Characterisation of Cyber Armed Conflicts

SOHYUN SHIN

Durham University

Characterisation of Cyber Armed Conflicts

Sohyun Shin

A Thesis Submitted for

the Degree of Doctor of Philosophy

Durham Law School

November 2016

Abstract

The revolutionary adoption of computer technology to the means and methods of armed conflict, along with the rapid pace of information technology development, has raised great concerns about how best to deal legally with this new phenomenon. One of the most fundamental concerns is how to characterise cyber armed conflict within the context of international law. Therefore, this thesis aims to discuss how to characterise conflicts occurring in and through cyberspace in terms of *jus in bello* in order to legally regulate these events. The thesis addresses three separate types of categorisation: 'actors' and 'intensity', which are based on the existing definition of kinetic armed conflict, and 'geography', which is a particularly difficult issue within characterisation.

After examining the legal nature of armed conflict, chapter 3 addresses international cyber armed conflict from the angle of 'actors' in classification. Drawing examples from the cyber armed forces established in several states, the chapter looks at how to identify irregular armed forces in cyberspace in terms of international humanitarian law (IHL).

Chapter 4 deals with non-international cyber armed conflict which consists of 'organised armed group' as one party to the conflict in terms of 'actors' and the 'intensity' criterion. While the concept of organised armed group is comparatively well-established, the meaning of 'organisation' and 'armed' in the cyber context should be reconsidered. Bearing in mind that the assessment standards for intensity have not yet been definitively established even in kinetic armed conflicts, the process of assessing the intensity of cyber armed conflict is also examined.

Chapter 5 addresses the geographical issues surrounding cyber armed conflict. Given the physically borderless nature of cyberspace, current IHL rules are not a good fit for characterising cyber armed conflict. To respond to these issues, the chapter analyses whether

the existing bifurcated structure of characterisation (IAC and NIAC) can be sustained or a new third type of transnational armed conflict is required. Criticising the relevant theory of ‘zone of hostilities’, the author concludes that characterisation of cyber armed conflict should be approached on a non-geographical basis.

Table of Contents

Copyright Declaration

Acknowledgements

Arriving at the finish line of the long journey of my Ph.D., I would like to dedicate this thesis to my mother who has shown me endless patience and love along the way. I will be forever indebted to Professor Gleider Hernandez. Gleider has been an exemplary supervisor and mentor, guiding me academically with his competence and seemingly endless knowledge of international law while displaying sincere compassion and kindness for me personally. Gleider – I could never have done this without your support. Thank you for everything. Professor Michael Schmitt provided truly inspirational advice at the early stage to help me determine the theme and structure of this thesis. In addition, the graduate student support system, including the academic support office, counselling service centre, and Ustinov College, helped me get through health and other issues. Lastly, I want to thank my dear friends who studied together, supported each other, and spent far too much time in the PG research room. Using this thesis about cyber armed conflicts as a momentum, I hope to do even more research on cyber issues in international law over the course of my career.

Abbreviation

Additional Protocol I	Protocol Additional to the Geneva Conventions of 12
also AP I	August 1949, and Relating to the Protection of Victims of International Armed Conflicts
Additional Protocol II	Protocol Additional to the Geneva Conventions of 12
also AP II	August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts
ASIL	American Journal of International Law
ARSIWA	Articles on the Responsibility of States for Internationally Wrongful Acts
BYBIL	British Yearbook of International Law
CCD COE	Cooperative Cyber Defence Centre of Excellence
CUP	Cambridge University Press
CWC	Chemical Weapons Convention
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPH	Direct Participation in Hostilities
DPRK	Democratic People's Republic of Korea
ETS	European Treaty Series
EU	European Union
EJIL	European Journal of International Law

Geneva Convention I	Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949
Geneva Convention II	Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949
Geneva Convention III	Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949
Geneva Convention IV	Geneva Convention Relative to the Protection of Civilian Persons in Time of War of August 12, 1949
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
IAC	International Armed Conflict
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
ICTR	International Criminal Tribunal for Rwanda
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International Humanitarian Law
IRRC	International Review of Red Cross
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organisation

NIAC	Non-International Armed Conflict
NPT	Non-Proliferation Treaty
OECD	Organisation for Economic Co-operation and Development
OUP	Oxford University Press
PCA	Permanent Court of Arbitration
PCIJ	Permanent Court of International Justice
PMSCs	Private Military and Security Companies
RCADI	*Recueil des Cours de l'Académie de Droit International*
RMA	Revolution in Military Affairs
ROK	Republic of Korea
SCADA	Supervisory Control and Data Acquisition
SCSL	Special Court for Sierra Leone
TAC	Transnational Armed Conflict
UK	United Kingdom
UN	United Nations
UNTS	United Nations Treaty Series
URL	Universal Resource Locator
US	United States (of America)
USCYBERCOM	United States Cyber Command
YBIHL	Yearbook of International Humanitarian Law

Chapter 1 – Introduction

'Cyber attacks' occur daily in many of areas such as banking, government sites, broadcasting, media, military facilities, electricity, and commerce, yet little is known about the legal characters of these attacks or how they are identified in terms of international law. Cyber clashes between people can be largely divided into three legal categories. First, criminal law copes with cyber crimes such as cyber fraud, criminal copyright infringement, and child pornography in cyberspace.[1] Second, human rights law deals with issues including freedom of speech, defamation, and freedom of expression cases in cyberspace ruled by private laws and international human rights law.[2] Third, from the perspective of national and international peace and security, novel trends such as military use of information technology and cyberspace as a battlefield are subject to international humanitarian law (IHL) (*jus in bello*) and the law of use of force (*jus ad bellum*) in international law.[3]

Among these legal categories, this thesis ultimately focuses on the field of IHL in regard to cyber attacks. It investigates how to characterise (or classify)[4] cyber

---

[1] Jonathan Clough, *Principles of Cybercrime* (CUP 2010); Andreas Rahmatian, 'Cyberspace and Intellectual Property Rights' in Nicholas Tsagourias and Russell Buchan (eds), *Researcg Handbook on International Law and Cyberspace* (Edward Elgar 2015) Philipp Kastner and Frédéric Mégret, 'International Legal Dimensions of Cybercrime' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

[2] David P. Fidler, 'Cyberspace and Human Rights' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

[3] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012); Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014); Keiichiro Okimoto, *The Distinction and Relationship between Jus ad Bellum and Jus in Bello* (Hart Publishing 2011)

[4] In IHL, both terms of characterisation and classification are interchangeable.

conflicts in terms of the laws of armed conflict (LOAC). In other words, this thesis aims to offer a framework for classifying armed conflict situations in cyberspace in order to apply the relevant IHL rules through reconsidering whether and how the existing criteria of classification (actors, intensity, and additionally, geography) apply to those situations, and examining whether the existing rules are in itself applicable to cyber armed conflicts or required to be amended.

Why it is important to classify a cyber conflict as an international armed conflict (IAC) or a non-international armed conflict (NIAC) under IHL is based on the very fundamental bifurcated structure of IHL itself. IHL began in order to regulate inter-state wars and expanded to intra-state war between government and non-state entities. In principle, the rules of IHL are divided into two sets, for IACs and NIACs. Some scholars suggest that the contemporary rules applicable in IACs and NIACs are substantially similar, if not identical.[5] There is a tendency of convergence of IAC and NIAC in IHL.[6] For example, the 1993 Chemical Weapons Convention,[7] the 1997 Anti-Personnel Mines Ban Convention[8] and the 1999 Second Protocol to the Hague

[5] James G. Stewart, 'Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict' 85 IRRC 313-350; Marko Milanovic and Vidan Hadzi-Vidanovic, 'A Taxonomy of Armed Conflict' in Nigel D. White and Christian Henderson (eds), Research Handbook on International Conflict and Security Law (Edward Elgar 2013) 256-257; Emily Crawford, The Treatment of Combatants and Insurgents under the Law of Armed Conflict (OUP 2010) 6-47; Lindsay Moir, 'Towards the unification of international humanitarian law?' in Richard Burchill, Nigel D. White and Justin Morris (eds), *International Conflict and Security Law* (CUP 2005) 108-119.

[6] Marco Sassòli, 'The Convergence of the International Humanitarian Law of Non-International and International Armed Conflicts - The Dark Side of a Good Idea' in Giovanni Biaggini, Oliver Diggelmann and Christine Kaufmann (eds), *Polis und Kosmopolis: Festschrift für Daniel Thürer* (Dike / Nomos 2015) 680-681.

[7] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (adopted 13 January 1993, entered into force 29 April 1997) 1974 UNTS 45 (at art 1(1) 'Each State Party to this Convention undertakes never under any circumstances:')

[8] Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction (adopted 18 September 1997, entered into force 1 March 1999) 2056 UNTS 211.

Convention for the Protection of Cultural Property in the Event of Armed Conflict[9] apply to both IAC and NIAC. Another example is how the fundamental principles prohibiting weapons that cause superfluous injury or unnecessary suffering[10] and indiscriminate weapons by nature[11] apply in both IAC and NIAC.[12] The first decision of the International Criminal Tribunal for the former Yugoslavia (ICTY) in the *Tadić* Case held that a number of rules regulating IAC are also applicable to NIAC as customary international law.[13]

If the division between IAC and NIAC has realistically faded, the purpose of this thesis examining whether cyber conflict can be classified as an IAC or a NIAC would be insignificant. However, the author does not agree with this opinion of convergence of IAC and NIAC in relation to IHL. Although there are some convergent tendencies of IAC and NIAC, it is the outcome from the course that regulation of NIAC and the protection of people during NIAC have expanded, not because the distinction of IAC and NIAC has faded in IHL. On the other hand, even if rules regulating IAC have nearly reached the status of custom in situations of armed conflict not of an

[9] Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict (adopted 26 March1999, entered into force 9 March 2004) 2253 UNTS 172.

[10] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I), art 35(2); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law Volume I: Rules* (ICRC, CUP 2005) 237-244 Rule 70.

[11] Additional Protocol I, art 51(4); ibid 244-250 Rule 71.

[12] William H. Boothby, 'Differences in the Law of Weaponry When Applied to Non-International Armed Conflict' 88 International Law Studies 197.

[13] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* (Jurisdiction) ICTY (2 October 1995) para 96-127 ('Notwithstanding these limitations, it cannot be denied that customary rules have developed to govern internal strife. These rules,…, cover such areas as protection of civilians from hostilities, in particular from indiscriminate attacks, protection of civilian objects, in particular cultural property, protection of all those who do not (or no longer) take active part in hostilities, as well as prohibition of means of warfare proscribed in international armed conflicts and ban of certain methods of conducting hostilities.' (ibid para 127))

international character, it cannot be asserted whether states would consent to the full convergence of two sets of rules between IAC and NIAC because states even tend to be reluctant to admit the existence of NIAC in their territories.[14] The rules applicable in IAC do not yet fully map onto the rules applicable in NIAC, and there thus remains a clear division between the classifications of IAC and NIAC.[15] Some rules of IAC do not exist for or even analogically apply to NIAC. For example, combatant and prisoner of war (POW) status only exist in IACs. Perfidy, which is prohibited in IAC, has been carried out in NIAC. There is no treaty explicitly applying the prohibition of perfidy to NIAC.[16] Even though state practice and other international legal instruments seem to try to establish war crime of perfidy in NIAC,[17] it is still uncertain whether and to what extent perfidy is prohibited in NIAC.

This introductory chapter centres research questions in order to look into the classification of cyber armed conflicts. After setting up the methodology and scope of the research, the fundamental and main terms used in the thesis is scrutinised, and then overall thesis structure is lastly addressed.

---

[14] Tom Ruys, 'The Syrian Civil War and the Achilles' Heel of the Law of Non-International Armed Conflict' 50 Stanford Journal of International Law 247 257-260; Sandesh Sivakumaran, *The Law of Non-International Armed Conflict* (OUP 2012) 9-29.

[15] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* para 126.

[16] Robert L. Pratt, 'The International Legal Prohibition on Perfidy and Its Scope in Non-International Armed Conflicts' 56 Virginia Journal of International Law 1 3-4. ('In fact, the travaux of Additional Protocol II reveals that the perfidy prohibition was deliberately removed from the agreement. Additionally, state practice, which could help identify whether a prohibition on perfidy in NIACs is customary international law, is inconsistent.')

[17] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90, art 8(2)(e)(ix); Michael N. Schmitt, Charles H.B. Garraway and Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict with Commentary* (IIHL 2006); Richard B. Jackson, 'Perfidy in Non-International Armed Conflicts' 88 International Law Studies 237; Pratt, 'The International Legal Prohibition on Perfidy and Its Scope in Non-International Armed Conflicts'.

I. Research Questions

It should be noted that regardless of the exact legal character of a cyber conflict or cyber operation, the international community already accepts the premise that cyber operations constitute threats or attacks that have a quasi-military character or have a similarly critical effect on their economic and social survival.[18] Hence, the most urgent and significant question is how well and precisely a nation may be prepared to cope with cyber armed conflict situations in terms of international law.[19] In this regard, there have been researches and academic literatures comprehensively dealing with cyber armed conflicts.[20] However, classification for cyber armed conflicts seems not to be researched in detail. Compared to those precedent efforts, this thesis intends to specifically focus on the process of classification itself. In order to lay out applicable LOAC rules to cyber armed conflicts or to create a new regime for cyber armed conflicts in the future,[21] classifying the concerned armed conflict should be in

[18] The issues of 'Developments in the Field of Information and Telecommunications in the Context of International Security' has been on the United Nations Agenda since 1998. To date, there have been Groups of Governmental Experts (GGE) that examines the existing and potential threats from the cyberspace and reports to the UN General Assembly since 2004. (UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/65/201 16 July 2010)) In 2013, the GGE reported its recommendations to promote peace and stability in state use of Information and Communication Technologies (ICTs). Especially, it emphasised 'the importance of building capacity in states that may require assistance in addressing the security of their ICTs and suggested additional work to elaborate common terms and definitions.'(UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98 24 June 2013)) Then, it significantly expands the discussion of norms, especially how international law applies to the use of ICTs by states, in 2015. (UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174 22 July 2015))

[19] For the overall feature of cyber conflicts, Herbert Lin, 'Cyber Conflict and International Humanitarian Law' 94 IRRC 515.

[20] Roscini, *Cyber Operations and the Use of Force in International Law*; Dinniss, *Cyber Warfare and the Laws of War*; Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014)

[21] There are two different stands at large about this issue, representatively West countries including the United States of America (US), the United Kingdom (UK), and other NATO member states and a

advance carried out. Hence, this thesis has singled out characterisation as an urgent need to cope with future cyber armed conflicts.

Conflict situations do not exist fixed: some situations could be characterised in a very early stage of their occurrence, whereas other situations change or develop their legal characters according as the situations concerned have unfolded. In this regard, the author used the expression of 'process' of characterisation above. It is necessary to take the existing system of LOAC into account in order to identify a given conflict situation. That is to say, the bifurcated structure of LOAC as international and non-international armed conflict should be considered in organising the discourse of this thesis. Therefore, the flow of this thesis as follows: international cyber armed conflicts, non-international cyber armed conflicts, and transnational armed conflicts as newly suggested category of armed conflict. It is also helpful for the readers to understand the course of war (armed conflict): the development of armed conflict from 'war between states' to internal armed conflict and technologically developed armed conflict such as cyber war. In addition, unique characteristics and novel trends occurring in cyberspace should be necessarily reflected in characterising cyber armed conflicts. The author picked up three points of those characteristics and trends relating to the requirements of characterisation as follows.

---

group of Russia, China, and other their close states. This point will be mentioned in detail later in the thesis.

1. Changes and Expansion of Actors in Cyber Hostilities

The traditional and basic version of armed conflict is an inter-states war, between at least two sovereign nations. If two states are found as the parties to a given conflict situation, the concerned conflict would be classified as an IAC. In this regard, the criterion of actors would be first considered in classification. Cyber warriors become more diverse and their tasks or way of conducts are different from them of kinetic warfare. For example, private military and security companies (PMSCs)[22] could be more broadly and closely involved in cyber sector and even private individuals can more easily participate in cyber hostilities in a direct or indirect way. On the other hand, the difficulty in identifying actors in cyber conflicts is amplified due to the limitations of technology and the asymmetries among actors in tracing attackers and proving the origin of attacks. It should be noted at the same time that the principle of distinction between private and military actors, objects, or networks is still valid in cyberspace as one of the most fundamental principles supporting IHL regime. The foregoing is common in both international and non-international armed conflicts. First of all, it is more difficult to distinguish between state actors and non-state actors in virtual space rather than in kinetic space. In the Georgian-Russian armed conflict in 2008, even though there were strong suspicions about their connections, it was not

[22] About the definition and roles of PMSCs, ICRC, *The Montreux Document - On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict* (2008); Hannah Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (CUP 2011); For the latest development in the field of PMSCs, Tilman Rodenhäuser and Jonathan Cuénoud, 'Speaking law to business: 10-year anniversary of the Montreux Document on PMSCs' Humanitarian Law & Policy Bolg <http://blogs.icrc.org/law-and-policy/2018/09/17/speaking-law-business-10-year-anniversary-montreux-document-pmscs/?utm_source=ICRC+Law+%26+Policy+Forum+Contacts&utm_campaign=c1e18b2fd7-EMAIL_CAMPAIGN_2018_09_13_08_22_COPY_01&utm_medium=email&utm_term=0_8eeeebc66b-c1e18b2fd7-105936333&mc_cid=c1e18b2fd7&mc_eid=3e837c1a9e> accessed 25 September 2018. And about the Montreux Document Forum since 2014, visit its official site <http://www.mdforum.ch/>.

proven to the end whether the hackers targeting Georgian objects were involved with Russian government or military forces.[23] Secondly, it means that when a group of individuals or individuals engage in cyber operations on behalf of a government, attribution is much more difficult to be recognised than in kinetic operations. Since cyber outsourcing has expanded to various sectors and roles in the recent past, it is also necessary to reconsider the tests of attribution in international law. These issues are centred in chapter 3 to classify an IAC out of cyber conflicts.

As regards 'actors' criterion, it is also required to consider how to view the structure of organisation which may constitute 'organised armed groups' in non-international cyber armed conflicts. It is simultaneously helpful to distinguish an individual of 'direct participation in hostilities' (DPH) cases, which deprive individuals of the protection of civilians 'for such time',[24] from a regular member of an organised armed group, which treats ones as its standing members (similar to 'combatant' status in an IAC). Chapter 4 addresses these issues in terms of non-international cyber armed conflict.

2. Intensity Measuring in Cyber Conflict

It is not always obvious, even for the parties involved in the situation concerned, whether armed violence has reached the threshold of an armed conflict as the situation

[23] Richard Stiennon, *Surviving Cyberwar* (Government Institutes 2010); Andreas Hagen, 'The Russo-Georgian War 2008' in Jason Healey (ed), *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (A CCSA Publication 2013)

[24] Additional Protocol I, art 51(3); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Additional Protocol II), art 13(3)

progresses. Even though IHL treaties do not supply the definition of an armed conflict, article 2(1) of the Additional Protocol (AP) II stipulates that 'situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature' do not constitute armed conflict.[25] It is not easy to draw a clear line between a violent situation which presents lower than this threshold and an armed conflict, although it bears mentioning that the required intensity could be different between IAC and NIAC.[26] In examining the criterion of intensity, the meaning of 'attack' and the definition of 'cyber attack' in terms of IHL shall be initially considered because 'cyber attack' can be regarded as a sort of minimum measuring unit to assess a cyber operation having legal effects in terms of IHL.[27] In this regard, cyber attack is first examined later in this chapter. The most important issue is the determination of methods to be used in order to distinguish non-international cyber armed conflict from situations which fall short of this cyber armed conflict threshold, such as internal cyber disturbances and tensions. In order to advance with the assessment, the constituent aspects of intensity such as 'gravity' and 'duration' should be concretised based on the discourse for the intensity of non-international kinetic armed conflicts. Lastly, the temporal scope of cyber armed conflicts needs to be examined with regard to the fluctuating character of intensity.

