reinforces the view that rather than codifying contentious and untested cyber-specific norms, it would be more productive to analyze developments in computer technology and the practice of States as derived from national internet regulation.[495] This will inform the specific norms relative to the relevant material proof that should be used in the identification of perpetrators of cyber attacks.[496] Moreover, meaningful norms can only evolve by reference to practice as opposed to stipulation in treaty form because the relevant tools for easier identification are still being developed.[497]

The technical problem of identifying cyber attackers and attributing responsibility cannot in itself satisfactorily explain the preference for the progressive evolution of cyber-specific norms through practice over their immediate stipulation in treaty form.[498] But the legal problem of specifying the attribution criteria and its corresponding standard of evidence certainly can.[499] More specifically, there is much disagreement over the requisite level of State control for responsibility to attach and the prosecutorial burden of proof.[500] At present, it has not been settled whether the appropriate level of State control is that of overall control or effective control.[501] Similarly, it remains unclear whether culpability should be proved beyond any reasonable doubt or beyond any doubt.[502]

The Tallinn Manual does not take a clear position as regards the contentious issues surrounding attribution and the correlative burden of proof.[503] Although regrettable, this decision is understandable since the Tallinn Manual was not intended to stipulate any hard and fast rules

[493] Roscini (n 4) 33.
[494] UN Doc/A/66/152, 15 July 2011, p 18.
[495] US Department of Defence, Cyberspace Policy Report, 4.
[496] Dinstein (n 58) 112.
[497] Kesan & Hayes (n 63) 482.
[498] Roscini (n 4) 33.
[499] Shackleford & Andres (n 278) 990.
[500] Muir (n 263) 10.
[501] *Nicaragua* judgment, para 115; *Tadic*, paras 131, 145.
[502] *Genocide* judgment, paras 403-405.
[503] Tallinn Manual (n 8) Rule 6, para 10; Tsagourias (n 62) 32.

in this regard, but only to outline generally accepted principles of law and to "capture all reasonable positions" in its commentary.[504]

5.5 Problematic Enforcement

The efficacy of any ban or conditional restriction imposed by international treaties on the use of certain weapons turns significantly on enforcement. As has been stated (5.4), the attribution of cyber operations to a State poses fundamental challenges to effective enforcement.[505] First, the unique nature of cyber warfare means that it requires a different approach and special expertise in order to understand fully the contours of the rights, responsibilities, and remedies involved.[506]

Secondly, it is not easy to ascertain whether, in fact, an international wrongful act has been committed when cyber operations are resorted to.[507] Even where it is possible to find a violation of international law, an additional challenge remains: the problem of attribution. The inherent interconnectivity of the internet effectively makes cyberspace an environment conducive for anonymous cyber conduct designed to avoid detection. It has been observed that "the internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work."[508] This poignantly highlights the difficulty with which the current enforcement machinery of international law will have to contend with, and it is submitted that the present capacity for enforcement is insufficient.

Thirdly, the primary judicial enforcement machinery of international law is currently the jurisdiction of the ICJ, which is limited in expertise on the technical issues surrounding cyber operations.[509] One of the key cyber challenges that will likely impede the efficacy of the current enforcement mechanism of international law is the issue of jurisdiction,[510] a challenge

---

[504] Ibid at 6.
[505] Tsagourias (n 62) 234.
[506] Kelsey (n 453) 1450.
[507] The problem of uncertainty surrounding conclusive attribution similarly challenges the determination of whether an international wrongful conduct has occurred. See Article 55, Articles on the Responsibility of States for Internationally Wrongful Acts (2001).
[508] J Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (2011) 32.
[509] Brown (n 423) 213-14; Kelsey (n 453) 1450.
[510] T Scassa & RJ Currie, 'New First Principles? Assessing the Internet's Challenges to Jurisdiction' (2011) 42 *Georgetown Journal of International Law* 1079.

recognized by United States Department of Defence: "[t]he long distance and anonymous nature of computer network attacks may make detection and prosecution unlikely".[511]

Finally, the fact that there is an increasing number of non-State entities that have acquired significant cyber warfare capabilities coupled with their well known non-compliance with international restrictions makes it all the more difficult to enforce any conventional prohibitions.[512] Indeed, States will invariably reject any treaty provision that constrains their cyber action against non-State actors who disregard prohibitions imposed by that treaty.[513]

6. The Case for Alternative Avenues for Norm Evolution

The conclusion of a treaty regulating State cyber conduct may provide definitive guidance on the expectations of nations facing the threat of, or contemplating launching, cyber operations. However, the international law-making process has its own barriers that may prevent timely and meaningful codification of cyber-specific norms.[514] Presently, it is reasonable to state that the codification of new norms to govern cyber operations in the form of an international convention is neither viable nor desirable.[515]

The better approach would be for the international legal community to continue the journey that was began by the drafting of the Tallinn Manual, and to embark on a more consultative and representative exercise (say under the auspices of the United Nations) with a view to collating views of a broader constituency of States and non-State actors. The next step should be to distil the general rules and principles of international law and to apply them in the specific context of cyber operations, with all the necessary modifications. These rules and principles can then be expressed in the form of a non-binding instrument adopted by one of the organs of the United Nations.

Having been adopted by a wide constituency and with the additional legitimacy of an instrument adopted under the auspices of the United Nations, the norms set forth in the non-binding instrument will likely gain extensive acceptance. The cyber-specific norms can then be

---

[511] Department of Defence, Assessment, 8.
[512] VM Padmanabhan, 'Cyber Warriors and the *Jus in Bello*' (2013) 89 *International Law Studies* 296; JA Lewis, 'The "Korean" Cyber Attacks and Their Implications for Cyber Conflict' (2009) 8 Centre for Strategic and International Studies.
[513] Ellis (n 462) 14.
[514] Muir (n 263) 8.
[515] Kelsey (n 453) 1449.

expanded and clarified via the process of State practice, whether by means of national legislation, general codes of conduct, or articulation in military manuals and operational rules of engagement.[516] This process of the evolution of cyber-specific norms will have the unique advantage of a bottom-up approach to the emanation of customary norms and general principles of law that are derived from actual practice.[517]

It is nonetheless important to acknowledge the positive effect of treaty norms in the effective regulation of warfare capabilities. Unlike the formation of cyber-specific norms through the formation of a customary rule or via the emanation of a general principle of law, the articulation of treaty norms will be much clearer, more systematic, and arguably more efficient. However, it is useful to recall that the unique nature of cyber weapons and cyberspace; in contrast to kinetic weapons that are deployed in the physical domain (land, air, sea, and space), the potential consequences of cyber operations in networked environments is not yet fully known. This makes it difficult to develop precise rules by means of a treaty.[518]

Therefore, it will be far more prudent to set in motion a process that will see cyber-specific norms develop over time and be clarified through practice.[519] It can thus be concluded that instead of relying on a treaty to found new norms to govern the conduct of cyber operations, cyber-specific norms should evolve primarily through consistent and representative practice. At present, however, it would be premature to attempt to articulate norms to conclusively govern activity in cyberspace which will invariably continue to evolve.[520]

7. CONCLUDING OBSERVATIONS

This Chapter has discussed two different approaches to the development of international legal norms: treaty and practice. It has shown that the latter approach has been comparatively more successful than the former, in large part, because it is free from political and other institutional hurdles. After discussing the merits and demerits of both approaches, it has demonstrated that the challenges that will likely encumber a proposed treaty on cyber operations will render it ineffective.

---

[516] Ibid.
[517] B Cheng, *General Principles of Law as Applied by International Courts and Tribunals* (2006) 23-24.
[518] HM Government (n 31) 29.
[519] GK Walker, 'Information Warfare and Neutrality' (2000) 33 *Vanderbilt Journal of Transnational Law* 1079, 1200-01.
[520] HM Government (n 31) 29.

The approach that I have argued for been endorsed in this Chapter is to let cyber-specific norms develop, gain wide acceptance, and be clarified through the process of practice. This argument has been put forth on the basis that the emergence of cyber-specific norms through the channels of custom, the emanation of general principles of law, or edicts of military law and conduct would have a better prospect of advancing the legal regulation of cyber warfare than via treaty law. This is primarily because the process will not only secure the credibility and legitimacy of the final product, but it would also be free of the challenges that are likely to prevent the drafting of a meaningful treaty. Moreover, because neither the potential of cyberspace operations nor the pace of technological development can be predicted, it is far more appropriate to progressively develop cyber-specific norms on a case-by-case basis in the context of practice.