---

[25] Additional Protocol II, art 2(1)

[26] Similarly, for the determination of use of force amounting to armed attack to resort to self-defence based on article 51 of the UN Charter, the International Court of Justice (ICJ) stated that 'as regards certain particular aspects of the principle in question, it will be necessary to distinguish the gravest forms of the use of force (those constituting an armed attack) from other less grave forms.' (*Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14 para 191)

[27] 'Attack' is defined as 'acts of violence against the adversary, whether in offence or in defence' at article 49(1) of the AP I. For reference, the LOAC governs some cyber operations affecting the delivery of humanitarian assistance, even when those operations do not rise to the level of an attack. (Michael N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 540-542)

Chapter 4 addresses these issues of intensity surrounding non-international cyber armed conflicts.

3. De-geographical Approach to Classification

Even though the territorial requirement in and of itself has not been an original criterion of classification, there is a limited consideration of geographical aspects with respect to article 1(1) of the AP II [28] and the common article 3 to the Geneva Conventions [29] in terms of classification of an armed conflict. It especially becomes a problematic issue in discussing kinetic warfare as to whether extraterritorial armed conflict[30] situations should be considered as NIAC, IAC, or transnational armed conflict (TAC), which is newly suggested as the third category of armed conflict. This debate surrounding extraterritorial armed conflicts has also raised some points worthy to be correspondingly considered for characterising non-international cyber armed conflict on the ground that borderlessness of cyberspace allows non-state actors to launch cyber attacks against a state everywhere in the world.

---

[28] Additional Protocol II, art 1(1) – Material field of application

1. This Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol. (underlined by the author)

[29] Geneva Conventions I-IV, art 3

1. In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions: … (underlined by the author)

[30] In the thesis, an 'extraterritorial armed conflict' refers to 'the situation where ongoing hostilities between a state and a non-state actor take place, at least in part, outside the territory of the state'. See details in Chapter 5 – Transnational Cyber Armed Conflict? III. Transnational Armed Conflict: A New Type of Armed Conflict?

Accordingly, chapter 5 addresses geographical issues surrounding a new type of TAC. There is one suggestion relating to the geographical scope of an armed conflict, so-called 'zone of hostilities' (or zone of combat).[31] This theory explains that non-state actors are targetable on the basis that the geographical scope of the concerned armed conflict is already practically expanded to the location of them in the situation of extraterritorial armed conflict. Then, the question also arises as to whether the aforementioned theory is genuinely connected to the classification of non-international cyber armed conflict. Briefly described, the theory of 'zone of hostilities' is illogically policy-oriented for the purpose of targeting itself, so it is only necessary to be examined not to bring about confusion in the research of classification. Chapter 5 argues that a de-geographical approach should be taken for the characterisation of cyber armed conflicts and in the same context TAC does not need to be added as a new type of armed conflict. In conclusion, geographical issues can be said to be incidental and subsidiary compared to the two original conditions of 'actors' and 'intensity' for classifying an armed conflict.

[31] For more detailed contents and development of the theory, Laurie R. Blank, 'Defining the Battlefield in Contemporary Conflict and Counterterrorism: Understanding the Parameters of the Zone of Combat' 39 Georgia Journal of International and Comparative Law 1; Jennifer C. Daskal, 'The Geography of the Battlefield: A Framework for Detention and Targeting outside the "Hot" Conflict Zone' 161 University of Pennsylvania Law Review 1165; Rosa Ehrenreich Brooks, 'War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror' 153 University of Pennsylvania Law Review 675.

II. Methodology

1. Research Methods

Methodologies taken in legal studies vary according to research questions, purposes, and contexts.[32] As this thesis interacts with IHL and looks for applying this legal framework to cyber conflict, it will progressively develop (that is, adapt) IHL where necessary to meet the overriding objectives of IHL and these interpretations are preferred because they represent an appropriate compromise (or balance) between the principles of military necessity and humanity. In doctrinal research of international law, the identification of rules leads to the determination of their subjects and of the facts or situations to which they apply in that the legal system, which itself offers a theoretical framework to select facts and to concatenate them in its context.[33] The points of issues under discussion in this thesis start from the positive rules of IHL, including treaties and customary international law. Other aspects, such as soft law, non-state practice, and other things related to the extent that they lead to reactions by states, would be incidentally considered.

When facing a new phenomenon, like cyber armed conflicts, the questions arise as to how this new development fits in with the relevant area of law, or if it does not seem to fit in, how the existing set of rules should be rearranged in order to accommodate

[32] Philip Langbroek and others, 'Methodology of Legal Research: Challenges and Opportunities' 13 Utrecht Law Review 1 1-4.

[33] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' 17 Deakin Law Review 83 107-108.

this novelty.[34] 'In a case for which no relevant rule of international law can be found, logical reasoning makes it possible to determine whether such a situation implies liberty of action or whether, on the contrary, some form of regulation is necessary; the latter is applicable especially where its absence would lead to a conflict between several states exercising their liberty of action, or when the results of such a situation would be unsatisfactory.'[35] The ICT environment offers both opportunities and challenges to the international community in determining 'how norms, rules and principles can apply to state conduct of ICT-related activities' from a general cyber security as well as a military perspective.[36] As later seen in this thesis, states, international organisations (including the UN, NATO, and CCDCOE, etc.) and academics have committed to establish the rule of law over cyberspace with diverse policy considerations, which would be economic, political, diplomatic, or technological. After depicting what the new development actually consists of, the questions of 'how the new development can be made consistent with the rest of the legal system and in which sense other related concepts are affected and how current distinctions should be adapted and modified'[37] needs to be addressed.

The characterisation of cyber armed conflicts is an emerging area within IHL, so it requires a more comprehensive analysis. In this regard, throughout the thesis, the

---

[34] Ibid 108.

[35] Christian Dominicé, 'Methodology of International Law' in Christian Dominicé, Jeanne Belhumeur and Luigi Condorelli (eds), *L'ordre Juridique International Entre Tradition et Innovation* (Graduate Institute Publications 1997) <https://books.openedition.org/iheid/1334?lang=en> accessed 25 March 2019.

[36] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174 22 July 2015) 7.

[37] Pauline C. Westerman, 'Open or Autonomous? The Debate on Legal Methodology as a Reflection of the Debate on Law' in Mark Van Hoecke (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2011) 89.

author has attempt to cautiously delineate between *lex lata* (what the law is) and *lex ferenda* (what the law should be) in characterisation standards. When discussing those situations where cyber conflicts do not dovetail with the current IHL, it is necessary to examine the general principles of IHL and international law. Reference could need to be made to other legal frameworks, such as international human rights law, international criminal law or domestic laws. If, despite all these courses, a legal void is located, the thesis may need to suggest *lex ferenda* as long as it is possible and allowed based on the understanding of international law with a more policy-oriented approach. The problem of *lacunae* should also be approached by legal reasoning.[38] The rule or the principle of solution may be determined with the help of analogy, which involves locating similar situations arising and arguing that similar cases should be governed by the same principle and have similar outcomes. The similarity of the two situations must be evident.[39] So after having identified a rule its application could be extended to cover a case, situation, or legal relationship not explicitly envisaged by it.[40] As a whole, it can be also said that a kind of hybrid approach is taken by taking policy considerations into account in this research.

Since the thesis aims to develop a framework for characterising cyber conflicts in order to apply IHL to cyber armed conflicts and to find legal *lacuna* under the current

[38] There would be by and large empirical observation and logical reasoning that coordinatingly lead to analyse international legal order. The former links to the inductive method that identifies the rules of law by observing their effectiveness in the international community. The latter links to the deductive method that determines the existence of rules of international law by a process of reasoning based on principles, legal facts or on formal modes of creation. These inductive and deductive methods are not necessarily exclusive each other, rather their blended utilisation constitutes the notion of legal reasoning. (Hutchinson and Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' 105, 110-112; Dominicé, 'Methodology of International Law')

[39] Dominicé, 'Methodology of International Law'.

[40] Ibid.

framework, it starts with analysing the classification rules of kinetic armed conflict as defined under existing IHL. On the basis of balanced scrutiny of existing IHL rules of classification in kinetic space, the thesis looks into each aspect of characterisation for cyber armed conflicts. In addition to gathering information on the ground, if necessary, potential scenarios of cyber armed conflict could be assumed to exist somewhere else. The author takes the position that the crucial principles supporting the existing IHL, such as the principles of distinction, humanity, and military necessity, should apply identically to cyber armed conflicts. It should be also remembered that a policy-oriented approach cannot overturn the rulings in international law such as the strict distinction between *jus ad bellum* and *jus in bello,* or proportionality as a general principle.[41]

2. Scope of Research

A contemporary armed conflict mostly consists of kinetic and cyber hostilities. Cyber tactic and methods are ordinarily accompanied in order to directly support military operations in kinetic battlefield. Before deploying ground forces into a battlefield or bombarding targets, for example, cyber operations take place to neutralise or incapacitate the defensive radar systems. Cyber operations are also conducted during kinetic military operations when it is necessary for strategic purposes. As seen in the Georgian situation in 2008, cyber attacks now frequently accompany kinetic armed conflicts.[42] When Russia invaded the Crimean Peninsula in 2014, the armed conflict

[41] Michael Newton and Larry May, *Proportionality in International Law* (OUP 2014)

[42] In the 2006 war against Hezbollah, Israel alleges that cyber-warfare was part of the conflict, where the Israel Defence Force (IDF) intelligence estimates several countries in the Middle East used Russian hackers and scientists to operate on their behalf. (_____, 'Israel Adds Cyber-Attack to IDF'

between Ukraine and Russia was spread on cyberspace where state-sponsored groups of hackers conducted destructive cyber operations from both sides of the conflict.[43] Before involving in Syrian armed conflict, the US government reportedly established 'a battle plan that featured a sophisticated cyber attack on the Syrian military and President Bashar al-Assad's command structure'.[44] Later in 2017, the US launched a series of cruise missiles at an airbase in Syria.[45] Classifying this type of kinetic – cyber mixed armed conflict does not matter, since it satisfies the conditions for being an armed conflict.

Whether and how a purely stand-alone cyber armed conflict can exist as a matter of law is the most critical idea under the scrutiny of this thesis. This situation is hypothetical since it has not yet occurred. However, from the author's viewpoint, it has been proven through a series of past events that cyber armed conflicts may occur in the near future.[46] The thesis examines the framework for the classification of stand-

---

<http://www.defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/> Military.com accessed 25 March 2016)

[43] Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyberwar' WIRED <https://www.wired.com/story/russian-hackers-attack-ukraine/> accessed 23 September 2018.

[44] David E. Sanger, 'Syria War Stirs New U.S. Debate on Cyberattacks' *The New York Times* (24 February 2014) <http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?nl=todaysheadlines&emc=edit_th_20140225&_r=0> accessed 25 October 2018.

[45] Michael R Gordon, Helene Cooper and Michael D Shear, 'Dozens of U.S. Missiles Hit Air Base in Syria' *New York Times* (6 April 2017) <https://www.nytimes.com/2017/04/06/world/middleeast/us-said-to-weigh-military-responses-to-syrian-chemical-attack.html> accessed 25 October 2018.

[46] An incident in Estonia in 2007 attracted much attention in that it demonstrated how large-scale, concentrated cyber attacks are capable of functionally paralysing a state. The Estonian government strengthened their emergent partnership with the EU and NATO and invited the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) to be based in Tallinn. Cyber attacks were carried out during the armed conflict between Georgia and Russia in 2008. (Eneken Tikk, International Cyber Incidents: Legal Considerations 67-71) In Belarus in 2008 and 2009, the cyber attacks occurred at the domestic level between the state and its people. (Fyodor Pavlyuchenko, 'Belarus in the Context of European Cyber Security' in Christian Czosseck and Kenneth Geers (eds), The Virtual Battlefield: Perspectives on Cyber Warfare (CCDCOE Publications 2009) 1-3) As an example of a comparatively powerful state's covert cyber operations against another state, the Iranian 'Stuxnet' incident, reportedly launched in mid-2009, is assumed to be the virus designed by an American-Israeli project to sabotage

alone cyber armed conflicts based on the analysis of the current IHL rules of classification.

Ancillary rules not directly relating to classification such as 'neutrality', 'espionage', or 'targeting' would be only briefly mentioned at the relevant parts if necessary, and as long as it does not disturb the main flow of thesis. For example, the concept of cyber espionage is examined in the course of clarifying the definition of cyber attack in terms of LOAC and neutrality or targeting is mentioned to the limited extent to examine whether geography of armed conflict has an effect on the classification of cyber armed conflict.

This thesis also abstains from looking into the issues related to *jus ad bellum*, which consider the legitimacy and legality of the use of force, surrounding cyber armed conflicts. It does not touch on cyber operations occurring independently of an armed conflict in any detail.

---

the Iranian nuclear programme. (David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran' *The New York Times* (1 June 2012) <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0> accessed 12 August 2012) It was also reported that South Korea is to develop Stuxnet-like cyber weapons in an attempt to damage North Korean nuclear facilities. ('South Korea to develop Stuxnet-like cyberweapons' *BBC News* (21 February 2014) Technology <http://www.bbc.co.uk/news/technology-26287527> accessed 24 February 2014) The predominant trend of these attacks is the apparent willingness of states to engage in covert cyber operations against each other, different from the Estonian or Georgian incidents. (Jason Healey, 'Part 1: A Brief History of US Cyber Conflict ' in Jason Healey (ed), *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (A CCSA Publication 2013) 75); The question about whether a stand-alone cyber armed conflict will occur will be dealt with again in chapter 6.

III. Terms and Definitions

There has been continued discourse on the proper and agreed definitions of key terms surrounding cyber conflicts. Since cyber conflicts are a comparatively recent development, there is no broadly accepted framework to decently encompass it. For this research, it is necessary to point out the definitions of key terms to unfold discussion.

1. Cyberspace

As there have been multiple terms used for the location of cyber conflicts – for instance, the computer network, the Internet, cyberspace, or simply the Net – it is not easy to find a fixed definition of this space in formal documents. According to the US Deputy Secretary of Defence, cyberspace is defined as 'the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries'.[47] According to the UK government, 'cyberspace is an interactive domain made up of digital networks that are used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services.'[48]

[47] Deputy Secretary of Defence Memorandum, *The Definition of Cyberspace* (12 May 2008); The US Department of Defence holds this definition is consistent with the definition of cyberspace provided in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23); In 2006, the Department of Defence Joint Staff defined cyberspace as 'a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures'. (The United States Department of Defence, *National Military Strategy for Cyberspace Operations* (2006) 11)

[48] Cabinet Ofiice, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (25 November 2011)

Russia uses a different term, 'information space', which is defined as 'the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself'.[49] The 'information infrastructure' refers to 'the total complex of technical means and systems of the formation, conversion, transfer, use, and storage of information'.[50] The Chinese regards 'information space' as 'a new place for communicating with all of the world's population'.[51] It is 'the integration of all the world's communications networks, databases and information, forming a landscape huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space'.[52] Both Russia and China use the concept of 'information space', which is less well-established than in the West and refer to 'cyberspace' for translation of foreign texts or reference to foreign approaches.[53]

The *Tallinn Manual* 2.0 similarly defines cyberspace as 'the environment formed by physical and non-physical components, characterised by the use of computers and the electromagnetic spectrum, to store, modify, and exchange data using computer networks'.[54] After all, it is important to bear in mind that cyberspace does not only

[49] The Ministry of Foreign Affairs of the Russian Federation, Draft Convention on International Information Security, art 2 (22 September 2011) <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publish> accessed 24 October 2018.

[50] Ibid.

[51] Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in K. Podins, J. Stinissen and M. Maybaum (eds), *2013 5th International Conference on Cyber Conflict* (NATO CCDCOE Publications 2013) 419.

[52] Ibid.

[53] Ibid 418-419.

[54] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 564.

refer to the virtual world made by the Internet, but also embraces all the physical components needed to create the virtual space itself.[55]

All the above-mentioned definitions of cyberspace suggest that 'cyberspace' as a concept is more than computers and digital information on the Internet. Cyberspace can be said to have three layers: first, as the most concrete layer, the infrastructure of the cyber world is the physical layer of computers, integrated circuits, processors, storage devices, cables, and communications infrastructure and any additional communication infrastructure. The second layer incorporates software, which is a variety of systems of instructions for action and reaction programmed by humans. The third layer, the least concrete of the three, is the layer of data that creates information and is contained by machines.[56] An operative working definition of 'cyberspace' could thus be as follows: inter-connected networks of information technology infrastructures, including the Internet, telecommunication networks, mission-specific networks, computers, and computer embedded systems. The virtual environment – data stored and information processed by computers and transferred over these networks – is also included.[57] As cyberspace is an operational domain of practical implications, it also requires the allocation of resources to support the organisation,

[55] For the unique character of cyberspace differentiating from earlier information networks, Daniel T. Juehl points out 'the inseparable linkage of the technology, the human uses, and the impact of the interconnectivity in the modern world' that manifest 'its foundation in the physical world' and 'the use of the electromagnetic spectrum as the means of movement within the domain'. (Daniel T. Juehl, 'From Cyberspace to Cyberpower: Defining the Problem' in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds), *Cyberpower and National Security* (National Defense University Press 2009) 25-31)

[56] Lior Tabansky, 'Basic Concepts in Cyber Warfare' 3 Military and Strategic Affairs 75 77-78.

[57] Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Reasearch Handbook on International and Cyberspace* (Edward Elgar 2015) 15; About the structure of cyberspace in depth, Elihu Zimet and Edward Skoudis, 'A Graphical Introduction to the Structural Elements of Cyberspace' in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds), *Cyberpower and National Security* (National Defense University Press 2009) 91-112.

training, and equipping of 'cyber-forces'.[58] In this thesis, the author adopts the definition of *Tallinn Manual*, which is comparatively newly researched.

2. Cyber Operations

Cyber operations[59] are broadly described as 'operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system.'[60] Cyber operations are defined in the *Tallinn Manual* 2.0 as 'the employment of cyber capabilities to achieve objectives in or through cyberspace'.[61] According to this definition, cyber operations are a common denominator for cyber activities. This common denominator can be used in a variety of situations, by a variety of actors, and for various reasons.[62] Hence, expressions such as, 'cyber operations as armed attacks', 'cyber operations as use of force',[63]

[58] Stuart H. Starr, 'Towards an Evolving Theory of Cyberpower' in Christian Czosseck and Kenneth Geers (ed), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009) 6.

[59] As a similar term 'information operations' 'rely on three distinct yet interrelated dimensions that in the aggregate comprise the global information environment such as the physical platforms, system and infrastructures that provide global connectivity to link information systems, networks, and human users; the massive amounts of informational content that can be digitally and electronically sent anywhere, anytime, to almost anyone, a condition that has been enormously affected and augmented by the convergence of numerous technologies; and the human cognition that results from greatly increased access to content and can dramatically impact on human behaviours and decision-making'. (Juehl, 'From Cyberspace to Cyberpower: Defining the Problem' 28)

[60] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (31st International Conference of the Red Cross and Red Crescent, 2011) 36.

[61] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 564.

[62] Paul Ducheine, 'The Notion of Cyber Operations' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 214.

[63] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 330-337, Rule 69.

'cyber operations as threat of force',[64] and 'cyber operations as an attack'[65] are possible. It is important to bear in mind that the term 'cyber operations' includes, but is not limited to, cyber attacks.[66] As subgroups of cyber operations, terms (or concepts) such as computer network attack (CNA), cyber conflict, cyber warfare, and cyber terrorism are derived from it.

2.1. Cyber Exploitation

Cyber exploitation is used in cyberspace in both war and peacetime, and refers to actions or operations carried out over an extended period of time to obtain information that would otherwise be kept confidential from the computer system or networks of an adversary or potentially adversary factions.[67] Critically, a cyber exploitation is distinguished from a cyber attack in that it does not intend to destroy a computer system or network, but to cause malfunction within system use. Even the most successful cyber exploitation is one that a user never recognises.[68]

It is not easy in practice to distinguish cyber attacks from cyber exploitations including espionage. Not all cyber attacks have a prompt violent effect on the

[64] Ibid 338-339, Rule 70.

[65] Ibid 415-420, Rule 92.

[66] According to the Manual, cyber attack is a term of art referring to a specific category of cyber operations, which is 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'. (ibid 415, Rule 92)

[67] William A. Owens, Kenneth W. Dam and Herbert S. Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press 2009) 11.

[68] Ibid 10-11; Herbert S. Lin, 'Offensive Cyber Operations and the Use of Force' 4 Journal of National Security Law and Policy 63 63.

adversary.[69] Non-recognisable cyber attacks, which the aggrieved party does not know that it is being attacked, can be conducted.[70] The non-recognisable cyber attacks seem similar with cyber exploitations in that these operations are invisible and hiding for a certain period of time and intangible to the aggrieved party, as long as not breaking out of its negative kinetic effects on the target. The only difference between the two is that cyber exploitations do not bring about any changes or damages on the target,[71] while non-recognisable cyber attacks prove their violent effects in the end. Hence, it is required to draw a line between a cyber attack, which may be silent for a while, and cyber exploitations, which are silent and non-recognisable so long as the targeted adversary is unaware. For instance, when a party invading a military computer network system degrades the defence capability or disrupts the normal operations, a series of invasion or installations of malware can qualify as a cyber attack. On the contrary, operations for the preparation of yet-scheduled attacks, such as data theft, interception, or observation of and scouting around overall frame of the system to comprehend weak points as well as merits of the target, would be regarded

[69] Owens, Dam and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* 89-91.

[70] Ibid 88-89. (For example, as seen in Iranian STUXNET case, 'once introduced into a targeted system, the payload sits quietly and does nothing harmful most of the time. However, at the right moment, the program activates itself and proceeds to destroy or corrupt data, disable system defences, or introduce false message traffic. The 'right moment' can be triggered because a certain date and time are reached, because the payload receives an explicit instruction to activate through some covert channel, because the traffic it monitors signals the right moment, or because something specific happens in its immediate environment.')

[71] 'Cyber exploitations' refers to cyber operations to support the goals and missions of the party conducting the exploitation, usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks. 'Cyber exploitations do not seek to disturb the normal functioning of a computer network system from the user's point of view – the best cyber exploitation is one that such a user never notices.' (ibid 11)

as cyber exploitations. This is because a concrete future attack has been yet unscheduled and undecided, even though the ensuing attacks are foreseeable.[72]

Cyber espionage[73] is the most representative example of this. Espionage is defined as 'the consciously deceitful collection of information, ordered by a government or organisation hostile to or suspicious of those the information concerns, accomplished by humans unauthorised by the target to do the collecting.'[74] Traditionally, espionage has not been regarded as illegal in international law.[75] Espionage itself is not relevant to the use of force for *jus ad bellum* or armed conflict for *jus in bello*. LOAC only

[72] If it is not for an unscheduled attack expected to be carried out on one day or other, but for the concretely planned attack, the operation would be already encompassed as a part of an attack and considered as the initiation of it.

[73] Cyber espionage can be used to indicate both industrial cyber espionage and a sort of espionage referring to attacks carried out by states on other states in the context of national security. There can be some overlap between the two. About cyber espionage, 'once downloaded or intruded, malware communicated back to a command-and-control server. Live intruders then remotely jumped onto the infected machine and used their new access to move across the network, implanting even more malware and exfiltrating key data. So, 'operational shady RAT (Remote Administration Tool)' was rather unremarkable. Shady RAT illustrates an important change in the art of stealing secrets. Cyber espionage is basically the use and targeting of computers to obtain a secret of some fort. One of the big changes from past espionage is not just the global scale of cyber operations but their increasingly economic quality.' (Peter W. Singer and Allan A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (OUP 2014) 91-96) General Keith Alexander, the director of the National Security Agency, which oversees United States Cyber Command, suggested that the loss of industrial information and intellectual property through cyber espionage constitutes the 'greatest transfer of wealth in history'. He said that 'U.S. companies lose about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber crime, a number that rises to $338 billion when the costs of down time due to crime are taken into account'. (Josh Rogin, 'NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'' *Foreign Policy* (9 July 2012) <http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/> accessed 15 March 2016) The British government has itself estimated the annual cost of cybercrime to the United Kingdom's economy at £27 billions. However, these figures mostly based on computer security company reports have been widely contested as being far too high. (Peter Warren and Michael Streeter, *Cyber Crime & Warfare: All that Matters* (Hodder & Stoughton 2013) 8)

[74] Geoffrey B. Demarest, 'Espionage in International Law' 24 Denver Journal of International Law and Policy 321 326.

[75] Christopher S. Yoo, 'Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (OUP 2015) 188-190.

partly deals with espionage during war, as in the Hague Regulations.[76] However, cyber espionage, as a relatively new phenomenon, needs to be reconsidered.

Cyber espionage is defined as 'any act undertaken clandestinely or under false pretences that use cyber capabilities to gather, or attempt to gather information'.[77] Cyber espionage requires more than just access to a computer system; electronic information must be copied.[78] Copying information is required to distinguish cyber espionage from mere hacking, which describes the practice of accessing computer system and networks but does not necessarily entail the copying of information.[79] The *Tallinn Manual* 2.0 distinguishes between cyber espionage, which necessarily takes place in territory controlled by one of the parties to the armed conflict, from computer network exploitation and cyber reconnaissance, which are conducted from outside enemy-controlled territory.[80] Although cyber espionage is basically not relevant to LOAC and does not violate international law, it does not mean that all the methods taken for cyber espionage are lawful. The constituent acts for the cyber

[76] Convention (IV) Respecting the Law and Customs of War on Land and its Annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2277 (Hague Regulations), art 29-31

[77] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 168.

[78] Katharina Ziolkowski, 'Peacetime Cyber Espionage - New Tendencies in Public International Law' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (CCDCOE 2013) 429; 'Cyber espionage describes the use of cyber operations to copy confidential data that is resident in or transiting through cyberspace, even if it is not read or analysed. By focusing upon the copying of data, this definition emphasises that cyber espionage does not affect the availability or integrity of data or the networks and systems upon which that data resides.' (Russell Buchan, *Cyber Espionage and International Law* (HART Publishing 2019) 17-18); Ido Kilovaty, 'World Wide Web of Exploitations — The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach' 18 Columbia Science & Technology Law Review 42 46-49.

[79] Russell Buchan, 'Cyber Espionage and International Law' in Nicholas Tsagourias and Russell Buchan (eds), *Reasearch Handbook on International and Cyberspace* (Edward Elgar 2015) 170-174.

[80] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 410-411.

espionage concerned can qualify unlawfulness.[81] States can also regulate cyber espionage by domestic legislations. After all, this thesis mainly deals with cyber operations as they pertain to an attack.

2.2. Cyber Attack

As low-intensity cyber operations such as cyber exploitations or cyber espionage have been increasing in practice, growing confusion of the term 'cyber attacks' facilitated the conflation or misunderstanding between merely lower intensity cyber operations and cyber operations reaching 'attack' or 'armed attack' in the legal sense.[82] Cyber operations pose a particular challenge for the definition of attack because cyber acts in and of itself do not necessarily involve violence. In case of a stand-alone cyber conflict without any physical confrontation between the parties, it is more indispensable to clarify the legal definition of a cyber attack in order to apply the LOAC to some qualified cyber operations. This is also linked to the intensity of cyber attack itself and the threshold of cyber armed conflict.

It is necessary to draw a clear line between 'armed attack' and 'attack' under the UN Charter system beforehand.[83] It is because the term 'cyber attack' is used without

[81] Ibid 170-171, 412; Yoo, 'Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures' 189-190.

[82] Laurie R. Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015) 94-101.

[83] Compared to the prohibition of 'use of force' stipulated in article 2(4) of the UN Charter, as an exception of it in article 51 of the Charter suggests a different threshold by using the term 'armed attack'. Then, the term 'attack' is critically and separately used in IHL as examined below. In order to understand 'armed attack', about the difference between 'use of force' and 'armed attack', the ICJ showed that the gap between the two is not necessarily big in *Oil Platforms* Case through holding that 'the Court does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the "inherent right of self-defence".' (*Oil Platforms (Islamic Republic of*

precise distinction between cyber armed attack concerning *jus ad bellum* [84] and cyber attack concerning *jus in bello*.[85] The distinction between armed attack and attack in the kinetic context is comparatively well-established in terms of LOAC and use of force. This confusion in using the term 'cyber attack' seems to come from the rhetorical expressions to conflate broader cyber security issues with cyber warfare; to conflate espionage, crime, and other acts of sabotage or coercion with actual conflict about a wide range of cyber operations.[86] It could be understood because any adverse action against a computer or a computer network is described as an attack in the media and technical literatures.[87] In the end, the use of the term 'attack' encompasses far more activities than that which falls within either the LOAC definition of attack or the *jus ad bellum* definition of attack.[88] In this regard, it is useful to understand how the terminology of cyber attack matches – or does not match – with the legal notions of attack in the relevant bodies of law.[89] Only restrictive kinds of cyber operations reported in the media can be regarded as a cyber attack in terms of LOAC.

Iran v. United States of America) (Merits) [2003] ICJ Rep 161 para 72) On the other hand, Dinstein suggests that 'use of force' is a wider term compared to an 'an armed attack'. (Yoram Dinstein, *War, Aggression and Self-Defence* (6th edn, CUP 2017) 205) In addition, he argues that 'what the gap denotes is that a use of force not involving loss of life or significant destruction of property falls sort of an armed attack. If a soldier of state A shoots across the border of state B, killing a cow, this is an instance of use of force. But absent a minimal degree of gravity, the act (albeit unlawful) does not rank as an armed attack.' (Yoram Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' 89 International Law Studies 276 279)

[84] About the distinction among cyber attacks amounting to an armed attack, use of force, or mere intervention, Russell Buchan, 'Cyber Attack: Lawful Uses of Force or Prohibited Interventions? ' 17 Journal of Conflict & Security Law 211.

[85] Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' 78.

[86] Ibid 85.

[87] Paul A. Walker, 'Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine' 1 National Secuirty Law Brief 33 36.

[88] Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' 89; Walker, 'Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine' 36.

[89] Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' 88.

AP I codified the definition of 'attack' as 'acts of violence against the adversary, whether in offence or defence'.[90] This would be a good starting point to define 'cyber attack'. Putting the definition of attack in the cyber context, cyber attacks may be first defined as violent cyber operations against the adversary, whether in offence or defence. In the kinetic sense of attack, an 'act of violence' is understood as having a negative kinetic effect, not limited to activities that release kinetic forces. In the case of chemical, biological, or radiological attacks, these means or methods of warfare in and of themselves do not release kinetic forces, while their effects are kinetically harmful.

By the same token, 'violent cyber operations' could be also understood as having a kinetic harmful effect against the targeted adversary.[91] That is to say, the concept of cyber attack takes the consequence-based approach, not instrument-based approach, which based on a weapon or an operation itself. The problem that arises with pushing the button on a keyboard is that usually the outcome that directly results is inherently non-violent in that pushing the button may start a distributed denial of service (DDoS) against a website, launch a computer worm program, or send a command to activate a malicious software program infiltrated into the network systems of the adversary. All those outcomes that could result from pushing the keyboard button, while not inherently violent in and of themselves,[92] invoke the malicious ICT actions of one sort

[90] Additional Protocol I, art 49(1)

[91] Roscini, *Cyber Operations and the Use of Force in International Law* 178-182.

[92] Walker, 'Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine' 40. (Yet, each of these actions, while not using force to cause injury, could easily fit within the expansive definition of 'computer network attack' in that denials of service can be used to disrupt websites or even to deny access to those websites, albeit only on a temporary basis.)

or another against computer network or information systems. Those actions have consequences that may or may not be the desired result of the button pusher. In this regard, a cyber operation that alters the running of a SCADA (Supervisory Control And Data Acquisition) system[93] controlling an electrical grid and brings about a fire qualifies as a cyber attack due to its violent consequences, even though it only uses a non-physical way of attack.

The *Tallinn Manual* 2.0 also defines a cyber attack as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[94] The ICRC regards cyber attacks in LOAC as 'cyber operations by means of virus, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked'.[95] After all, a cyber operation that destroys an object and causes damage to persons or objects is an attack. Cyber operations that interfere or cause inconvenience such as a denial of service for blocking the Internet are not considered to be attacks.[96] In conclusion, a cyber attack refers to a cyber operation, whether in offence or in defence, that brings about violent consequences against the adversary. By the definition of a cyber attack as such, non-violent cyber operations, such as

[93] 'Computer systems and instrumentation that provide for monitoring and controlling industrial, infrastructure, and facility-based processes, such as the operation of power plants, water treatment facilities, electrical distribution systems, oil and gas pipelines, airports, and factories.' (Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Glossary 567)

[94] Ibid (Rule 92 – Definition of cyber attack) 415.

[95] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* 37.

[96] Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' 93.

psychological cyber operations, cyber espionage and embargoes, do not qualify as attacks.[97]

Bearing in mind that the consequences of a cyber operation determine whether the operation constitutes an attack in terms of LOAC, some commentators include acts that result in neutralisation of objects, based on the definition of military objective, which talks of the destruction or neutralisation of an object that offers direct military advantage.[98] But, it is quite possible that the cyber operations neutralising an object, such as shutting down the electricity grid, without directly destroying it, qualifies an attack as long as the operations actually bring about violent consequences. After all, 'neutralisation' being referred at the article 52(2) of the AP I to interpret 'military objectives' does not add another category other than violent consequences for the definition of attack.[99]

The question then arises as to whether information itself is eligible to be a 'military objective' being subject to legitimate or legal targeting. In other words, would intangible assets such as information or data, which has a certain value, either in cyberspace or in reality, be considered the same as other tangible properties, which are objects of direct attacks in the conflict situation? Cyber operations against data

[97] Oona A. Hathaway and others, 'The Law of Cyber-Attack' 100 California Law Review 817 829; Owens, Dam and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* 11-12, 81; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 415.

[98] Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' (International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law) 4.

[99] Additional Protocol I, art 52(2) ('military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage'); Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare (1923 Hague Draft Rules of Air Warfare) (December 1922 - February 1923), art 24(1)

that is stored or installed in the adversary computer network system could also be considered as an attack as long as the operation results in the injury or death of people or damage or destruction of objects in terms of LOAC.

As seen above, cyber attacks are admitted in terms of LOAC as long as it brings about physically violent effects on the attacked computer systems or other targets in and through cyberspace. Then the question arises as to whether cyber operations which deteriorate some degree of functionality of an object constitute damage or destruction for the definition of attack. For example, after a cyber operation disrupts the computer-based control system of the electricity grid, if the operation causes the normal operating of the grid to cease and then some parts of the targeted system such as mainboard have to be replaced in order to resume the control system, would the concerned cyber operation be regarded as an attack?[100] The majority of the international group of experts working on the *Tallinn Manual* 2.0 takes the position that 'if restoration of functionality requires replacement of physical components', the concerned interference comes to attack.[101] On the other hand, there is another opinion to extend disruption to the extent that the functionality can be restored by reinstallation of the system or of particular data.[102] If a cyber operation hinders the targeted computer systems from performing their originally intended function and reinstallation is fully or partially required to restore the designed function of an object, the operation qualifies as an attack. In addition, a few experts suggest that interference with functionality that necessitates data restoration, while not requiring

[100] Robin Geiss, 'Cyber Warfare: Implications for Non-International Armed Conflicts' 89 International Law Studies 627 644-645.

[101] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 417.

[102] Ibid 417-418.

physical replacement of components or reinstallation of the operating system, qualifies as an attack.[103] From this point of view, when the target object loses its usability, the concerned operation satisfies the damage requirement for being an attack.[104]

The author takes the consequence-based approach as to whether a certain cyber operation qualifies as an attack in terms of LOAC. In this regard, cyber attacks via cyberspace or in itself should bring about violent effects on the adversary. Then, without considering the violent result outside of computer network system, putting in the same context, 'replacement' being physically required could be included as a kind of violent effects, whereas neither 'reinstallation' nor 'loss of functionality' would be excluded. The excessive considerations about functionality risk the concept of cyber attack based on its violent consequence in that this expansion of cyber attack gives rise to imprudent application of IHL rules, even though other rules of law, such as non-intervention, state responsibility, or criminal law, can still respond to the wrongful act. Reinstallation of the whole programme or restoration of data could lead to consuming more time and lessening more functionality rather than replacement of the components. Moreover, replacement could seem to be a sort of formal condition to juxtapose a cyber attack with a kinetic attack, not to be a substantial requisite coming from material differences between them. However, for the present, in which no one is able to exactly predict the possible future development of cyber operations, the author would rather not exclude replacement from cyber attack. It is still not inclusive of reinstallation and the loss of functionality because the consequence-based

[103] Ibid.

[104] Ibid 418.

approach for a ‘cyber attack’ cannot be sustained. It is also difficult to draw a clear line between cyber operations exceeding mere inconvenience and those which significantly disrupt ordinary functions of military or civilian critical infrastructures. Hence, replacement of the attacked objectives could only refer to violent consequence of cyber operations.

IV. Structure

This thesis focuses on how to offer the framework of classification of cyber armed conflicts on the basis of the existing criteria of classification in IHL. Prior to looking into the details of classification, chapter 2 deals with general changes of LOAC according to the development and application of science and technology in warfare from the historical perspective and then it finds that there has always been the course of tension and balance between ‘military necessity’ and ‘humanity’ as normative values to respond to new phenomena in the progress and development of IHL. Bearing in mind this mechanism to incorporate new phenomena in battlefield into IHL regime, chapter 3 examines international cyber armed conflict mainly characterised by actors being parties of the concerned conflict based on the fundamental concepts analysed in this chapter. As the first substantive criterion of classification, both parties to the conflict must be states or state-affiliated actors for being an IAC. In the case of state affiliation, it is necessary to prove whether actor’s conduct can be attributable to a state. Which attribution test would fit in cyber armed conflicts would also be considered as there has been several theories in international law. Then, the question as to whether intensity matters in IAC needs to be reconsidered in international cyber armed conflict. Chapter 4 examines non-

international cyber armed conflict. For the criterion of actors, an ‘organised armed group’ must be analysed especially ‘virtually’ organised armed groups in cyberspace. Then, for being a non-international cyber armed conflict, the intensity assessment is important to consider. To draw a line between a non-international cyber armed conflict and lower intensity of disturbance, the judicial reviews and decisions of international courts and tribunals are referenced. Lastly, chapter 5 first examines geographical issues in classification of kinetic armed conflicts. Then, it analyses the question whether a new type of TAC could be also required in the cyber context as argued in the situation of extraterritorial armed conflict in kinetic space and eventually answers the question whether geographical considerations should be included in classifying cyber armed conflicts. Reaching the end of those chapters, the characterisation of cyber armed conflicts will be more clearly outlined and the applicable rules of IHL for them will be identified.

Chapter 2 – Classification in International Humanitarian Law

I. Introduction

The main concern of this thesis is how to confirm the existence of cyber armed conflict being subject to the application of international humanitarian law (IHL) through examining the criteria of classification of armed conflict. Prior to research on the classification of cyber armed conflicts, it is necessary to examine the meaning of classification from the perspective of development of international law. This classification to determine whether an armed conflict exists in terms of IHL is based on the bifurcated structure of international armed conflict (IAC) and non-international armed conflict (NIAC) firmly established through a long history of the law of armed conflict (LOAC). As a very traditional area of international law, the law of warfare has developed not only by reflecting many novel changes in both technologies and ideologies but also by adjusting itself to new eras. For instance, the current IHL regime is already the product acquired by experiencing the two World Wars and humanitarian disasters including a number of civil wars, regional conflicts, terrorism, and so forth.

The changing character of war is first addressed in analysing cyber armed conflicts. It is necessary to understand how the development of science and technologies provoked changes in the performance and history of war. While some aspects of cyber warfare are a completely unique phenomenon, there has always been a relationship between technology and war which allows us to apply the existing IHL regime to

cyber armed conflict of today. In this regard, the first section of changing character of war describes how the development of information and communication technology (ICT) have concretely changed the character of war in the contemporary era, and then analyses the attitude and position which has been taken by the international community and states how to respond these changes.

The question of who identifies the legal character of a given conflict situation needs to be addressed because there are always more than two belligerent parties to the conflict, who must comply with the rules of IHL during hostilities, in any armed conflicts. Bearing in mind that no actual cyber armed conflict has been occurred yet to date, the course of classification established in the kinetic context is considered.