Chapter V

CONCLUSION

1. Introduction

The utility of cyber space as a platform for waging warfare presents numerous challenges to current international law. Indeed, the increasing use of cyber operations brings with it some unique difficulties because the existing rules do not provide specific rulings on the application of the current law to the emergent aspects of these new forms of warfare. This situation is further complicated by the fact that the legal regulation of certain aspects of the use of force and armed conflict are not well settled, even in the context of kinetic operations. Hence, the resulting ambiguity makes it difficult for parties to a cyber incident to determine with certainty what the specific rules are that should guide their conduct.

Recognizing that technological changes in general and the hostile use of cyber operations in particular pose a significant challenge to the current international law, the Tallinn Manual was drafted to provide some clarity in this regard. In particular, the Manual sought to elaborate how current international law applies to cyber operations in terms of the *jus ad bellum* (the law on the use of force) and the *jus in bello* (the law of armed conflict). This dissertation has examined selected aspects of the Manual and consequently suggested how the overall legal regulation of cyber operations can be improved.

2. Concluding Observations

This research has focused on the Rules of the Tallinn Manual with a view to reviewing its content and to suggest how cyber-specific norms can develop. Its analysis of certain Rules of the *jus ad bellum* and the *jus in bello* has shown some progressive aspects of the Manual, but has also revealed that the Manual only partially addresses, or does not at all, address some critical legal issues. This is problematic because the fundamental issues which the Manual was supposed to clarify have only been discussed superficially. For instance, the Manual and particularly the commentary fails to discuss in sufficient detail the legal issues surrounding attribution and the relevant evidentiary standard. This illustrates how difficult it will be for States to draw any practical guidance regarding this legal issue.

In light of the normative deficiencies of the Tallinn Manual, this research explored a comparative approach whereby the future of legal regulation of cyberspace operations was mapped on the experience of other non-binding instruments of international law. It was shown that the Manual follows the trends set by earlier instruments, and like its predecessors, it can supply the basis for the emergence of binding norms. The discussion in this research compared two different approaches to the development of international legal norms, namely codification under the auspices of the United Nations and the evolution of norms through State practice. This entailed a comparison of the relative successes of the Naval Warfare Manual and the Turku Declaration of Minimum Humanitarian Standards in terms of developing binding legal norms that are extensively accepted.

The historical development and subsequent practice of the above instruments reveals that there is a far better success rate when norms evolve through State practice than when they are codified in the form of international treaties. In particular, the adoption of the norms set forth in the Naval Warfare Manual has by far been more successful than the case with the Turku Declaration, in large part, because its norm-development process was free from political and other institutional hurdles. On the basis of its critical analysis of the merits and demerits of a proposed international convention to govern cyber operations, this research concludes that these daunting challenges will likely encumber such a project rendering it ineffective. It would thus be undesirable to try and codify international rules for cyberspace, at least for the present time.

The better approach, which has been endorsed in this research, is to encourage cyber-specific norms to develop, gain wide acceptance, and be clarified through the process of practice. It has been systematically argued in this research that the emergence of cyber-specific norms through the means of custom, the emanation of general principles of law, or edicts of military law and conduct would have a much better prospect of advancing the international legal regulation of cyber warfare than through treaty law.

This is mainly because the process will not only secure the credibility and legitimacy of the final product, but it would also be free of the numerous and unresolved challenges that are likely to prevent the drafting of a meaningful convention. Moreover, because neither the (beneficial or harmful) potential of cyberspace operations nor the pace of technological development can be

predicted, it is far more appropriate to progressively develop cyber-specific norms on a case-by-case basis in the context of practice.

BIBLIOGRAPHY

Books and Book Chapters

A Aust, *Modern Treaty Law and Practice* (2013).

A Cassese, *International Law* (2005).

A Chayes, *The Cuban Missile Crisis: International Crises and the Role of Law* (1974).

A Randelzhofer, 'Article 2(4)' in B Simma (ed), *The Charter of the United Nations: A Commentary* (2002).

A Randelzhofer, 'Article 51' in B Simma (ed), *The Charter of the United Nations: A Commentary* (2012).

AJK Bailes & A Wetter, 'Security Strategies' in *Max Planck Encyclopedia of Public International Law* (2012) Vol. IX.

A Klimburg (ed), *National Cyber Security Framework Manual* (2012).

B Cheng, *General Principles of Law as Applied by International Courts and Tribunals* (1987).

B Simma et al (eds), *The Charter of the United Nations* (2012).

BW Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?* (2001).

C Gray, *International Law and the Use of Force* (2008).

C Greenwood, 'Self-Defence' in *Max Planck Encyclopedia of Public International Law* (2012).

C Lotrionte, 'Active Defence for Cyber: A Legal Framework for Covert Countermeasures' in J Carr (ed), *Inside Cyber Warfare* (2012).

CD Guymon (ed), *Digest of United States Practice in International Law* (2012) 594.

D Albright, P Brannan & C Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Nantaz Enrichment Plant?* (2010).

D Fleck, 'Introduction' in D Fleck (ed), *The Handbook of International Humanitarian Law* (2013).

E Tikk et al, *Cyber Attacks against Georgia: Legal Lessons Identified* (2008) 5.

E Tikk, K Kaska & L Vihul, *International Cyber Incidents – Legal Considerations* (2010).

F Coomans & MT Kamminga, *Extraterritorial Application of Human Rights Treaties* (2004).

F Schreier, *On Cyberwarfare*, DCAF Horizon 2015 Working Paper (2012).

G Ress, 'Interpretation' in B Simma (ed), *The Charter of the United Nations – A Commentary, Volume I* (2012).

HH Dinniss, *Cyber Warfare and the Laws of War* (2012).

HHG Post, 'Some Curiosities in the Sources of the Law of Armed Conflict Conceived in a General International Law Perspective' in LANM Barnhoorn & KC Wellen (eds), *Diversity in Secondary Rules and the Unity of International Law* (1995).

I Brownlie, *Principles of Public International Law* (2008).

ICRC, *Basic Rules of the Geneva Conventions and their Additional Protocols – Understanding Humanitarian Law* (2009).

ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*.

J Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (2011).

J Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (2002).

J Healy & K Grindal (eds), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (2013).

J Healey & L van Bochoven, *NATO'S Cyber Capabilities: Yesterday, Today and Tomorrow* (2011).

J Richardson, *Stuxnet as Cyber Warfare: Applying the Law of War to the Virtual Battlefield* (2011).

J Ringmose & S Rynning, *Come Home, NATO! The Atlantic Alliance's New Strategic Concept* (2009).

JB Moore (ed), *International Law Digest* (1906).

J-M Henckaerts & L Doswald-Beck, *Customary International Humanitarian Law, Vol I: Rules* (2005) Vol I.

K Dörmann, *Computer Network Attack and International Humanitarian Law*, International Committee of the Red Cross, 19 May 2001.

K Dörmann, 'The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint' in K Byström (ed), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law* (2004).

K Zemanek, 'Armed Attack' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (2010).

LF Damrosch et al, *International Law: Cases and Materials* (2001).

M Bothe, 'Comments' in HHG Post (ed), *International Economic Law and Armed Conflict* (1994).

M Fitzmaurice & O Elias, *Contemporary Issues in the Law of Treaties* (2005).

M Ignatief, *Virtual War: Kosovo and Beyond* (2000).

M Roscini, *Cyber Operations and the International Law on the Use of Force* (2014).

M Rishmawi, *A Commentary on the United Nations Charter on the Rights of the Child, Article 4: The Nature of State Parties' Obligations* (2006).

M Wood, 'State Practice' in *Max Planck Encyclopedia of Public International Law* (2012) Vol IX.

MM Whiteman, *Digest of International Law* (1963) Vol. 1.

MN Schmitt & BT O'Donnell (ed), *Computer Network Attack and International Law* (2002).

MN Schmitt, HA Harrison-Dinniss & TC Wingfield, 'Computers and War: The Legal Battlespace' Background Paper for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law' (Cambridge 25-27 June 2004).

MN Shaw, *International Law* (2002).

N Cox, *Technology and Legal Systems* (2006).

N Lubell, *Extraterritorial Use of Force Against Non-State Actors* (2010).

N Melzer, *Cyber Warfare and International Law* (2011).