Lastly, the normative tension between military necessity and humanity that prevails over the whole IHL regime is examined to identify the normative principles that guides interpretation of IHL. New means and methods in an armed conflict are provided on the ground of military necessity with the development of science and technologies. At the same time, the obligation of humane treatment and humanitarian consideration should be taken into account whenever military necessity is required. These two common and fundamental normative values incarnated in LOAC would be examined not only in interpreting classification rules but also in examining legal *lacuna* for cyber armed conflicts. The balance between military necessity and humanitarian considerations should also be achieved in the characterisation of cyber armed conflicts.

II. Changing Character of War

1. Historical Development of War

Armed conflicts evolve over time but the legal framework does not always follow these factual developments. Before the Clausewitz's *On War*,[1] which is regarded as the preeminent work of war nature study in a historical context, there has been continuous change in war throughout history. However, this thesis starts from the somehow established concept of war such as Clausewitz's war definition. Clausewitz understands that the nature of war is a product of the relations between 'primordial violence, the interplay of probability and chance within it, and its subordination to politic'.[2] War features the presence of armed violence delivered through combat for the political or policy purpose, and 'war is always a human, moral, and social activity'.[3]

The contemporary concept of war came to be internationally legalised in detail after the experiences of the two World Wars.[4] The existing framework is essentially aligned to the Geneva Conventions[5] with some evolution in the 1970s via the

[1] Carl von Clausewitz, *On War (Translated by Michael Howard and Peter Paret)* (Oxford World's Classics 2007)

[2] Steven Haines, 'The Nature of War and the Character of Contemporary Armed Conflict' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 10.

[3] Ibid 10-12.

[4] Even though there had been some substantial conventions resulted from Hague Conferences of 1899 and 1907, and other instruments such as Kellogg-Briand Pact, the detailed concept of war used in contemporary era was established after World War II.

[5] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (Geneva Convention I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949 (adopted 12

Additional Protocols (APs).[6] Historically, Hugo Grotius in his *De jure belli ac pacis* discerned both concepts of war, just war and legal war (*bellum solemne*). The former is about the justice of war to the domain of national law, which applied in conscience, whereas the latter is about the legality of war to the domain of the positive law, which was externally enforceable.[7] Later, Oppenheim defined war as follows: 'war is a contention between two or more states through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.'[8] On the other hand, Dinstein, analysing war in the technical and in the material sense, defined war as 'a hostile interaction between two or more states, either in a technical or in a material sense. War in the material sense is generated by actual use of armed forces, which must be comprehensive on the part of at least one party to the conflict.'[9]

These conceptions of war can be summarised as follows: first, states had sustained a 'monopoly over war',[10] so most of the rules surrounding war were state-centric; second, the purpose (or motivation) of war had been legitimised or determined based

---

August 1949, entered into force 21 October 1950) 75 UNTS 85 (Geneva Convention II); Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Geneva Convention III); Geneva Convention Relative to the Protection of Civilian Persons in Time of War of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (Geneva Convention IV)

[6] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Additional Protocol II)

[7] Hugo Grotius, *De jure belli ac pacis libri tre* (1625); Marc Weller, 'Introduction: International Law and the Problem of War' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) 37, 41.

[8] L. Oppenheim, *International Law II War and Neutrality* (2 edn, Longmans, Green and Co. 1912) 60.

[9] Yoram Dinstein, *War, Aggression, and Self-defence* (5 edn, CUP 2011)

[10] Andreas Wenger and Simon J. A. Mason, 'The Civilianization of Armed Conflict: Trends and Implications' 90 IRRC 835 835.

on political, religious, cultural, ethical, or social reasons, not genuinely for material gain; third, the scope of battlefield had been somehow limited in location in both inter-state war and intra-state war. These conventional characteristics still partly remain in contemporary wars to date but there are different features of war that are emerging.

Regarding the changing character of war, some commentators suggest war generation theory and the recent war patterns are called as 'fourth generation of war'.[11] The so-called fourth generation war features all the changes in the above-mentioned three main features of conventional war.

First, states lost their monopolistic status in war and the role of non-state actors has come to be bigger and diverse. For example, civilian employees came to play an important role in maintaining and operating technically highly complex weapon systems in military force. For this kind of maintenance, establishing regular departments in the respective sector of military forces is non-economical. Thus, to improve the flexibility and efficiency in this area, military forces started to rely on the market and the rise of private military and security companies (PMSCs) appeared. For instance, after the Iraq war from 2007 to 2011, the US had hired civil contractors in

[11] Haines, 'The Nature of War and the Character of Contemporary Armed Conflict' 18-20; There is an articulated formula to explain the evolution of war with marking generation shifts to historical war developments. For example, William S. Lind constructs that the first generation of war ran roughly from 1648 to 1860. The relevance of the first generation springs from the fact that the battlefield of order created a military culture of order. This was gradually replaced with second generation of war developed by the French Army during and after World War I. The third generation of war, also a product of World War I, was developed by the German Army and is commonly known as blitzkrieg or manoeuvre warfare. Third generation war is based not on firepower and attrition but speed, surprise, and mental as well as physical dislocation. This third generation of war can cover the whole of World War II. Then, in the fourth generation of war, the most radical change is that states lose their monopoly on war with the appearance of non-state opponents such as al-Qaeda, Hamas, Hezbollah, and the Revolutionary Armed Forces of Colombia. (William S. Lind, 'Understanding Fourth Generation of War' 84 Military Review 12 12-14)

Iraq to assist or substitute its forces.[12] As the functions of PMSCs have extended close to the traditionally monopolistic role of states relating to the use of force, various legal problems engaged in private contractors have increased.[13] Implementing the principle of distinction in their tasks and regulations would be more difficult in case of a mix of services across private and governmental areas. This change of human resources in an armed conflict is more intensified in cyberspace in which individuals are capable to participate with anonymity and without proximity.

Revolutionary technological developments in military force[14] have major impacts on the relationship between military and civilian spheres as well. The involvement of civilians in hostilities of IAC and NIAC can be explained with two trends: one is the decline of inter-state wars and the technical revolution in military operations that

[12] Global Policy Forum, PMSCs in Iraq < https://www.globalpolicy.org/pmscs/50154-iraq.html > accessed 5 November 2018.

[13] In terms of LOAC, for example, the use of force by PMSC personnel in an armed conflict is regulated by different rules pursuant to their legal status in LOAC. The question of whether they are combatants belonging to a state party to the concerned conflict is problematic. Otherwise, even if they are civilians, the question of whether they are civilians directly participating in hostilities should also be examined.

[14] About military technology development, there is a vast amount of literature dedicated to the concept of 'revolution in military affairs' (RMA). Historical analysis of change and development in military affairs can be categorised into two main concepts: 'military revolution' and 'revolution in military affairs'. (Gil-li Vardi, 'The Change from Within' in Hew Strachan and Sibylle Scheipers (eds), *The Changing Character of War* (OUP 2011) 79-90) The concept of military revolution was introduced by Michael Roberts in 1955 to proclaim 'the originality, the importance, and the historical singularity of certain developments in the art of war in post-Renaissance Europe' between 1560 and 1660. (Geoffrey Parker, 'The "Military Revolution," 1560-1660 - a Myth?' 48 The Journal of Modern History 195 195) On the other hand, the concept of RMA could be more important for the thesis. RMA is defined as a *fundamental* change, or discontinuity, in the way military strategy and operations have been planned and conducted. (Barry R. Schneider and Lawrence E. Grinter (eds), *Battlefield of the Future 21st Century Warfare* (Air University Press 1998) 43) According to Andrew Marshall, RMA means 'a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organisational concepts, fundamentally alters the character and conduct of military operations'. 'Such revolutions have occurred many times in history for a variety of reasons. The most obvious cause is a technological 'push'. The invention of gunpowder, the steam engine, the submarine, the internal combustion engine, the airplane, the aircraft carrier, and the atom bomb are some of the most obvious innovations which led to fundamental changes in the conduct of warfare.' (Lothar Ibrügger, *The Revolution in Military Affairs - Special Report* (1998) NATO Parliamentary Assembly Science and Technology Committee http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html, accessed 29 February 2016)

evokes the growing role of civilians; the other is the increase of intra-state armed conflict and more pervasive role of civilian agents.[15] Since the end of the Cold War, the outbreak of NIAC has been increasing. In a NIAC, civilians are no longer only objects or the victims of hostilities. They are also participants as seen the rules of 'direct participating in hostilities' (DPH). Civilians are not only playing an ever-greater role in high-technology warfare but also an increasingly important and complex role in low-technology conflicts, as seen in various types of organised political violence within states. In situations where state institutions are weak or non-existent, the lines between the public and private domains are blurred; there is no clear state, no clear civil society, and therefore also no clear distinction between civilians and non-civilian players. Recently, total warfare between states has decreased whereas regional, local, and intra-state warfare has been increasing.[16] The end of the Cold War transformed the bipolar and state-centric security map into a multipolar and complex landscape because balance and stability by superpowers from the both ideological camps have decreased. Highly advanced technology incorporated into the military arena has also accelerated the blurring of the military and civilian domain. Among non-state entities, organised armed groups play an important role in NIAC with the comparatively concrete standards to identify it in LOAC.[17]

---

[15] Wenger and Mason, 'The Civilianization of Armed Conflict: Trends and Implications' 837-846.

[16] Ibid 850.

[17] Additional Protocol I

Article 1 – Material field of application

1. This Protocol, which develops and supplements article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol. (underlined by the author to emphasise.)

Second, the purpose of an armed conflict becomes more complicated and comprehensive than it has been historically. In the course of war, a financial or criminal goal could be mixed with a political one. This change makes it difficult to estimate the nature of the concerned conflict situation. For example, criminal activity with the intent to acquire material gain needs to be examined in terms of the change in the purpose of war. The definition of organised armed groups also needs to be scrutinised in this regard. Transnational organised criminal groups such as gangs (acting to gain material interests through drug dealing, human trafficking, arms dealing, extortion, or smuggling) use violence against state authorities or against rival criminal groups in the same area.[18] This kind of conflict could reach the identical level of violent intensity that would qualify it as an armed conflict if it were originated from political purpose. Clashes or insurgency between criminal gangs and a government have intensified to the point that they come to resemble gang warfare. In effect, Mexican authorities deal with a variety of gangs involved in hostilities against each other or with its security forces.[19] These gangs occasionally have an effective control of a certain area of territory, referred to as 'plazas'.[20] According to article 1(1) of the AP I, the term 'organised armed group' does not express whether it excludes criminal groups or not.[21] Therefore, if it could be claimed that a criminal organisation which takes a degree of territorial control, and conducts violent acts against a state or other organised armed groups to the extent that it can be regarded as

[18] Haines, 'The Nature of War and the Character of Contemporary Armed Conflict' 24.

[19] Ibid 25.

[20] John P. Sullivan and Adam Elkus, 'Plazas for Profit: Mexico's Criminal Insurgency' Small Wars Journal (26 April 2009) <http://smallwarsjournal.com/jrnl/art/plazas-for-profit-mexicos-criminal-insurgency> accessed 1 March 2016.

[21] Wenger and Mason, 'The Civilianization of Armed Conflict: Trends and Implications'.

the party to the concerned conflict, it could also be included in the category of organised armed groups, and then the whole situation could qualify as a NIAC.

On the contrary, organised armed groups that originally gathered for political purpose could expand their activities to criminal area to support their aims. This is a phenomenon more frequently seen in terrorism groups such as Al-Qaeda. However, this is easier to deal with because the fact that the organised group carries out criminal activities in addition to, or for the furtherance of, its original political purpose does not change the legal character of that organised group itself. Complications arise, though, when criminal gangs and politically motivated organised armed groups coalesce to pursue some strategic objective.[22] There would be some views that purely criminal activities prevent the concerned organised crime and the responses thereto from being deemed a NIAC. About this point, the International Committee of the Red Cross (ICRC) expressed that 'under IHL, the motivation of organised armed groups involved in armed violence is not a criterion for determining the existence of an armed conflict' by a strictly legal reading.[23] Cyberspace offers better opportunities and places for those terrorists to gather and organise their individual warriors, to train and command-and-control them, and to raise fund for their activities. Cyber organised groups could feature more diverse goals of their activities at the same time.

[22] Haines, 'The Nature of War and the Character of Contemporary Armed Conflict' 24.

[23] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (31st International Conference of the Red Cross and Red Crescent, 2011) 11; As the grounds of this, 'firstly, to introduce it would mean to open the door to potentially numerous other motivation-based reasons for denial of the existence of an armed conflict. Secondly, political objective is a criterion that would in many cases be difficult to apply as, in practice, the real motivations of armed groups are not always readily discernible; and what counts as a political objective would be controversial. Finally, the distinction between criminal and political organisations is not always clear-cut; it is not rare for organisations fighting for political goals to conduct criminal activities in parallel and vice versa.' (ibid)

Third, geographical limitations in an armed conflict have more or less vanished and the physical battlefield has expanded to the virtual space and 'ultimately the human mind' through the revolution in military affairs.[24] In other words, the object of warfare and the concept of attack have evolved from physical destruction of the adversary's military force to virtual control over, or incapacitation of, cyberspace. For example, the so-called extraterritorial armed conflict in kinetic space, which does not fully fit with common article 3 of the Geneva Conventions and AP II, made an appearance. Accordingly, there has been an argument that a new type of an armed conflict, 'transnational armed conflict' (TAC) needs to be recognised in LOAC. [25] Terrorist networks such as Al-Qaeda benefit from the existence of weak states and lawless regions. By exploiting the vulnerability of global markets and modern infrastructures, they wage their battle in geographically remote areas. A similar loss in the protective function of geography is also apparent in the realm of organised crime and the illegal trafficking of both people and goods. Violent political conflicts today are likely characterised by asymmetric structures, and thus marked by a growing involvement of civilians. For example, the United States, which seemed to demonstrate invincibility in conventional warfare, could only be outmanoeuvred by asymmetric warfare. The recent events in Palestine, Lebanon, Iraq, Iran, Afghanistan, and Pakistan reveal just how geographical borders seem to disintegrate amid asymmetric conflicts. The most obvious feature of this change appears in respect of cyber armed conflict. Irrespective of international cyber armed conflict or non-

[24] Wenger and Mason, 'The Civilianization of Armed Conflict: Trends and Implications' 839.

[25] Extraterritorial armed conflict refers to the conflict situation between a state and a non-state actor that takes place, at least in part, outside the territory of the state. For more details, see, Chapter 5 – Transnational Cyber Armed Conflict?

international cyber armed conflict, it is almost impossible to clearly draw the geographical lines in actual cyber armed conflict situations.[26]

2. Emergence of Cyber Conflict

Schmitt examines three challenging aspects of conflict; the emergence of cyber warfare, the continuation of transnational terrorism, and the increasing complexity of cyberspace as a battlespace.[27] These three aspects seem interconnected to each other in the direction of strengthening challenges with the first two likely contributing to the complexity of the third.[28] In conclusion, it is predictable that the evolvement of cyber armed conflict and cyberspace will have a great impact on every area of the LOAC.

Cyber armed conflict is unique and strong in that all the above-mentioned changes are intermingled with each other. Civilianisation, purpose changes, and the collapse of geographical limits in war are all closely involved in cyber development. At this point, cyber armed conflict is the most revolutionary development to impact on the paradigm of modern warfare in history. The question then arises as to whether the advent of cyber means and methods of warfare are completely novel phenomena in the history of war. Otherwise, it is necessarily useful to look into similar historical experiences of technological development that had an impact on war. Through this analysis, it would be possible to understand what aspects of cyber armed conflict are comparatively unique and noteworthy in terms of LOAC. Compared to submarine and

[26] About 'geography' of cyber armed conflict, see, Chapter 5 – Transnational Cyber Armed Conflict?

[27] Michael N. Schmitt, 'Classification in Future Conflict' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 455-477.

[28] Haines, 'The Nature of War and the Character of Contemporary Armed Conflict' 31.

nuclear weapons appeared in relatively recent times in military arm system, the influence of cyber is more inclusive and comprehensive.

In case of submarines, with this new technology, a new set of rules dealing with this were incorporated into the existing law of maritime war.[29] The international rules governing the conduct of submarine warfare are divided into three branches of international law: the law of the sea, the law of neutrality, and the law regulating the conduct of military operations (the latter two are included in IHL).[30] With regard to nuclear weapons, due to the unprecedented violent power and its definitive sweeping capacity of destruction, states decided to establish an independent regime only for nuclear powers in the form of the NPT (Treaty on the Non-Proliferation of Nuclear Weapons) regime.[31] These two developments give examples of how to possibly regulate cyber armed conflict: one is, as seen in submarine example, that cyber armed conflict can be regulated by the existing regime of IHL by direct application, analogical application, or if necessary, partial amendment; the other is, like the NPT regime, the invention of a novel system suitable for cyber armed conflict.

There are two big streams that states take their positions about the regime for cyber armed conflict. First, the group of western states centred by North-Atlantic Treaty

[29] A. Pearce Higgins, 'Submarine Warfare' 1 BYBIL 149 ('the advent of the submarine does not require the making of new laws, that the old rules are sufficient, but need rigid enforcement.')

[30] Ashley Roach, 'Legal Aspects of Modern Submarine Warfare' 6 Max Plank Yearbook of United Nations Law 367 368.

[31] Treaty on the Non-Proliferation of Nuclear Weapons (adopted 1 July 1968, entered into force 5 March 1970) 729 UNTS 161 (NPT); 'Nuclear weapons constitute a category of their own that sets them apart from all other known weapons. In the absence of effective defence, mutual deterrence is the only protection against them.' (Azar Gat, 'The Changing Character of War' in Hew Strachan and Sibylle Scheipers (eds), *The Changing Character of War* (OUP 2011) 41) Furthermore, the states that have or are capable of developing nuclear weapons are limited in number, whereas cyber warfare capacity is far more accessible to all the states, and even to individuals.

Organisation (NATO) member states have taken the former position: there is no need to establish a new special regime only for cyber armed conflict.[32] They argue for maintaining the current IHL regime to apply to cyber conflict directly or by analogy.[33] Second, the other group of states, represented by China and Russia, insist on founding a special regime analogous to the international NPT regime for cyber security.[34] This framework would be equipped with treaties and, if needed, special international institutions. This direction could have inherent legitimacy because the international community established similar special regimes such as treaties ruling the Arctic, the Antarctic, canals, international rivers, and outer space throughout history.[35]

The Shanghai Cooperation Organisation (SCO) member states[36] agreed that the existing treaties lack adequate codes of conduct in communications between different countries, omitting a broad spectrum of cyber security abuses, which could escalate into cyber conflict. In September 2011, a Draft Convention on International Information Security was released at the 'international meeting of high-ranking

---

[32] Jeffrey T.G. Kelsey, 'Hacking into International Humanitarian Law: the Principles of Distinction and Neutrality in the Age of Cyber Warfare' 106 Michigan Journal of International Law 1427 1430-1431.

[33] Rex Hughes, 'A Treaty for Cyberspace' 86 International Affairs 523 535; Jack Goldsmith, 'Cybersecurity Treaties - A Skeptical View' *Future Challenges in National Security and Law,* edited by Peter Berkowitz <http://www.futurechallengesessays.com> ; Benjamin Mueller, *The Laws of War and Cyberspace: On the Need for a Treaty Concerning Cyber Conflict* (LSE IDEAS Strategic Update 2014) 5, 10-11.

[34] John Markoff and Andrew E. Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace' *The New York Times* (27 June 2009) <http://www.nytimes.com/2009/06/28/world/28cyber.html> accessed 18 June 2016; Stephen Moore, 'Cyber Attacks and the Beginnings of an International Cyber Treaty' 39 North Carolina Journal of International Law & Commercial Regulation 223 251-254; Mueller, *The Laws of War and Cyberspace: On the Need for a Treaty Concerning Cyber Conflict*.

[35] The Antarctic Treaty (adopted 1 December 1959, entered into force 23 June 1961) 402 UNTS 71; Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (adopted 27 January 1967, entered into force 10 October 1967) 610 UNTS 205; Rex Hughes, 'Towards a Global Regime for Cyber Warfare' in Christian Czosseck and Kenneth Geers (ed), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009) 8.

[36] China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. < http://www.sectsco.org/EN123/> accessed 5 November 2018.

officials responsible for security matters' in Yekaterinburg, Russia.[37] Then, in 12 September 2011, China, Russia, Tajikistan, and Uzbekistan jointly presented an International Code of Conduct for Information Security at the UN.[38] In contrast, the rest of states have not shown a special movement towards special regime or treaty for cyber conflict. In 2015, those countries again proposed an International Code of Conduct for Information Security to the UN General Assembly.[39] Later on 25 June 2016, Russia and China jointly proclaimed the Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law. In the document, two states argue that 'states have the right to participate in the making of, interpreting and applying international law on an equal footing, and have the obligation to comply with international law in good faith and in a coherent and consistent manner.'[40] They express their intention not to follow the international legal order established only by Western states.[41] The attitude of the two states is also consistent with their stance toward international law development about cyber armed conflict.

---

[37] Conflict Studies Research Centre and Institute of Information Security Issues (Moscow State University), *Russia's "Draft Convention on International Information Security" A Commentary* (2012)

[38] UN General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/66/359 14 September 2011)

[39] UN General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/69/723 13 January 2015)

[40] The Ministry of Foreign Affairs of the Russian Federation, *The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law* (2016) <http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2331698 > accessed 28 June 2016.

[41] Ibid.

6. The Russian Federation and the People's Republic of China share the view that good faith implementation of generally recognized principles and rules of international law excludes the practice of double standards or imposition by some states of their will on other states, and consider that imposition of unilateral coercive measures not based on international law, also known as «unilateral sanctions», is an example of such practice. The adoption of unilateral coercive measures by states in addition to measures adopted by the United Nations Security Council can defeat the objects and purposes of measures imposed by the Security Council and undermine their integrity and effectiveness.

One source points out there is no international consensus on the application of LOAC to current cyber conflicts and then insists that the time is ripe to begin building up a global cyber security regime to bring normative clarity to the cases of cyber conflicts under the Charter system.[42] However, the law, as it stands, could capture most of these new phenomena. It is natural in every law field that factual developments precede legal ones.[43] It is always unavoidable to witness some degree of legal void or mismatch between fact and law. A degree of indeterminacy that the law should catch up remains as well. The lawyers' role is important at this point as they have a duty to prevent a chaotic situation even in the situation of legal *lacuna* or mismatching. Thus, we must undertake interpreting the existing positive law as much as possible to solve these legal *lacuna* and mismatches, even when the process of discussing a new regime is underway. LOAC may continue to be applied to cyber armed conflict, unless the international community and states reach an agreement to invent a new separate regime for it, as they did in the case of landmines[44] and the NPT. It is worthwhile to examine a framework of classification of cyber armed conflict in order to apply the existing rules of IHL and clarify what new rules or modifications may be necessary.

[42] Hughes, 'Towards a Global Regime for Cyber Warfare' 5-6.

[43] William H. Boothby, 'The Legal Challenges of New Technologies: An Overview' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Springer 2014) 24-27.

[44] Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction (adopted 18 September 1997, entered into force 1 March 1999) 2056 UNTS 211.

III. Classification of Armed Conflicts

In order to determine whether or not IHL applies to a certain situation of violence, it must first be assessed whether or not that situation amounts to an 'armed conflict'. The legal framework governing armed conflict situations is called IHL (or LOAC), which deals with rights and duties of the parties to the armed conflict based on the principles of humanity and military necessity.[45] IHL consists of 'Geneva law', which mainly addresses the protection of victims, and 'Hague law',[46] which mainly

[45] Jonathan Crowe and Kylie Weston-Scheuber, *Principles of International Humanitarian Law* (Edward Elgar 2013) 24-43.

[46] Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulation concerning the Laws and Customs of War on Land (adopted 29 July 1899, entered into force 4 September 1900) 32 Stat. 1803 (Hague Convention II); Convention (III) for the Adaptation to Maritime Warfare of Principles of the Geneva Convention of 22 August 1864 (adopted 29 July 1899, entered into force 4 September 1900) 32 Stat. 1827; Convention (IV) Concerning the Prohibition of Launching of Projectiles and Explosives from Balloons (adopted 29 July 1899, entered into force 4 September 1900) 32 Stat. 1839; Hague Convention (IV), Declaration I Concerning the Prohibition, for the Term of Five Years, of the Launching of Projectiles and Explosives from Balloons or Other New Methods of a Similar Nature (adopted 29 July 1899, entered into force 4 September 1900) 32 Stat. 1839; Hague Convention (IV), Declaration II Concerning the Prohibition of the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases (adopted 29 July 1899, entered into force 4 September 1900) 187 Consol. T.S. 453; Hague Convention (IV), Declaration III Concerning the Prohibition of the Use of Bullets Which Expand or Flatten Easily in the Human Body (adopted 29 July 1899, entered into force 4 September 1900) 187 Consol. T.S. 459; Convention (III) Relative to the Opening of Hostilities (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2259 (Hague Convention III); Convention (IV) Respecting the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2277 (Hague Convention IV); Convention (IV) Respecting the Law and Customs of War on Land and its Annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2277 (Hague Regulations); Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2310 (Hague Convention V); Convention (VI) Relating to the Status of Enemy Merchant Ships at the Outbreak of Hostilities (adopted 18 October 1907, entered into force 26 January 1910) 205 Consol. T.S. 305 (Hague Convention VI); Convention (VII) Relating to the Conversion of Merchant Ships into War-Ships (adopted 18 October 1907, entered into force 26 January 1910) 205 Consol. T.S. 319 (Hague Convention VII); Convention (VIII) Relative to the Laying of Automatic Submarine Contact Mines (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2332 (Hague Convention VIII); Convention (IX) Concerning Bombardment by Naval Forces in Time of War (adopted 18 October 1907, entered into force 26 January 1910) 205 Consol. T.S. 345 (Hague Convention IX); Convention (X) for the Adaptation to Maritime War of the Principles of the Geneva Convention (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2371 (Hague Convention X); Convention (XI) Relative to Certain Restrictions With Regard to the Exercise of the Right of Capture in Naval War (18 October 1907, entered into force 26 January 1910) 36 Stat. 2396 (Hague Convention XI); Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War (18 October 1907, entered into force 26 January 1910) 36 Stat. 2415.

addresses the means and methods of concrete warfare.[47] In particular, Geneva law, represented by the Geneva Conventions of 1949 and their APs,[48] consists of two categories of rules: one is for IAC [49] and the other is for NIAC.[50] At this point, we can touch on why the classification of conflicts is relevant. When a conflict occurs, identifying its legal character has an immediate priority because the appropriate set of rules applicable to that conflict can be determined by its characterisation. That is to say, classification (or characterisation) of an armed conflict as IAC or NIAC is the preliminary step in applying IHL to cyber armed conflicts.[51]

[47] The ICJ explained that Hague law 'fixed the rights and duties of belligerents in their conduct of operations and limited the choice of methods and means of injuring the enemy in an international armed conflict', while Geneva Law 'protects the victims of war and aims to provide safeguards for disabled armed forces personnel and persons not taking part in the hostilities'. 'These two branches of the law applicable in armed conflict have become so closely interrelated that they are considered to have gradually formed one single complex system, known today as international humanitarian law. The provisions of the Additional Protocols of 1977 give expression and attest to the unity and complexity of the law.' (*Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 para 75); Keiichiro Okimoto, *The Distinction and Relationship between Jus ad Bellum and Jus in Bello* (Hart Publishing 2011) 6-12; Crowe and Weston-Scheuber, *Principles of International Humanitarian Law* 1-43; Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn, CUP 2016) 1-24; Dieter Fleck, *The Handbook of International Humanitarian Law* (2 edn, OUP 2008) 45-57.

[48] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (Geneva Convention I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (Geneva Convention II); Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Geneva Convention III); Geneva Convention Relative to the Protection of Civilian Persons in Time of War of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (Geneva Convention IV); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Additional Protocol II)

[49] Geneva Conventions I-IV, art 2; Additional Protocol I

[50] Geneva Conventions I-IV, art 3; Additional Protocol II

[51] Jelena Pejić, 'Status of armed conflicts' in Elizabeth Wilmshurst & Susan Breau (ed), *Perspectives on the ICRC Study on Customary International Humanitarian Law* (CUP 2007) 77.

In classifying a given conflict situation, the very first question to arise is who will assess and characterises it in a legal way. Put it another way, it could be about the question whether classification is subjective or objective. If it is subjective, the assessment by the concerned parties to the conflict over a given situation would be regarded critical. Otherwise, objective assessment by other entities such as the international community would be important. This issue needs to be respectively examined in international and non-international armed conflicts.

Since the Geneva Conventions started to use the concept of armed conflict to convey the idea that humanitarian law needs to apply whenever armed forces battled with each other, regardless of official classification, characterising an IAC in case of inter-state war does not create major problems. Instead, the objective nature of the term armed conflict guarantees that lack of official recognition would not impede an application of IHL as long as at least two contracting states are involved.[52] This idea is also confirmed by the International Court of Justice (ICJ) in its *Wall* Advisory Opinion.[53] Pictet's commentary emphasises that even one wounded soldier may trigger the application of the Geneva Conventions in an IAC.[54] On the other hand, for instance, as long as the concerned states form a consensus of regarding what has occurred as a mere incident, and provided that the incident finishes quickly and has no influence on other states, it would be hard to rebut such a determination. The

[52] Andreas Paulus and Mindia Vashakmadze, 'Asymmetrical War and the Nothing of Armed Conflict - A Tentative Conceptualization' 91 IRRC 95 98.

[53] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136 para 95.

[54] Jean S. Pictet (ed) *The ICRC Commentary I on the Geneva Convention of 12 August 1949* (ICRC 1952) 32; There are attempts to apply the intensity criterion restrictively and not to regard small-scale military confrontations between states as a triggering event of an IAC. (Mary Ellen O'Connell, 'Defining Armed Conflict' 13 Journal of Conflict & Security Law 393 393-400)

violence, where more than two states' armed forces involved can be objectively regarded as an IAC, while there is still another possibility for them to subjectively regard the violence as a mere incident. However, the latter approach cannot be accepted on the basis of the object and purpose of IHL that intends to expand humanitarian protection as wide as possible in IAC.[55]

Rather, very low intensity level required to be an IAC compared to that of a NIAC seems to make state parties to the conflict confused in interpreting the legal nature of the concerned conflict situation. In terms of NIAC, the rules of IHL obviously requires a certain level of intensity exceeding 'internal disturbances and tensions such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts' compared to IAC.[56] The reason why the concerned states regard as a mere incident may be due to its very much low intensity not due to the consensus between them. Thus, it can be said that the characterisation of IAC based on the criteria of 'actors' and 'intensity' is an objective process.[57]

The question of who determines the classification of armed conflict seems more complicated with regard to intra-state conflicts.[58] If taking a purely subjective

[55] Geneva Conventions I-IV, art 2

… The Convention shall apply to any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. (underlined by the author) …

[56] Additional Protocol II, art 1(2)

[57] Andrew Clapham, 'The Concept of International Armed Conflict' in Andrew Clapham, Paola Gaeta and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015) 12, 16.

[58] In the specific context of the AP II, the issue of who would decide whether the threshold of NIAC in the AP II is surpassed was discussed among states. There were by and large three positions: some states took the position that the High Contracting Party on whose territory the concerned conflict was taking place would make the decision; another state took the position that both the concerned state and organised armed groups would make the decision; and, the third group of states took the position that an objective determination of the concerned situation is required. (*Official Records of the Diplomatic*

approach in assessing the existence of NIAC, there may be far less chance for internal confrontation to be classification as a NIAC rather than internal disturbances. This is because states tend to negate the existence of NIAC regulated by IHL within their territories. States may seek to downplay the violence, whereas non-state armed groups may tend to exaggerate it.[59] States prefer to claim a given situation as a domestic issue calling armed groups as criminals or terrorists. That is to say, characterisation of a given situation in the legal sense could be different depending on the subject who assesses the situation. Since parties to the conflict are highly likely to assess the situation in favour of themselves, it seems more justifiable to characterise the violence from the objective viewpoint of neutral observers.[60] On this point, the International Criminal Tribunal for Rwanda (ICTR) took the same position that 'the ascertainment of the intensity of a NIAC does not depend on the subjective judgement of the parties to the conflict'.[61]

Looking into a comparatively recent practice, in the case of Syrian civil war, the Syrian government had denied the existence of a NIAC within its territory and argued that it was an internal rebellion or riots.[62] However, at a certain point, the ICRC officially and carefully proclaimed the existence of a NIAC in Syria and evoked the

---

Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict (1974-1977) Vol 8) The discussion shows some implications surrounding a general issue of this section, who determines intensity.

[59] Sandesh Sivakumaran, *The Law of Non-International Armed Conflict* (OUP 2012) 156.

[60] However, if so, there could be the remaining concern that the characterisation may have 'minimal impact on the parties to the conflict'. (ibid)

[61] *The Prosecutor v. Jean-Paul Akayesu* (Judgement) ICTR-96-4-T, T Ch I (2 September 1998) para 603.

[62] Louise Arimatsu and Mohbuba Choudhury, *The Legal Classification of the Armed Conflicts in Syria, Yemen and Libya* (Chatham House International Law PP 2014/01, 2014) 7-12.

parties to that conflict to comply with the rules of IHL.[63] Although this statement from the ICRC in and of itself has no binding effect in the legal sense, it cannot be ignored that the recognition by ICRC brought about considerable effects on the international community as an authoritative international humanitarian institution.[64] Likewise, the existence of NIAC seems unlikely to be determined in one go and as it arises, rather seems likely to be decided as it gradually progresses and the recognition of its existence spreads over the international community.

According to the report of the Independent International Commission of Inquiry on the Syrian Arab Republic, 'since the outset, civilians have borne the brunt of the suffering inflicted by the warring parties'.[65] The report claimed that 'the violence in the Syrian Arab Republic evolved from unrest in March 2011 into internal disturbances and the emergence of a NIAC in February 2012.'[66] Furthermore, the

[63] ICRC, *Syria: Parties to the Fighting Must Distinguish between Civilians and Fighters* (News Release 27 May 2012) < https://www.icrc.org/en/doc/resources/documents/news-release/2012/syria-news-2012-05-27.htm> accessed 25 April 2016; 'Syria in Civil War, Red Cross Says' *BBC NEWS* (15 July 2012) <http://www.bbc.co.uk/news/world-middle-east-18849362> accessed 3 June 2015 ICRC, *Syria: Parties to the Fighting Must Distinguish between Civilians and Fighters*Later, the Syrian Government also admitted the situation as a NIAC. (James Crawford, 'Sovereignty as a Legal Value' in James Crawford and Martti Koskenniemi (eds), *The Cambridge Companion to International Law* (CUP 2012))

[64] B. S. Chimni, 'Legitimating the International Rule of Law' in James Crawford and Martti Koskenniemi (eds), *The Cambridge Companion to International Law* (CUP 2012); Els Debuf, 'Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities' 97 IRRC 319; Tristan Ferraro, 'The ICRC's Legal Position on the Notion of Armed Conflict Involving Foreign Intervention and on Determining the IHL Applicable to This Type of Conflict' 97 IRRC 1227.

[65] The Independent International Commission of Inquiry on the Syrian Arab Republic, *Report of the Independent International Commission of Inquiry on the Syrian Arab Republic* (2015) A/HRC/28/69 para 2.

[66] Ibid para 1; In this report, the Commission characterises the concerned situation by the timeline: 'as protests erupted in Dara'a city in March 2011, government forces opened fire on demonstrators. As the unrest evolved into armed violence in late 2011, the Government intensified its ground assaults on restive areas. By 2012, as the country moved towards civil war, government forces had committed a number of mass killings of civilians during ground assaults.' (ibid para 7-8) It shows the Commission as a subsidiary international organisation assesses the development of the concerned situation on the basis of both intensity and organisation criteria for characterising a NIAC. For the intensity assessment, the Commission considered the details of weapons and tactics used by the governmental forces in actual conflict.

commission concluded that government forces and anti-government fighters had committed the crimes against humanity of murder and torture, war crimes and gross violations of international human rights and humanitarian law.[67]

In conclusion, characterising a NIAC can be also said to be an objective process to assess the intensity of a given conflict situation and to identify the actors involved in that situation. On the other hand, the recognition or stance of the parties to the conflict cannot be completely ignored in reality in such a case of invitation of humanitarian aids from outside. Nevertheless, there is no alteration that classification of armed conflicts should be examined on the basis of legal standards from the objective perspective in the end.

IV. Military Necessity and Humanity: Normative Values

The principle of humanity, or humanitarian consideration, which operates to protect the population (whether combatants or non-combatants) and its property, permeates the whole IHL mechanism. The preamble to the 1868 St Petersburg Declaration states that 'considering that the progress of civilisation should have the effect of alleviating as much as possible the calamities of war; … the employment of such arms would therefore be contrary to the law of humanity'.[68] In *Corfu Channel* case, the ICJ confirmed that 'elementary considerations of humanity' is a general and well-

[67] The Independent International Commission of Inquiry on the Syrian Arab Republic, *Syrian Government forces and anti-Government groups responsible for war crimes: UN Commission of Inquiry* Press release (15 August 2012) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/PRCoISyria15082012_en.pdf> accessed 29 April 2018.

[68] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Saint Petersburg, 29 November / 11 December 1968 <https://ihl-databases.icrc.org/ihl/INTRO/130?OpenDocument> accessed 25 October 2018.

recognised principle of international law.[69] The ICJ, in the advisory opinion on *Nuclear Weapon*, also held that the principle is an 'intransgressible principle of international customary law'.[70] Martens Clause,[71] which refers to customary law and is self-evident, shows that IHL is an exception of the positivist premise that all which is not forbidden in international law is permitted. In the advisory opinion on *Nuclear Weapons*, the ICJ confirmed that 'the Martens Clause, whose continuing existence and applicability is not to be doubted, as an affirmation that the principles and rules of humanitarian law apply to nuclear weapons.'[72] Article 1(2) of the AP I also stipulates the principle of humanity as well.[73]

On the other hand, the principle of military necessity shores up the IHL system by safeguarding states' 'ability to pursue and safeguard vital national interests'.[74] Means and methods taken in an armed conflict are driven to gain military advantages over the enemy. This principle recognises the appropriateness of considering military

---

[69] *Corfu Channel case* (Merit) [1949] ICJ Rep 4 22.

[70] *Legality of the Threat or Use of Nuclear Weapons* para 79.

[71] Martens Clause was introduced in the Preamble to the 1899 Hague Convention II on the Laws and Customs of War on Land, taking its name from a statement by Fyodor Fyodorovich Martens, the Russian delegate at the Hague Peace Conferences of 1899. The original text read as follows: 'Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.'; More about the Martens Clause, Theodor Meron, 'The Martens Clause, Principles of Humanity, and Dictates of Public Conscience' 94 AJIL 78.

[72] *Legality of the Threat or Use of Nuclear Weapons* para 87.

[73] Additional Protocol I, art 1

2. 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. (underlined by the author)

[74] Michael N. Schmitt, 'Military Necessity and Humanity in Internaitonal Law: Preserving the Delicate Balance' 50 Virginia Journal of International Law 795 799.

factors in setting the rules of warfare.[75] In other words, states, as the first existence of crafting IHL, therefore insist that 'legal norms not unduly restrict their freedom of action on the battlefield, such that national interests might be affected'.[76] The discourse of military necessity can be developed in each individual practice or associated with a certain provision of law in the way that some military necessity is considered for a kind of conduct. Military necessity comes out prominently in the 1863 Lieber Code,[77] which appeared during the Civil War.[78] Military necessity has been contemplated as deviation from a rule grounded in humanitarianism of some IHL rules, which mostly address protecting property, such as Hague Regulations

[75] Ibid 798-799.

[76] Ibid.

[77] U.S. War Department, General Order No. 100, 24 April 1863; Burrus M. Carnahan, 'Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity' 92 AJIL 213.

[78] Instructions for the Government of Armies of the United States in the Field (Lieber Code)

Article 14

Military necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war.