N Melzer, *Targeted Killing in International Law* (2008).

N Shachtman & PW Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cyber Security is Misplaced and Counterproductive', Brookings Institution, 15 August 2011.

N Tsagourias, 'The Tallinn Manual on International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' in TD Gill et al (eds), *Yearbook of International Humanitarian Law* (2012).

O de Frouville, 'Attribution: Private Individuals' in J Crawford *et al* (eds), *The Law of International Responsibility* (2010) 257-282.

P Berkowitz (ed), *Future Challenges in National Security and Law* (2011).

R Arnold & PA Hildebrand, *International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenges* (2005).

R Gardiner, *Treaty Interpretation* (2008).

R Garnett & P Clarke, 'Cyberterrorism: A New Challenge for International Law' in A Bianchi (ed), *Enforcing International Law Norms Against Terrorism* (2004).

R Heinsch, 'Methodology of Law-Making: Customary Law and New Military Technologies' in D Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (2013).

R Kolb & R Hyde, *An Introduction to the International Law of Armed Conflicts* (2008).

R Lehiten et al *Computer Security Basics* (2006).

S Haines, 'Weapons, Means and Methods of Warfare' in E Wilmshurst & S Breau (eds), *Perspectives on the ICRC Study on Customary International Humanitarian Law* (2007).

S Rosenne, *The Law and Practice of the International Court* (2006) 645.

S Skogly, *Beyond National Borders: States' Human Rights Obligations in International Cooperation* (2006).

SC Neff, *The Rights and Duties of Neutrals* (2000).

T Gazzini, *The Changing Rules on the Use of Force in International Law* (2006).

T Karimova, 'The Nature and Meaning of "International Assistance and Cooperation" under the International Covenant on Economic, Social and Cultural Rights' in E Reidel et al (eds), *Economic, Social and Cultural Rights: Contemporary Issues and Challenges* (2014).

T Treves, 'Customary International Law' in *Max Planck Encyclopedia of Public International Law* (2012).

U Haußler, *Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty* (2008).

WA Owens, KW Dam & HS Lin (eds), *Technology, Policy, Law, and Ethics Regarding US Acquisitions and Use of Cyberattack Capabilities* (2009).

WH Boothby, *Weapons and the Law of Armed Conflict* (2009 OUP).

Y Dinstein, 'Computer Network Attacks and Self-Defense' in MN Schmitt & B O'Donnell (eds), *Computer Network Attack and International Law* (2002).

Y Dinstein, *War, Aggression and Self-Defence* (2012).

Y Sandoz et al, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (1987).

Articles

AJ Schaap, 'Cyberwarfare Operations: Development and Use under International Law' (2009) 64 *Air Force Law Review* 121.

AT Guzman, 'Saving Customary International Law' (2005-2006) 27 *Michigan Journal of International Law* 151.

AM Weisburd, 'The International Court of Justice and the Concept of State Practice' (2009) 31(2) *University of Pennsylvania Journal of International Law* 295.

BT O'Donnell & JC Kraska, 'Humanitarian Law: Developing International Rules for the Digital Battlefield' (2003) 8 *Journal of Conflict and Security Law* 133.

C Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 541.

C Garraway, 'The Use and Abuse of Military Manuals' (2004) 7 *Yearbook of International Humanitarian Law* 431.

C Lotrionte, 'Active Defense for Cyber: A Legal Framework for Covert Countermeasures' in J Carr (ed), *Inside Cyber Warfare* (2012) 282.

CC Joyner & C Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 *European Journal of International Law* 825.

D Allan & C Brown, 'The *Mavi Marmara* at the Frontlines of Web 2.0' (2010) 40 *Journal of Palestinian Studies* 63.

D Brown, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harvard International Law Journal* 179.

D Brown, 'The Role of Regional Organizations in Stopping Civil Wars' (1997) 41 *Air Force Law Review* 235.

D Thurer, '"*Soft Law" – eine neue Form von Vlkerrecht?*' (1985) 104 *ZSchwR* 429-453.

D Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) *Journal of Conflict and Security Law* 279.

D Petrasek, 'Moving Forward on the Development of Minimum Humanitarian Standards' (1998) 92 *American Journal of International Law* 557.

DB Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 *Lewis and Clarke Law Review* 1023.