Article 15

Military necessity admits of all direct destruction of life or limb of 'armed' enemies, and of other persons whose destruction is incidentally 'unavoidable' in the armed contests of the war; it allows of the capturing of every armed enemy, and every enemy of importance to the hostile government, or of peculiar danger to the captor; it allows of all destruction of property, and obstruction of the ways and channels of traffic, travel, or communication, and of all withholding of sustenance or means of life from the enemy; of the appropriation of whatever an enemy's country affords necessary for the subsistence and safety of the army, and of such deception as does not involve the breaking of good faith either positively pledged, regarding agreements entered into during the war, or supposed by the modern law of war to exist. Men who take up arms against one another in public war do not cease on this account to be moral beings, responsible to one another and to God.

Article 16

Military necessity does not admit of cruelty -- that is, the infliction of suffering for the sake of suffering or for revenge, nor of maiming or wounding except in fight, nor of torture to extort confessions. It does not admit of the use of poison in any way, nor of the wanton devastation of a district. It admits of deception, but disclaims acts of perfidy; and, in general, military necessity does not include any act of hostility which makes the return to peace unnecessarily difficult.

article 23(g),[79] article 53 of the Geneva Convention IV,[80] article 54(5), 62(1), 67(4), 71(3) of the AP I,[81] and article 17 of the AP II.[82]

When one party to the conflict brings a certain military operation into consideration, it starts from military necessity for the 'proper purpose or legitimate ends'[83] to achieve a

[79] Hague Regulations, art 23

In addition to the prohibitions provided by special Conventions, it is especially forbidden

(g) To destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war; (underlined by the author)

[80] Geneva Convention IV, art 53

Any destruction by the Occupying Power of real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations, is prohibited, except where such destruction is rendered absolutely necessary by military operations.

[81] Additional Protocol I

Article 54 – Protection of objects indispensable to the survival of the civilian population

5. In recognition of the vital requirements of any Party to the conflict in the defence of its national territory against invasion, derogation from the prohibitions contained in paragraph 2 may be made by a Party to the conflict within such territory under its own control where required by imperative military necessity.

Article 62 – General protection

1. Civilian civil defence organizations and their personnel shall be respected and protected, subject to the provisions of this Protocol, particularly the provisions of this Section. They shall be entitled to perform their civil defence tasks except in case of imperative military necessity.

Article 67 – Members of the armed forces and military units assigned to civil defence organisations

4. The *matériel* and buildings of military units permanently assigned to civil defence organizations and exclusively devoted to the performance of civil defence tasks shall, if they fall into the hands of an adverse Party, remain subject to the laws of war. They may not be diverted from their civil defence purpose so long as they are required for the performance of civil defence tasks, except in case of imperative military necessity, unless previous arrangements have been made for adequate provision for the needs of the civilian population.

Article 71 – Personnel participating in relief actions

3. Each Party in receipt of relief consignments shall, to the fullest extent practicable, assist the relief personnel referred to in paragraph 1 in carrying out their relief mission. Only in case of imperative military necessity may the activities of the relief personnel be limited or their movements temporarily restricted.

(underlined by the author)

[82] Additional Protocol II, art 17 – Prohibition of forced movement of civilians

1. The displacement of the civilian population shall not be ordered for reasons related to the conflict unless the security of the civilians involved or imperative military reasons so demand. Should such displacements have to be carried out, all possible measures shall be taken in order that the civilian population may be received under satisfactory conditions of shelter, hygiene, health, safety and nutrition. (underlined by the author)

goal in the concerned armed conflict. Then, at the same time, that military operation should satisfy the standards of legitimacy and legality. Proportionality test would be used for the sake of getting this legitimacy.[84] There are several factors or concepts such as 'unnecessary suffering', [85] 'superfluous injury',[86] and 'incidental injury and collateral damage',[87] which are anticipated from the considered military operation, contemplated in the process of proportionality test of the military operation. It is a humanitarian consideration that is reflected in these proportionality tests. Hence, it concludes that militarily required operations in practice are legalised and legitimised by complying with the rules of IHL, which is established upon the two prominently fundamental pillars of humanitarianism and military necessity.

---

[83] Rotem M Giladi, 'Reflections on Proportionality, Military Necessity and the Clausewitzian War' 45 Israel Law Review 323 325.

[84] 'The term proportionality recurs across an array of disciplines and usages; each conveys legally distinct meanings and applications as a technical matter such as the application of proportionality in both *jus ad bellum* and within *jus in bello*. The same term has very different meanings with often profound and context specific implications.' The principle of proportionality hereof refers to 'the rule that limits the severity of lethal force so that it only is properly employed in a way that is commensurate with the goal to be achieved'. (Michael Newton and Larry May, *Proportionality in International Law* (OUP 2014) 2-3)

[85] Hague Regulations, art 23

In addition to the prohibitions provided by special Conventions, it is especially forbidden

(e) To employ arms, projectiles, or material calculated to cause unnecessary suffering;

(underlined by the author)

[86] Additional Protocol I, art 35 – Basic rules

2. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering. (underlined by the author)

[87] 'Collateral damage, also called incidental damage, consists of both unavoidable and unintentional damage to civilian personnel and property incurred while attacking a military objective. Incidental damage is *not* a violation of international law. While no LOAC treaty defines this concept, its inherent lawfulness is implicit in treaties referencing the concept.' (The US Judge Advocate General's Legal Centre and School, *Operational Law Handbook* (17th ed. U.S. Army 2017) 18) Then, article 51(5) of the AP I suggests some a clue in referring to 'indiscriminate attack'.

Additional Protocol I, art 51 – Protection of the civilian population

5. Among others, the following types of attacks are to be considered as indiscriminate:

b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated. (underlined by the author)

In regards to the relationship between military necessity and humanity as underlying normative values of LOAC, the major opinion argues that these two values take an antipodal position and require adjusting their balance in each norm of IHL.[88] The other opinion takes the position that these two values are not inevitably conflictual but should be jointly satisfied.[89] However, the latter opinion does not seem to vary from the former that much; military necessity and humanitarian considerations are conceptually situated at the antipodal sides, but ultimately pursue the equilibrium point through a check and balance compromise. This could be seen as being jointly satisfied. IHL ruling armed conflicts is a compromise between military necessity and humanitarian considerations.[90] Its rules comply with both military necessity and the dictates of humanity. It should be noted that consideration of military necessity cannot be used as a justification for the act departing from the rules of humanitarian law in armed conflicts.[91] The admissible excuse is only when the positive rule of IHL expresses its exception for the reasons of military necessity. Schmitt points out that 'military necessity exists in equipoise with the principle of humanity, which seeks to limit the suffering and destruction of warfare. This symbiotic relationship determines in which direction, and at what speed, IHL evolves. It also determines the manner of

[88] Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* 8-12; Dieter Fleck (ed) *The Handbook of International Humanitarian Law* (3rd edn, OUP 2013) 34-38; Schmitt, 'Military Necessity and Humanity in Internaitonal Law: Preserving the Delicate Balance'.

[89] Nobuo Hayashi, 'Military Necessity as Normative Indifference' 44 Georgetown Journal of International Law 675 687.

[90] Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* 9-10. ('In following a middle road, LOIAC allows Belligerent Parties much leeway (in keeping with the demands of military necessity) and nevertheless curbs their freedom of action (in the name of humanitarianism).')

[91] Fleck, *The Handbook of International Humanitarian Law* 36-37; Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* 10-12.

its application on the battlefield.'[92] Then, when the balance between military necessity and humanity appears illogical or inappropriate in the light of some circumstances, the parties to the concerned conflict would invoke the rebalance of an existing rule. Any such rebalancing cannot be used for justification in order to deviate from what states have agreed upon in IHL or customary international law. In conclusion, the whole process of equilibrating between military necessity and humanity could be also understood for the furtherance of a joint satisfaction of the two values.

Put it in the cyber context, the pursuit of military necessity would prevail in cyber operations by actors because, as a new form of warfare, it provides unprecedented military benefits as seen in the previous sections above. When it comes to legal *lacuna* especially, states and non-state actors would be easily enticed into interpreting relevant laws in favour of their own military advantage or arguing their rights to behave on the basis of military necessity and the legal maxim of 'everything which is not forbidden is allowed'. On the other hand, humanitarian consideration would be a corresponding defensive base against that argument to achieve balanced rules for cyber armed conflict. Humanity, as the most fundamental and important base of IHL, must be undoubtedly reflected in the characterisation of cyber armed conflict.

To fill gaps in existing law, this thesis would be guided by these two fundamental normative values in examining the framework for classification of cyber armed conflicts. The existing rules of IHL which have been established upon the balance between military necessity and humanity, would be considered from the angle of new

[92] Schmitt, 'Military Necessity and Humanity in Internaitonal Law: Preserving the Delicate Balance' 796.

cyber phenomenon in order to find the possible or necessary adjustment by interpretation. In this case, one of these two principles seems to provoke at the first stage how to respond to new cyber operations. On the other hand, if a new law is required, normative tension between military necessity and humanity would be still contemplated in its examination. In that case, humanity seems to take a weighty role to limit cyber operations freely conducted on the basis of military necessity.

Chapter 3 – International Cyber Armed Conflict

I. Introduction

In characterising an armed clash situation in terms of international humanitarian law (IHL), the uppermost criterion is to identify actors who take part in that situation because the question as to whether or not both parties to an armed conflict are states is the first standard to classify the concerned situation, as long as the bifurcated structure of the law of armed conflict (LOAC) having international and non-international armed conflict (NIAC) sustains. This fundamental premise to identify international armed conflict (IAC) also remains in the cyber context.

From the advent of international law, LOAC has been founded on the war between states.[1] There is neither a specific reason to support the complete dismantlement of a bifurcated structure of IHL nor a special regime with regard to cyber conflicts. International cyber armed conflict is limited to the hostile confrontations between states only occurring in or through cyberspace. It is important to first examine how to characterise international cyber armed conflict from the angle of actors' criterion based on the analysis of actors criterion in international kinetic armed conflict.

According to the provisions of law, the situation where state and state-affiliated actors conduct hostilities, *levée en masse,* and national liberation movement are classified as

[1] Hugo Grotius, *De jure belli ac pacis libri tre* (1625); L. Oppenheim, *International Law II War and Neutrality* (2 edn, Longmans, Green and Co. 1912)

IACs. For a state to be a party to the IAC, state armed forces or state's organ should take part in the conflict. State armed forces and organised armed groups who are integrated into the regular armed forces of a state as a standing army consist of regular state armed forces. Other state-affiliated groups such as militias, volunteer corps, organised resistance movements could be regarded as irregular armed forces so long as they are incorporated *de facto* in the armed forces.[2] State-sponsored groups whose activities attribute to a state could also be identified as irregular armed forces. These groups are characterised based on their conducts attributable to a state, whereas regular state armed forces and state-affiliated armed forces are identified based on their status relating to a state. This chapter examines how to identify those actors in the cyber context to classify international cyber armed conflict.

After examining the criterion of actors, the question whether intensity criterion is required in classifying international cyber armed conflict is considered compared to international kinetic armed conflict.

II. State and State-Affiliated Actors

The subject of IAC is a state.[3] When we find the actors of regular state armed forces and irregular armed forces examined in the following sections as parties to the

[2] The phrase of 'belonging to a party to the conflict' at article 4A(2) of the Geneva Convention III (Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949 (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135) refers to this *de facto* incorporation.

[3] As a preliminary step, it is questionable whether states in an IAC should gain recognition from other states or be sufficient with substantive statehood. Considering the object and purpose of IHL, it would be proper to follow substantive roles or status of the concerned subject. In this regard, it is unnecessary to achieve recognition and if actual statehood has confirmed, the concerned conflict should be seen as IAC. (When it comes to the establishment of state and statehood, James R. Crawford, *The Creation of States in International Law* (OUP 2007) 37-40)

conflict, that conflict becomes classified as an IAC. Cyber units as a part of regular state armed forces, which are fully in charge of cyber warfare, is the main actor in international cyber armed conflict.[4] Irregular cyber armed forces, such as cyber militia and voluntary cyber corps, which is stipulated in treaty law, are also affiliated to a state. These actors' conducts are immediately regarded as those of state. The individual members of regular and irregular armed forces are entitled to the status of combatant and prisoner of war (POW) under the rules of IAC. The status of combatant means a person who has the right to attack against the adverse party and enjoys immunity from the application of municipal law in respect of the acts undertaken as part of hostilities.[5] Those combatants are also entitled to become POW when falling within the power of the adversary under the Geneva Convention III.[6]

1. Regular State Armed Forces

1.1. State Practice of Special Cyber Forces

Cyber units of states are not revealed outside to the same degree. Their transparencies seem to depend on their military strategies or national regimes. Cyber units of state armed forces occasionally disguise themselves as civilian hackers in practice. Military and intelligence operations and weapons platforms have increasingly connected together via computer network systems in order to offer swift, knowledgeable, and

[4] About the increasing possibility of cyber attacks by nation states, Ponemon Institute, 'The Rise of Nation State Attacks' 4 Journal of Law & Cyberwarfare 1.

[5] 'Combatant' itself is the legal concept based on the membership of belligerent party in an IAC. The combatancy requirements appear to be reaffirmed through the Hague and Geneva norms and built up as customary international law. While technology may not have changed the antagonistic dynamics between warriors on battlefield, it certainly has affected the attributes of combatants.

[6] Geneva Convention III, art 4

efficient command and control. Commanders' decision-making processes also lean considerably on data provided by such systems, so the security and stability of this domain is crucial in actual armed conflicts. Logistical support, real-time provision of intelligence, and remote operations rely on computer network systems.[7]

As cyber defence capability has been stressed, many states have not only established specialised units in charge of cyber warfare but also intensified their roles and competence. War game or cyber warfare scenarios are routinely simulated and national cyber strategies have been established. Over 120 countries are reportedly engaged in developing cyber capability in the military arena,[8] and so a complete survey of each is beyond the scope of this thesis. In this regard, special cyber units of selected states (the US, Russia, China, the UK, and South and North Korea) are examined about their status, structures, or strategies in order to understand the trend or direction of cyber military capability evolution.

The United States Cyber Command (USCYBERCOM), which centralises command of cyberspace operations, organises existing cyber resources and synchronises defence of US military networks,[9] (leaving the protection of civilian networks up to the Department of Homeland Security)[10] could be selected as the most representative or developed example. It cooperates with National Security Agency (NSA) networks and has been concurrently headed by the Director of the NSA. It is recently

[7] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014) 18-19.

[8] Jeffrey Carr, *Inside Cyber Warfare* (O'Reilly Media 2010) 161.

[9] U.S. Cyber Command <http://www.cybercom.mil/About/Mission-and-Vision/> accessed 20 September 2017.

[10] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Syngress 2011) 70.

announced that all 133 of USCYBERCOM's cyber mission force (CMF) teams achieved full operational capability. The CMF has built capability and capacity since 2013 when the force structure was developed and the services began to field and train the force of over 6,200 soldiers, sailors, airmen, marines and civilians.[11]

As one of the most active countries with strong capability and capacity in cyber operations, Russia has established cyber warfare theories and facilities since at least the mid-1990s.[12] Through the then-abolished Federal Agency or Government Communications and Information (FAPSI) in 2003 and Federal Counterintelligence Service (FSK) succeeded to the KGB (the USSR's Committee of State Security) the Federal Security Service of the Russian Federation (FSB) was centred in dealing with information warfare matters. Under the Russian federal law, the FSB offers a military service, including General Staff of the armed forces of Russian Federation.[13]

In China, the People's Liberation Army (PLA) is the main governmental organ in charge of cyber warfare. Even though it has not published any specific doctrines, the concept of information has always been stressed in China's military strategies. It is trusted that the General Staff Department (GSD)'s 3rd department and 4th department are put in charge of cyber intelligence and cyber-warfare respectively,[14] even though both departments will most likely become integrated under the Strategic Support

[11] US Cyber Command News Release, 'Cyber Mission Force Achieves Full Operational Capability' (17 May 2018) <https://www.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/> accessed 25 May 2018.

[12] Carr, *Inside Cyber Warfare* 161-171.

[13] Andress and Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* 71; The Russian Government, Federal Security Service <http://government.ru/en/department/113/ > accessed 15 December 2017; Federal Security Service of the Russian Federation (FSB) <https://en.wikipedia.org/wiki/Federal_Security_Service> accessed 3 April 2018.

[14] Ibid 71.

Force (SSF), which will 'likely formulate the core of China's information warfare effort by comprising forces in the space, cyber and electromagnetic domains, thus finally bringing China's military-related informatisation activities under one umbrella'.[15]

The UK Ministry of Defence (MOD) takes charge of military cyber defence that deals with the military use of cyberspace. MOD's cyber policy follows the guiding principles of the UK Cyber Security Strategy[16] and pursues the transformative cross-government approach with Office of Cyber Security and Information Assurance (OCSIA) and other government departments to ensure harmonious departmental approaches.[17] The UK has openly discussed the existence of two Joint Cyber Units. The Joint Cyber Reserve Force (CRF) is part of the Joint Forces Cyber Group which was created in May 2013 to deliver cyber defence capability. The CRF provides support to the Joint Cyber Unit (Corsham), the Joint Cyber Unit (Cheltenham), and

[15] Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation* (CCDCOE, 2016) 19-26; Other than the PLA's cyber units and SSF, so-called 'cyber militia' such as a hacktivist group of the Red Hacker Alliance, IT companies, scientists, network engineers, foreign language speakers, and others with useful skills takes part in military exercises as part of the National Emergency Drill Structure in China. (ibid 26-27) Even though they are not directly managed by PLA's authorities, the extent of the cyber militias' connections and accountability to the government and the PLA remains unclear and deserves further examination. (Robert Sheldon and Joe MacReynolds, 'Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias' in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (OUP 2015))

[16] HM Government, *UK National Cyber Security Strategy 2016 to 2021* (1 November 2016) <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021#history> accessed 5 October 2018; Cabinet Ofiice, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (25 November 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 5 October 2018; HM Government, *A Strong Britain in an Age of Uncertainty* (8 October 2010) <https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty> accessed 5 October 2018.

[17] With the goal to transform the UK's cyber capabilities into becoming more flexible, advanced, and suitable for the battlespace, the UK Defence Cyber Operations Group (DCOG) was established and will work closely with other government departments, industry and international partners. The DCOG is 'a federation of the cyber units across defence' and will include the Joint Cyber Unit hosted by GCHQ at Cheltenham as well as the GOSCC and presumably its attached Joint Cyber Unit at Corsham. (Anna-Maria Osula, *National Cyber Security Organisation: United Kingdom* (CCDCOE, 2015) 16-17)

tri-service information assurance (IA) units.[18] The Joint Cyber Unit (Corsham) aims to proactively and reactively defend MOD networks against standing cyber attacks. The Joint Cyber Unit (Cheltenham), hosted by Government Communications Head Quarters (GCHQ), aimed to reach full operational capability by 2015 and is put in charge of developing new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace.[19] Comprehensive management and cyber defence for all the UK Armed Forces' and MOD's communications networks, including theatre networks, is provided by the new Global Operations and Security Control Centre (GOSCC), located at MOD Corsham. The centre also has the capabilities to undertake forensic analysis of the attacks and 'give possible indications of future vulnerabilities, attack vectors, and as best as can be done — attribution of source'.[20] In addition, the centre makes use of the Joint Cyber Unit (Cheltenham) that is embedded within the GOSCC and 'develops and uses a range of new techniques, including proactive measures, to disrupt threats to ... information security'.[21]

Republic of Korea's Cyber Command (ROKCYBERCOM) was established under the Ministry of Defence in 2010 in order to counter North Korea's cyber threats. Since then, the status and power of ROKCYBERCOM has been intensified as the cyber

[18] Working for Joint Forces Command, <https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment> accessed 5 June 2018.

[19] UK Ministry of Defence, *Supplementary Written Evidence from the Ministry of Defence* (2012) <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm > accessed 5 June 2018.

[20] UK House of Commons Defence Committee, *Defence and Cyber-Security Written Evidence* (2012) <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/1881.pdf > 4 accessed 5 June 2018.