DE Graham, 'Cyber Threats and the Law of War' (2010) 4 *Journal of National Security Law and Policy* 87.

DJ Betz & T Stevens, 'Analogical Reasoning and Cyber Security' (2013) 44 *Security Dialogue* 151.

DJ Ryan et al, 'International Cyberlaw: A Normative Approach' (2011) 42 *Georgetown Journal of International Law* 1179.

DS Rudesill, 'Precision War and Responsibility: Transformational Military Technology and the Duty of Care under the Laws of War' (2007) 32 *Yale Journal of International Law* 517.

E Benari, 'Israel to Establish Cyber Warfare Administration', Israel National News, 13 January 2012.

E Crawford 'Road to Nowhere? The Future for a Declaration on Fundamental Standards of Humanity' (2012) 3(1) *Journal of International Humanitarian Legal Studies* 43.

E Wilmshurst, 'The Chatham House Principles of International Law on the Use of Force in Self-Defence' (2008) 55(4) *International and Comparative Law Quarterly* 963.

ET Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford Journal of International Law* 207.

F Khan, 'States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis' Institute of Strategic Studies Islamabad (ISSI) *available at* http://www.issi.org.pk/publicationfiles/1328592265_43276030.pdf.

Forum: 'Direct Participation in Hostilities: Perspectives on the ICRC Interpretive Guidance' (2010) 42 *New York University Journal of International Law and Policy* 637.

GK Walker, 'Information Warfare and Neutrality' (2000) 33 *Vanderbilt Journal of Transnational Law* 1079, 1200-01.

H Hillgenberg, 'A Fresh Look at Soft Law' (1999) 10 *European Journal of International Law* 499-515.

H Koh, 'International Law in Cyberspace' (2012) *Harvard International Law Journal* 3.

H Koh, Legal Adviser, US Department of State, 'International Law in Cyberspace', Speech at USCYBERCOM Inter-Agency Legal Conference, 18 September 2012.

I Traynor, 'Russia Accused of Unleashing Cyber War to Disable Estonia', The Guardian, 17 May 2007: www.theguardian.com/world/2007/may/17/topstories3.russia.

J Arato, 'Subsequent Practice and Evolutive Interpretation: Techniques of Treaty Interpretation over Time and their Diverse Consequences' (2010) 9 *The Law and Practice of International Courts and Tribunals* 434.

J Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 *European Journal of International Law* 133.

J Kelsey, 'Hacking into International Humanitarian Law' (2008) 106 *Michigan Law Review* 1434.

JA Lewis, 'The "Korean" Cyber Attacks and Their Implications for Cyber Conflict' (2009) 8 Centre for Strategic and International Studies.

JA Ophardt, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 *Duke Law and Technology Review*.

JA Roach, 'The Law of Naval Warfare at the Turn of Two Centuries' (2000) 94 *American Journal of International Law* (2000) 64.

JB Bellinger & WJ Haynes, 'A US Government Response to the International Committee of the Red Cross Study on Customary International Humanitarian Law' (2007) 89 *International Review of the Red Cross* 445.

JC Woltag, Computer Network Operations below the Level of Armed Force' (2011) ESIL Conference Paper no 1/2011, 16-17.

JP Kesan & CM Hayes, 'Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace' (2011-2012) 25 *Harvard Journal of Law and Technology* 482.

JTG Kelsey, 'Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 *Michigan Law Review* 1427.

L Doswald-Beck, 'San Remo Manual on International Law Applicable to Armed Conflict at Sea' (1995) 35 *International Review of the Red Cross* 583-587.

L Henkin, 'The Reports of the Death of Article 2(4) Are Greatly Exaggerated' (1971) 65 *American Journal of International Law* 544.

L Zhang, 'A Chinese Perspective on Cyber War' (2012) 94 *International Review of the Red Cross* 805.

LL Muir, 'The Case Against an International Cyber Warfare Convention' (2011) 2 *Wake Forest Law Review* 5.

LR Blank, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 *International Law Studies* 437.

M Landler & J Markoff, 'Digital Fears Emerge after Data Siege in Estonia' New York Times, 29 May 2007, at A1.

M Milanovic, 'State Responsibility for the Acts of Non-State Actors: A Comment on Griebel and Plücken' (2009) 22 *Leiden Journal of International Law* 315.

M Roscini, 'World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 114.

MC Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 *Yale Journal of International Law* 437.

MC Waxman, 'Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions' (2013) 89 *International Law Studies* 116.

ME O'Connell & L Arimatsu, 'Cyber Security and International Law', p 9 International Law Meeting and Summary, held on 29 May 2012.

MJ Skelrov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1.

ML Movsesian, 'Judging International Judgments' (2007) 48 *Virginia Journal of International Law* 65.

MN Schmitt, 'Classification of Cyber Conflict' (2012) 17(2) *Journal of Conflict and Security Law* 245.

MN Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 929.

MN Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (2011) 56 *Villanova Law Review* 569.

MN Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 *New York University Journal of International Law and Policy* 697.

MN Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed' (2012) 54 *Harvard International Law Journal Online* 24.

MN Schmitt, 'War, Technology and International Humanitarian Law' HPHPCR, Occasional Paper Series 4 (2005) 43.

N Falliere, LO Murchu & E Chien, 'W32.Stuxnet Dossier', *Symantec Security Response Whitepaper*, Version 1.4, 11 February 2011.

N Tsagourias, 'Cyber Attack, Self-Defence and the Problem of Attribution' (2012) 17(2) *Journal of Conflict & Security Law* 233.

OA Hathaway et al, 'The Law of Cyber Attack' (2012) *California Law Review* 4.

R Bernhardt, 'Evolutive Treaty Interpretation, Especially of the European Convention on Human Rights' (1999) 42 *German Yearbook of International Law* 15.

R Geib, 'The Conduct of Hostilities in and via Cyberspace', War and Law in Cyberspace Panel, *American Law in Society Proceedings*, 2010.

R Ingber 'Untangling Belligerency from Neutrality in the Conflict with Al Qaeda' (2011) 47(1) *Texas International Law Journal* 75.

R Liivoja & TH McCormack, 'Law in the Virtual Battlespace: The Tallinn Manual and the *Jus in Bello*' (2013) Melbourne Legal Studies Research Paper No. 650.

RD Scott, 'Legal Aspects of Information Warfare: Military Disruption of Telecommunications' (1998) 45 *Naval Law Review* 57.

RE Overill, 'Reacting to Cyber-intrusions: Technical, Legal and Ethical Dimensions' (2003) 11 *Journal of Financial Crime* 163.

S Brenner, '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare' (2007) 97 *Journal of Criminal Law and Criminology* 379, 384-86.

S Kirchener, 'Distributed Denial-of-Service Attacks under Public International Law: State Responsibility in Cyber War' (2009) 8 *The IUP Journal of Cyber Law* 14.

SD Watts, 'Combatant Status and Computer Network Attack' (2010) 50 *Virginia Journal of International Law* 405.

SD Watts, 'Low-Intensity Computer Network Attack and Self-Defense' (2011) 87 *International Law Studies* 70.

SJ Shackleford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27(1) *Berkley Journal of International Law* 192.

SJ Shackleford & RB Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 *Georgetown Journal of International Law* 971.

SP Knauck, 'Information Warfare: New Challenges for Public International Law' (1996) 37 *Harvard International Law Journal* 272–292.

SW Brenner, '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare' (2006-07) 97 *Journal of Criminal Law and Criminology* 402.

T Check, 'Analyzing the Effectiveness of the Tallinn Manual's *Jus ad Bellum* Doctrine on Cyber Conflict: A NATO-centric Approach' 6.

T Scassa & RJ Currie, 'New First Principles? Assessing the Internet's Challenges to Jurisdiction' (2011) 42 *Georgetown Journal of International Law* 1079.

WH Taft, 'Self Defense and the Oil Platforms Decision' (2004) 29 *Yale Journal of International Law* 295.

WH von Heinnegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *International Law Studies* 126.

WJ Lynn, 'Defending a New Domain: The Pentagon's Cyber Strategy' (2010) September/October 97.

VM Padmanabhan, 'Cyber Warriors and the *Jus in Bello*' (2013) 89 *International Law Studies* 296.

Y Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' (2013) 89 *International Law Studies* 280.

Y Dinstein, 'The Creation of Customary International Law' (2006) 322 *Recueil des cours* 272.