[21] Cabinet Ofiice, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (2011)

threats and attacks from Democratic People's Republic of Korea (DPRK) has increased significantly over the past decade. Even though DPRK has taken advantage of cyber capabilities with an asymmetry strategy, it is difficult to comprehend the structure and management of their cyber units or departments conducting military cyber operations due to the lack of transparency within the North Korean regime.[22] Nonetheless, the most outstanding point of cyber warfare capability seems to be the scale and expertise of cyber warriors likely trained and commanded by General Bureau of Reconnaissance (GBR) under the Ministry of the People's Armed Forces.[23] A unit of the Korean People's Army (KPA) dedicating to cyber warfare is rumoured to exist.[24]

These days, the vast majority of military operations and services include a cyber component. There are few areas where internal and external security are as closely intertwined as they are in cyberspace. Hence, the threat situation in cyberspace necessitates a holistic approach in the framework of national cyber security policy. Ensuring cyber security and defence in both military and civilian sectors requires a whole-of-government task to be collectively performed. In this regard, most states tend to establish comprehensive a national cyber security strategy along with their military cyber plans. States have also incorporated cyber operation parts into their

[22] About North Korea's cyber capabilities, Rhea Siers, 'North Korea: The Cyber Wild Card 2.0' 6 Journal of Law & Cyberwarfare 155.

[23] Jong-In Im and others, 'North Korea's Cyber War Capability and South Korea's National Counterstrategy' 29 The Quarterly Journal of Defense Policy Studies 9 23-25.

[24] 121 Unit under the command and control of GBR is strongly presumed as a specialised cyber unit. Recently, it is also claimed that General Staff of KPA planned to establish separate 'Cyber Strategy Command'. (Yeonhap News, 'Claimed "North Korea, Pursuing the Establishment of Cyber Strategy Command' *The Seoul Shinmun* (Seoul, 16 November 2017) <http://www.seoul.co.kr/news/newsView.php?id=20171116800018> accessed 15 May 2018)

own military manuals or rule of engagement and trained their combatants to take these into account in practice.[25]

Regarding the legal status of membership of state cyber forces, members of cyber units and members of state armed forces who carry out cyber operations are by definition entitled to the status of combatant only except of *hors de combat* and POW.[26] The concrete mission assigned to individual members in cyber operation are not factored into determining their combatant status because their belonging to state armed forces itself qualifies.

1.2. Other State Armed Forces

Regular state armed forces such as Navy, Army and Air Forces other than specially designed cyber units examined above can also carry out cyber operations during their tasks. Those cyber operations could be used not only to facilitate their intrinsic duty but also consists of indispensable part of the duty. At any rate, all these cyber operations are conducted by regular state armed forces.

When militia and volunteer corps form part of such armed forces, their members are entitled to the status of combatant and POW in case of falling into the power of the enemy.[27] By nature, this kind of cyber militia and volunteer cyber corps integrated

[25] Office of Genral Counsel, *Department of Defense Law of War Manual* (US Department of Defense 2015 (Updated December 2016)) 1011-1026; UK Ministry of Defence, *Cyber Primer* (2nd edn, Development, Concepts and Doctrine Centre July 2016)

[26] Geneva Convention III, art 4A(1); About *hors de combat*, Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law Volume I: Rules* (ICRC, CUP 2005) 164-170.

[27] Geneva Convention III, art 4A(1)

into state armed forces are a party to the conflict. As long as they are forming part of state armed forces and conducting within the state's command and control system, those cyber militia and volunteer cyber corps are regarded as state armed forces, a party to international cyber armed conflict.

2. Irregular Cyber Armed Forces

Alongside regular state armed forces are irregular armed forces. Except above-mentioned state armed forces which is formed on a regular basis by domestic legislation, all other groups or units which fight on behalf of a state constitute irregular armed forces. In order for an organisation or unit to be an irregular armed force, it should satisfy some conditions corresponding to regular armed forces. To recognise who irregular armed forces are, it is necessary to identify what critical aspects of regular state armed forces are.

From the angle of classification of armed conflicts, hostilities conducted by these irregular armed forces are attributed to a state party, with which it is affiliated. When state A is engaged in an IAC with state B and an organised armed group is engaged in a NIAC with state B, if a state A has a certain degree of relationship with the organised armed group, the group can be regarded as irregular armed forces of state A, party to an IAC *vis-à-vis* state B and the whole conflict situation becomes one IAC between state A and B. On the other hand, an organised armed group could fight against state B. In this NIAC, if state A in effect uses the armed group as its proxy based on a certain degree of support and control, the concerned NIAC can also be

internationalised.[28] What matters most for the transformation of NIAC to IAC in classification is the nature and degree of relationship between a state party to the conflict and an organised armed group. In conclusion, two steps are required to admit internationalisation of a conflict in terms of classification.

There are no provisions about internationalisation of internal armed conflict as well as attribution or characterisation itself. Article 4(2) of the Geneva Convention III, which is originally designed to give POW status to members of militia, volunteer corps, and organised resistance movements under certain conditions, only offers the clues for classification. Literally speaking, this is for classifying individuals (members) of a group in order to apply the rules of IHL. Among five conditions of article 4(2), 'belonging to a party to the conflict' is not explained in detail. This affiliation makes the concerned group a part of the state party to the conflict and leads to the entitlement of POW to the members of the group. Entitlement of POW and combatant status means that members of the group would enjoy immunity and privilege in the battlefield as a state party to the conflict. On the other hand, this affiliation would also imply attribution of their conducts during war to the state party to the conflict.

2.1. Cyber Militia, Volunteer Cyber Corps, and Other Organised Groups

In actual battlefield, to classify a given conflict situation, one would recognise actors who conduct hostilities and then identify their legal status whether they are members

[28] *Prosecutor v. Dusko Tadić* (Judgement) ICTY IT-94-1-A (15 July 1999) para 84; About this internationalisation, there exists an opposing argument that an IAC cannot be established without direct war engagement between at least two states. (Keiichiro Okimoto, 'The Relationship between a State and an Organised Armed Group and Its Impact on the Classification of Armed Conflict' 5 Amsterdam Law Forum 33 36-37)

of state armed forces, members of an organised group belonging to a party to the conflict, or otherwise mere agents involving in the hostilities. There is no definition of cyber militia, volunteer cyber corps, organised resistance movement, or other organised cyber groups that are assimilated to state armed forces in treaty law. Cyber militia can mobilise themselves like a chain reaction and then go even further in tasks like instructing, training, and commanding their cyber warriors in the virtual world. For example, in the Georgian cyber conflict during the Russo-Georgian War in 2008, through a few numbers of websites, took a role of command and control for hackers.[29] This hierarchical structure among hackers provides beginners with concrete instructions, tools, and tactics to evade security firewalls of targets and to disguise their attacks to avoid any countermeasures.[30] 'Volunteer cyber corps', an organised group of hackers voluntarily operating cyber attacks against the adversary, can be also assimilated to state cyber armed forces as long as the group meets the conditions of article 4A(2) of the Geneva Convention III and customary IHL. Both cyber militias and volunteer corps also can be subject to article 43 of the AP I with an additional condition.

First of all, the question arises as to whether 'other militia, volunteer corps, and organised resistance movements' in article 4A(2) of the Geneva Convention III include 'organised armed groups' as a non-state counterpart to a state party in NIAC. The terms 'militia, volunteer corps, and organised resistance movement' in article

[29] Andreas Hagen, 'The Russo-Georgian War 2008' in Jason Healey (ed), *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (A CCSA Publication 2013) 201-204.

[30] Brian Krebs, 'Report: Russian Hacker Forums Fueled Georgia Cyber Attacks' *The Washington Post* (16 October 2008) Security Fix <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html> accessed 20 February 2014.

4A(2) are 'generic terms to cover group of volunteer fighters not enlisted in the regular forces but fighting for a party to the conflict'.[31] Frequent types of participants are civilians forming organised armed groups which turn against the government of their own state outside the context of self-determination.[32] Considering the development of this provision and the nature of organised armed groups in an armed conflict, the phrase of 'militia, volunteer corps, and organised resistance movements' seems to encompass 'organised armed groups' in terms of NIAC. Therefore, it can be said that an organised armed group which is a party to a NIAC switch to a party to an IAC when the group belongs to a state party to that IAC and meets the requirements of article 4A(2).

Article 4A(2) stipulates that members of other militias and other volunteer corps, including those of organised resistance movements, belonging to a party to the conflict are assimilated to state armed forces as long as they satisfy the following conditions: (i) subordination to responsible command;[33] (ii) a fixed emblem or sign; (iii) carrying arms openly; and (iv) compliance with LOAC.[34] The two conditions,

[31] Okimoto, 'The Relationship between a State and an Organised Armed Group and Its Impact on the Classification of Armed Conflict' 39.

[32] In the context of self-determination, article 1(4) of the Additional Protocol I stipulates 'fighting against colonial domination and alien occupation and against racist regimes' as IACs.

[33] This condition is designed 'to exclude individuals acting on their own in wartime. The operation of small units of irregular armed forces is permissible, provided that the other conditions are fulfilled, but there is no room for hostilities in an IAC being conducted by individuals on their own initiative.' (Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn, CUP 2016) 52); 'The implication was that such an organisation must have the principal characteristics generally found in armed forces throughout the world, particularly in regard to discipline, hierarchy, responsibility and honour.'(Jean S. Pictet (ed) *The ICRC, Commentary III on the Geneva Convention of 12 August 1949* (ICRC) 58)

[34] Geneva Convention III, art 4A(2); Annex to 1907 Hague Convention IV Respecting to the Laws and Customs of War on Land, art 1

The laws, rights, and duties of war apply not only to armies, but also to militia and volunteer corps fulfilling the following conditions:

1. To be commanded by a person responsible for his subordinates;

taking distinguishable signs and carrying arms openly, intend to achieve the goal of distinguishing combatants from civilians.[35] Since cyber operations, by nature, are remotely conducted, the adversary party to a conflict at a distance can hardly tell the attackers on the basis of distinctive signs and openly carried arms conditions as in kinetic space. In addition, it is highly likely to hide military usage of computer networks used in cyber operations by employing or spoofing civilian computer networks including civilian Internet Protocol (IP) address. Hence, it is necessary to consider how to decently adapt the 'distinct sign' requirement to fit in different circumstance of cyberspace. It is also required to reconsider 'carrying arms openly' condition, which raises some interpretive questions even in the kinetic context.[36]

---

2. To have a fixed distinctive emblem recognisable at a distance;
3. To carry arms openly; and
4. To conduct their operations in accordance with the laws and customs of war.

[35] In terms of 'the principle of distinction', the ICJ in its 1996 *Advisory Opinion on Nuclear Weapon* case confirmed the principle of distinction as 'aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants'. (*Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 para 78) Civilian population and civilian objects must be protected against direct attacks without any actual military involvement. In case of doubt as to whether a person is a civilian, that person shall be considered to be a civilian. (Additional Protocol I, art 50(1)) The principle applies in both IAC and NIAC. However, the concept of combatant is only relevant to IAC. Hence, there is no equivalent of combatant immunity or prisoner of war in NIAC. In *Tadić* Judgement of the Appeal Chamber of the ICTY, combatancy is reaffirmed. (*Prosecutor v. Dusko Tadić* (Appeal Judgement) para 92-93); Jens David Ohlin, 'The Combatant's Privilege in Asymmetric and Covert Conflicts' 40 Yale Journal of International Law 337 379-382.

[36] Bothe, in his commentary, notes that the drafters of the APs disagreed over how to interpret the requirement. On one view, arms should be visible only to the naked eye, while on the opposing view arms should be visible at night (due to infrared equipment) or even at a far distance (due to binoculars). The latter view, taken to its logical extreme, would suggest that arms should be visible at all times since modern armies can deploy spy airplanes and satellites to detect the enemy twenty-four hours a day regardless of location. Given the technological advance of artificially enhanced visual detection, the visibility requirement would now appear to be universal if one accepts this as a correct definition of the open arms requirement. (Michael Bothe, Karl Joself Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (2nd edn, Martinus Nijhoff Publishers 2013) 287-289) On the other hand, the ICRC commentary by Jean Pictet draws a distinction between carrying arms 'openly' versus carrying them 'visibly' or 'ostensibly'. Arms can still be carried openly even if they are not visible at all times. Thus, concealing weapons while walking into an engagement, for the purposes of feigning civilian status, is clearly prohibited. Pictet correctly observes that carrying arms openly is not just a physical description but rather is tied to deeper prohibitions against perfidy and general requirements of attribution, though the implications of this point are not explored. (Pictet, *The ICRC, Commentary III on the Geneva Convention of 12 August 1949* 61)

In the course of *Tallinn Manual* 2.0 discussion, some experts argued that individuals engaged in cyber operations should always comply with the requirement of a fixed distinctive sign, 'regardless of circumstances such as distance from the area of operations or clear separation from the civilian population'.[37] They emphasised that there is no exception of customary international law relating to combatant status in order to enjoy immunity and prisoner of war status. On the other hand, other experts suggested that an exception to this requirement could exist in the cyber context. Considering the original purpose of wearing a distinctive sign, 'the requirement only applies in circumstances in which the failure to have a fixed distinctive sign might reasonably cause an attacker to be unable to distinguish between civilians and combatants, thus placing civilians at greater risk of mistaken targeting.'[38]

Heather Dinniss suggests that a potential update to their provisions in the context of cyber would be to mandate that cyber operations be launched from a computer with a military IP address in order for the cyber warrior to receive combatant status.[39] However, at the same time, she casts a doubt on the practicality of such a requirement, explaining that a military IP address would place an immediate target on the computer involved in an attack.[40] About military IP address identification, Vijay Padmanabhan comments that military IP address use of cyber warriors in attacks incentivises transparency in cyber operations. Transparency decreases the risk of mis-targeting the

[37] Michael N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 405.

[38] Ibid 406.

[39] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 146.

[40] Ibid.

attacked state against a third state or civilian infrastructures to retaliate the precedent cyber attack due to false or disguised IP address.[41]

It should be discussed more whether new standards are required to be qualified as irregular cyber armed forces in the future. It is insufficient to conclude whether specially modified requirements of distinction are necessary for cyber warriors or if the concurrent conditions could apply in cyber operations as they are. If states distinguish military IP from civilian IP in the practice of cyber attacks, it could be a rule for 'a distinctive sign' of cyber combatant. The distinction between military and civilian computer network systems is not only clear-cut but also disguise or detour by dual use of networks seems more luring in cyberspace. At the same time, the clearer solutions could be suggested if more information technology is developed. Nonetheless, it could be required to alleviate the conditions to some extent in the future.[42]

Article 43 (1) of the Additional Protocol (AP) I for the first time offers the definition of 'armed forces': 'the armed forces of a party to a conflict consist of all organised armed forces, groups and units which are under a command responsible to that party for the conduct of its subordinates, … .' It also confirms that 'armed forces' includes organised armed groups as well as regular state armed forces. Then the question arises as to how interpret the phrase of 'under a command responsible to the party' in

[41] Vijay M. Padmanabhan, 'Cyber Worriors and the *Jus in Bello*' 89 International Law Studies 288 295-296.

[42] Dinstein suggests that the two conditions of distinction – 'a fixed distinctive emblem' and 'carrying arms openly'– could become alternative rather than cumulative, considering that when one is fulfilled the other may be deemed redundant. (Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* 64)

relation to 'belonging to a party to the conflict' of article 4A(2). Rather article 43(1) can be interpreted to offer the detailed nature of belonging in article 4A(2) about the relationship between an organised armed group and a state to the conflict. Therefore, a link required for an organised armed group to belong to a state party to an IAC means that the state has a responsible command over the organised group. When it comes to the details of that command relationship, it will be dealt with in the next section of attribution.

In addition, a paramilitary or armed law enforcement agency – even ununiformed – can be also incorporated into a state's armed forces as long as the adverse party has been notified of this.[43] Like this, AP I adds a further requirement that incorporation be notified to the adverse party, whereas under the customary IHL incorporation is solely a factual matter and failure to so notify the enemy does not preclude their treatment as a member of the armed forces.[44] Put it in the cyber context, 'police forces' equipped with military arms could be deployed for cyber military operations under the system of state armed forces.[45] In this case, the question arises as to how interpret the requirement of 'being notified to the adversary party' in cyberspace to apply AP I. This issue of notification to or recognition of the adversary is common to members of

[43] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I), art 43(3); Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC / Martinus Nijhoff 1987) para 1683.

[44] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law Volume I: Rules* 17.

[45] For the expression of 'police forces', it has to particularly take into account the differences in internal organisation in many states. 'Where a state had a law providing for the automatic incorporation of such forces into its armed forces in time of war, the notice requirement might be satisfied by notification to all parties to the protocol, through the depositary.' (Sandoz, Swinarski and Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* para 1682)

cyber militia or volunteer corps belonging to a party to the conflict to be assimilated to state armed forces.

In practice, as already mentioned in the special cyber armed forces part, states have developed their national cyber security policies by establishing military–civilian organic cooperation and taking an approach of comprehensive and harmonious collaboration between governments' departments as well as private–public sectors. This tendency also interferes in cyber militia. For example, Chinese government proclaimed the instructions to implement civil–military integration systems, cybersecurity projects, and innovation policies,[46] and in effect established the Central Commission for Integrated Military and Civilian Development. Under the instruction of the commission, China's first 'cybersecurity innovation centre', which is operated by 360 Enterprise Security Group (one of China's primary cybersecurity companies) for the purpose of fostering private sector cooperation to 'help the military win future cyber wars', was established in December 2017.[47] In other words, China's cyber militias are organised regardless of the occurrence of armed conflicts and are ready to be or already incorporated into state armed forces. It shows that cyber militia could appear with closer links to regular armed forces and broadly be organised unlike the traditional concept of militia. However, it is not obvious that the forgoing Chinese cyber militia qualifies as irregular armed forces in terms of positive law. There exist the cumulative conditions for being irregular armed forces as seen above. So, for the present, it needs more information such as internal structure or action plan of that

[46] Sheldon and MacReynolds, 'Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias' 188-190.

[47] Nicholas Lyall, 'China's Cyber Militias: China's cyber power is in the grip of dual trends: pluralism and centralization' *The Diplomat* (1 March 2018) <https://thediplomat.com/2018/03/chinas-cyber-militias/> accessed 15 July 2018.

organisation in order to conclude the legal nature of the Chinese cyber militia. Otherwise, that cyber militia might be deemed to form state armed forces as regular. Its legal nature cannot be precisely identified due to the lack of information.

2.2. Attribution to a State

In order for irregulars such as members of militia, volunteer corps, or other organised groups to qualify as lawful combatants, international rules and state practice require one more condition of 'belonging to a party to the conflict' (IAC).[48] It is also meant to be a responsible command relationship between an organised armed group and a state party to the conflict under article 43(1) of the AP I. About what 'belonging to a party to the conflict' refers to, a commentary suggests that a relationship of dependence and allegiance of these irregulars *vis-à-vis* that party to the conflict should be established.[49] It is essential that there should be a *de facto* relationship between the resistance organisation and the party to international law which is in a state of war. These then may be regarded as the ingredients of the phrase of 'belonging to a party to the conflict'.[50] 'Resistance movements must be fighting on behalf of a 'party to the conflict' in the sense of article 2, otherwise the provisions of article 3 relating to non-international conflicts are applicable, since such militia and volunteer corps are not entitled to style themselves a 'party to the conflict'.'[51]

[48] Geneva Convention III, art 4(2)

[49] Pictet, *The ICRC, Commentary III on the Geneva Convention of 12 August 1949* 57.

[50] *Prosecutor v. Dusko Tadić* (Appeal Judgement) para 94; Geneva Convention III, art 4A(2); Geneva Convention I, art 13(2); Geneva Convention II, art 13(2)

[51] Pictet, *The ICRC, Commentary III on the Geneva Convention of 12 August 1949* 57.

'IHL does not contain any criteria unique to this body of law for establishing when a group of individuals may be regarded as being under the control of a state, that is as acting as *de facto* state officials.'[52] There are no provisions or rules about 'attributability' of cyber attacks conducted by a group of hackers to a state. Instead, there are the theories of attribution delivered by international courts and tribunals, and Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), which is set out in the International Law Commission (ILC).[53] Article 4 of the ILC's ARSIWA stipulates the attributable state responsibility of state organ and article 8 stipulates that the conduct of non-state actors is attributed to a state when it is conducted 'on the instructions of, or under the direction or control of' that state. These two provisions are about 'the extent or threshold of control that a state should exercise over a private actor for the latter's conduct to be attributable' in terms of state responsibility law.[54] Even those set of rules and theories are not inclusive of cyber attacks in their determination since cyber attacks have increasingly occurred after the decisions of international jurisprudences. Therefore, it would be examined hereafter whether these rules and theories are analogically applicable to the attributability of conducts of a group of hackers to a state in cyberspace for the purpose of classification.

[52] *Prosecutor v. Dusko Tadić* (Appeal Judgement) para 98.

[53] International Law Commission, *Articles on the Responsibility of States for Internationally Wrongful Acts* (A/56/83 3 August 2001)

[54] Vladyslav Lanovoy, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' 28 EJIL 563 574.

Compared to other conventional means and methods of armed conflicts, attribution presents more difficulties in the cyber context.[55] As attribution continues to be a problem inherent in cyberspace, there is an especially large risk of uncontrolled escalation in the event of a cyber incident. There would be two divided stages of attribution in cyber attacks: the first is identifying the actor conducting cyber operations in person which also helps classify the concerned conflict situation in terms of IHL; the second leads to find who is responsible for those cyber operations by means of proving the existence of a state connecting to the actual actors.[56] In this section, the very first stage of attribution, that is, who conducted a cyber attack in person, is assumed to be certified as a group of hackers.[57] In other words, a technological and factual finding aspect of attribution to identify the actor is not considered in this section. Instead, the issue is whether or not a state is behind of the concerned group as the next stage of attribution.[58] In regard to classifying cyber armed conflicts, it is important to narrow the scope of discourse as to whether or not a state can be attributed to a concerned cyber attack.

---

[55] Neil C. Rowe, 'The Attribution of Cyber Warfare' in James A. Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 61-62; The term 'attribution' generally refers to ascribing a work or remark to a particular person or thing. 'Attribution' is in the thesis used to refer to identifying the actor directly conducting the concerned cyber operation and other actors behind that cyber operation. This part focuses on the attribution about whether or not a state is behind the actor conducting cyber operations.

[56] For comparison, Herbert Lin points out that 'which type of attribution is relevant depends on the goals of the relevant decision-maker' and distinguishes between 'attribution of malicious cyber activity to a machine, to a specific human being pressing the keys that initiate that activity, and to a party that is deemed ultimately responsible for that activity'. (Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' Aegis Paper Series <https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0> accessed 21 March 2017) According to Lin's opinion, this section only deals with the third type of attribution, attributing malicious cyber activity to the ultimate responsible party, on the premise that other two attributions of malicious cyber activity to a machine and a human intruder are confirmed.

[57] Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' 14 Melbourn Journal of International Law 496 502-504.

[58] For a similar approach to attribution, Rowe, 'The Attribution of Cyber Warfare' 67.

2.2.1. Effective control test

In order to judge whether a concerned organised group belongs to a state to the conflict from the angle of classification of armed conflicts, there are three possible approaches about attribution of the group's conducts to the state: one is effective control test developed by the International Court of Justice (ICJ); another is overall control test invented by the International Criminal Tribunal for the Former Yugoslavia (ICTY) appeal chamber in *Tadić* case; and the third is argued by some commentator even a low-threshold requirement for attribution.[59] These analyses easily confuse with the relation to state responsibility law.

In the *Nicaragua* case, the ICJ took the position that 'for this conduct to give rise to legal responsibility of the United States (US), it would in principle have to be proved that that state had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.'[60] That is, even though the Court admitted that the US participated 'in the financing, organising, training, supplying, and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operations' on the basis of the evidence in the possession of the Court in a preponderant or decisive way, it is still insufficient in itself 'for the purpose of attributing to the US that acts committed by the contras in

[59] Katherine Del Mar, 'The Requirement of 'Belonging' under International Humanitarian Law' 21 EJIL 105; 'The 'belonging' requirement is a much easier test to fulfil than the 'overall control' test developed by the ICTY in the *Tadić* case. Whereas 'overall control' amount to control exercised by a state over individuals insofar as the state 'organise, coordinates or plans the military actions' of the individuals, the 'belonging' requirement demands nothing more than a form of acceptance, either express or tacit, on the part of the state and the individuals concerned that the latter are fighting on behalf of the state.' (ibid 111-112)

[60] *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14 para 115.

the course of their military or paramilitary operations in Nicaragua'.[61] The Court pointed out that the forms of US participation mentioned above is the general control over a force with a high degree of dependency on it, which does not in themselves refer to the attribution to the US.[62] As a result, the concerned conflict between Contras and Nicaragua remained as NIAC. If the Contras had been recognised as *de facto* organ of the US through the attribution test, the conflict would have been IAC between the US and Nicaragua. This refers to a type of 'internationalisation' of internal conflict between an organised armed group and a state in its territory by the intervention of a foreign state.

The ICJ in its *Genocide* case in 2007 reaffirmed the position that 'it must be shown that this effective control was exercised, or that the states' instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.'[63] The Court is of the view that the particular characteristics of genocide do not justify the Court in departing from the criterion elaborated in the judgement of *Nicaragua* case. The Court rejected to subscribe to the 'overall control' test of the ICTY Appeal Chamber in that 'the ICTY was not called upon in the *Tadić* case, nor is it in general called upon, to rule on questions of state responsibility, since its jurisdiction is criminal and extends over persons only.'[64] However, it did not take any position on its applicability as an independent test for characterisation of

[61] Ibid.

[62] Ibid.

[63] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Judgement) [2007] ICJ Rep 43 para 400.

[64] Ibid para 403.

internationalised NIAC, but limitedly supported that 'insofar as the 'overall control' test is employed to determine whether or not an armed conflict is international, which was the sole question which the Appeal Chamber was called upon to decide, it may well be that the test is applicable and suitable.'[65]

2.2.2. Overall control test

In the *Tadić* case in which the ICTY was not concerned with state responsibility, the Appeal Chamber held two tests of internationalisation of internal conflict; when (i) another state intervenes in that conflict through its troops, or alternatively when (ii) some of the participants in the internal armed conflict act on behalf of that other state.[66] In examining the latter, the Appeal Chamber developed the 'overall control' test.

While the *Tadić* case in its Trial Chamber discussed and invoked the findings concerning the effective control test from the *Nicaragua* case, there are some other cases which have opposed this logic. In the *Delalić* case, the Trial Chamber criticised that the purpose and context to find criminality of individuals in an armed conflict in ICTY needs to be separated from those of the ICJ.[67] After more criticism from

[65] Ibid para 404.

[66] *Prosecutor v. Dusko Tadić* (Appeal Judgement) para 84.

[67] 'A lengthy discussion of the *Nicaragua* Case is also not merited in the present context. While this decision of the ICJ constitutes an important source of jurisprudence on various issues of international law, it is always important to note the dangers of relying upon the reasoning and findings of a very different judicial body concerned with rather different circumstances from the case in hand. The International Tribunal is a criminal judicial body, established to prosecute and punish individuals for violations of international humanitarian law, and not to determine state responsibility for acts of aggression or unlawful intervention. It is, therefore, inappropriate to transpose wholesale into the present context the test enunciated by the ICJ to determine the responsibility of the United States for the actions of the contras in Nicaragua.' (*Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić, and Esad Landžo* (Judgement) ICTY IT-96-21-T (16 November 1998) para 230)

commentators on the Trial Chamber's conclusion in the *Tadić* case, the Appeal Chamber established a different opinion from that of the Trial. The Appeal Chamber held that the Trial Chamber erred in referring to the ICJ's effective control test reasoning that the test was contrary to the very logic of state responsibility and it was inconsistent with judicial and state practice.[68] The Appeal Chamber pointed out that the degree of control might vary according to the circumstances and that the analysis should be guided by a flexible approach. They further adduced that 'for the attribution to a state of acts of these groups it is sufficient to require that the group as a whole be under the overall control of the state.'[69]

At the same time, the Appeal Chamber indicated that in the case of groups which are not militarily organised, the threshold should be higher as overall control was deemed to be insufficient and more specific instruction coming from the host state to the group in question were required.[70] The overall control may be deemed to exist 'when a state has a role in organising, coordinating, or planning the military actions of the military group, in addition to financing, training, and equipping or providing operational support the that group'.[71] 'Acts performed by the group or members thereof may be regarded as acts of *de facto* state organs regardless of any specific

[68] *Prosecutor v. Dusko Tadić* (Appeal Judgement) para 115-145.

[69] 'One should distinguish the situation of individuals acting on behalf of a state without specific instructions, from that of individuals making up an organised and hierarchically structured group, such as a military unit or, in case of war or civil strife, armed bands of irregulars or rebels. Plainly, an organised group differs from an individual in that the former normally has a structure, a chain of command and a set of rules as well as the outward symbols of authority. Normally a member of the group does not act on his own but confirms to the standards prevailing in the group and is subject to the authority of the head of the group. Consequently, for the attribution to a state of acts of these groups it is sufficient to require that the group as a whole be under the overall control of the state.' (ibid (Appeal Judgement) para 120); Mark R. Shulman, 'Discrimination in the Laws of Information Warfare' 37 Columbia Journal of Transnational Law 939 120.

[70] *Prosecutor v. Dusko Tadić* (Appeal Judgement) para 137.

[71] Ibid.

instruction by the controlling state concerning the commission of each of those acts.'[72]

Afterwards, the Trial Chamber in the *Rajic* case pointed out that the Appeal Chamber in the *Tadić* case had not established the degree of foreign state involvement needed to transform an internal conflict to an IAC. The Trial Chamber held that 'the significant and continuous military intervention of the Croatian Army in support of the Bosnian Croats in fact sufficed to transform the conflict into an international one.'[73] The Trial Chamber concluded that specific operational control was not necessary and general political and military control was sufficient.[74] As a result, the overall test established by the Appeal Chamber in *Tadić* case has been sustained in subsequent cases.

2.2.3. The relationship between classification and state responsibility

The ILC report of *Fragmentation of International Law* pointed out that 'the contrast between *Nicaragua* and *Tadić* is an example of a normative conflict between an earlier and a later interpretation of general international law.'[75] However, the author casts partial doubt on this analysis. 'Attribution' analysed in the judgements of both

[72] Ibid.

[73] *Prosecutor v. Rajic, Review of the Indictment Pursuant to Rule 61* ICTY IT-95-12-R61(13 September 1996) para 21.

[74] Ibid para 25-26.

[75] ILC, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law* (A/CN.4/L.682 13 April 2006) para 50. (… '*Tadić* does not suggest 'overall control' to exist alongside 'effective control' either as an exception to the general law or as a special (local) regime governing the Yogoslav conflict. It seeks to *replace* that standard altogether.')

international jurisprudences should be clearly identified first. There are attributions to impose state responsibility and the attributions for classification of a given conflict situation to impose criminal responsibility on individual participants in the concerned armed conflict. Classification of the given armed conflict is about to determine the applicable law to the situation as such if it is proved as an NIAC, under the ICC article 8(e)(f), the prosecuted individual's criminal responsibility (liability) would be judged. Of course, if the relationship between a concerned non-state armed group and a state is proven to be attributable, the given situation would be characterised as an IAC and then the IHL rules of IAC would apply to both. That said, the attribution test for state responsibility law is different in that it aims to ask for international legal responsibility for a state about internationally wrongful acts of its organs, agents, *de facto* organs, or other individuals pursuant to the attribution rules of ARSIWA. The ICJ effective control test is for state responsibility and the ICTY overall control test is for classification of armed conflict to impose individual criminality, therefore, for the purpose of this thesis, the attribution test should be analysed from the angle of classification.[76]

The attribution test could be different according to judicial bodies or the legal purposes required. It is argued that the issue of internationalisation of an ongoing NIAC should be examined via the lens of the rules of attribution under the law of state responsibility like ICJ, whereas some scholars have also suggested other tests,

[76] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* para 404-405; Antonio Cassese, 'The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgement on Genocide in Bosnia' 18 EJIL 649; Remy Jorritsma, 'Where General International Law meets International Humanitarian Law: Attribution of Conduct and the Classification of Armed Conflicts' 23 Journal of Conflict & Security 405.

especially 'overall control test'.[77] Considering the distinction between classification rules and state responsibility law, an organised armed group, which already meet the requirements of POW under article 4A(2) of the Geneva Conventions III or armed forces of the AP I, needs overall control from a state to belong to it.[78] Under the overall control, all the hostilities conducted by the organised armed group are attributed to the state and the concerned internal conflict becomes an IAC. Then, 'such responsibility can be assessed after determining the applicable law in the light of which the behaviour of state and individuals must be assessed.'[79] In other words, this organised armed group can be doubtlessly said to belong to a state if its conduct is attributable to that state under the international law of state responsibility.'[80]

2.2.4. Conclusive thoughts

Depending on the relationship between the intervening state and an organised group of hackers, there would be either one international cyber armed conflict or two parallel international cyber armed conflicts and non-international cyber armed conflict. It seems more difficult in cyberspace to prove how a state controls the organisation of hackers to conduct cyber attacks than in kinetic space due to the intrinsic

[77] Noam Zamir, *Classification of Conflicts in International Humanitarian Law: The Legal Impact of Foreign Intervention in Civil Wars* (Edward Elgar 2017) 126.

[78] 'The situation of an organised group is different from that of a single private individual performing a specific act on behalf of a state. In the case of an organised group, the group normally engages in a series of activities. If it is under the overall control of a state, it must perforce engage the responsibility of that state for its activities, *whether or not each of them was specifically imposed, requested or directed by the state*.' (*Prosecutor v. Dusko Tadić* (Appeal judgement) para 122)

[79] Jorritsma, 'Where General International Law meets International Humanitarian Law: Attribution of Conduct and the Classification of Armed Conflicts' 418.

[80] Russell Buchan, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' 15 Chinese Journal of International Law 741 755; Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) 35; *Prosecutor v. Ljube Boškoski, Johan Tarčulovski* (Judgement) ICTY IT-04-82-T (10 July 2008) para 199-203.

characteristics of the Internet such as invisibility and high speed. Although increasingly popular, the overall control is yet to be deemed to reflect customary law as an independent interpretation about attribution and internationalisation of an internal conflict.[81] This is not only because state practice reaching cyber armed conflict is limited even in the kinetic context but also because the control tests of attribution are still contested. However, the effective control test would play a role to limit the internationalisation of the concerned internal cyber conflict or to downplay the involvement of a state backing hacker groups in cyber operations.

There would be the case that another group of individuals, who does not reach the level of an organised armed group in IHL, can conduct hostilities under the effective control of a state as a *de facto* organ or a substitute of the state. This group of individuals cannot qualify as a party to the concerned armed conflict because they at least must be an organised armed group to influence classification of armed conflicts as NIAC or IAC in IHL. Instead, they only could be individually considered in assessing state responsibility. Put in another way, the question as to whether they conducted on the instruction or under direction of a state, even out of its legitimate order and scope, matters. It focuses on the issue of whether the concerned conduct of the group individuals attributes to a state. If a state-sponsored group of hackers is separately identified based on their concrete cyber operations, the effective control test for attribution would be applied to recognise state responsibility. The relationship between a group of hackers and the controlling state should be strictly proven. When

[81] Zamir, *Classification of Conflicts in International Humanitarian Law: The Legal Impact of Foreign Intervention in Civil Wars* 127; It should be additionally noted that members of the organised group acting on behalf of a state are not automatically entitled to all of the protections of the LOAC. (ibid 126)

a state takes overall control over a hacker group (not an organised armed group) such as 'coordinating and helping in the general planning of'[82] cyber attacks with them, it is not only relevant to classification itself but also insufficient to attribute the groups' cyber attacks to that state and to impose international responsibility on the state.

2.3. *Levée en Masse* and National Liberation Movement

An IAC exists when peoples are fighting against colonial domination, alien occupation, or racist regimes in the exercise of their right of self-determination.[83] This article 1(4) of the AP I is specially designed as IAC. *Levée en masse* in short means 'the spontaneous springing to arms of the population in defence of the country'.[84] The rules of *levée en masse* is already recognised in the Lieber Code and the Brussels declaration, and then codified in the Hague Regulations and the Geneva Convention III.[85] By the same token, the national liberation movement with violence against colonial regime refers to IAC and national liberation groups against colonial domination exercising the right of self-determination are regarded as irregular armed forces.[86] These specific situations can also occur in or through cyberspace.

---

[82] *Prosecutor v. Dusko Tadić* (Appeal Judgement) para 131.

[83] Additional Protocol I, art 1(4)

[84] *Levée en masse* originates from the French Revolution, 'tout citoyen est soldat quand il s'agit de combattre la tyrannie.'

[85] Instructions for the Government of Armies of the United States in the Field (24 April 1863) (Lieber Code), art 49, 51; Project of an International Declaration concerning the Laws and Customs of War (Brussels 27 August 1874) (Brussels Declaration), art 10; Convention (IV) Respecting the Law and Customs of War on Land and its Annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2277 (Hague Regulations), art 2; Geneva Convention III, art 4(A)(6)

[86] About the right of self-determination, UN Charter art 1(2); UN General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* (A/RES/25/2625 24 October 1970); Heather A. Wilson, *International Law and the Use of Force by National Liberation Movement* (OUP 1988); Christian Tomuschat, 'Self-Determination in a Post-Colonial World' in Christian Tomuschat (ed),

Levée en masse participants refer to the inhabitants of a non-occupied territory who, on the approach of the enemy, spontaneously take up arms to resist the invading forces without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.[87] They are neither organised to be admitted as an organised armed group nor belonging to armed forces. They are neither required to be commanded by a person superior to themselves nor wear a fixed uniform or sign to separate themselves from ordinary civilians. In addition, they cannot qualify as civilians in a normal view. Participants in *levée en masse* are unorganised, spontaneous, and carry arms openly at the approach of the invading enemy. The only exception in IAC to the rule of distinction between combatants (members of armed forces) and civilians is the *levée en masse*. *Levée en masse* participants are treated under LOAC as similar status with combatants enjoying some privileges. Compared to the armed forces (combatants) requirements, for the persons who take part in *levée en masse*, two more conditions should be satisfied to enjoy similar privileges with lawful combatants. They 'shall be regarded as belligerents if they carry arms openly and if they respect the law and customs of war.'[88] It has long been admitted that members of *levée en masse* are entitled to immunity from their direct involvement in hostilities and POW status on capture. Instead, this exceptional concept of *levée en masse* only lasts for a short period of

---

Modern Law of Self-Determination (Martinus Nijhoff Publishers 1993); Jochen A. Frowein, 'Self-Determination as a Limit to Obligations under International Law' in Christian Tomuschat (ed), *Modern Law of Self-Determination* (Martinus Nijhoff Publishers 1993)

[87] Hague Regulations, art 2; Geneva Convention III, art 4(6); Additional Protocol I, art 50(1)

[88] Hague Regulations, art 2; Geneva Convention III, art 4(A)(6)

time.[89] Beyond the initial invading moment or later occupation completed by the adversary state, there is no room for application of the rules of *levée en masse*.

The ICRC commentary to the Geneva Convention III states that 'the provision is also the notion of a *levée en masse* is applicable to populations which act in response to an order by their government, given over the wireless.'[90] Extension to orders given by cyber means this is appropriate as well as meaningful in unfolding the discourse of cyber *levée en masse*. The *Tallinn Manual* 2.0 Rule 88 states 'in an international armed conflict, inhabitants of unoccupied territory who engage in cyber operations as part of *levée en masse* enjoy combatant immunity and prisoner of war status.'[91] At the same time, the Manual affirms in its Rule 96 that '(d) in an international armed conflict, participants in a *levée en masse* may be made the object of cyber attacks.'[92][93]

There would be the situation in which members of population in a spontaneous and unorganised way become involved in offensive cyber operations in order to respond the invasion of their own country. This situation does not necessarily mean the communication or commander among participants by using the wireless mentioned in the commentary. Inhabitants in unoccupied territory facing invasion can resist the

[89] Pictet, *The ICRC, Commentary III on the Geneva Convention of 12 August 1949* 68.

[90] Ibid 67.

[91] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 408.

[92] Ibid 425.

[93] David Wallace and Shane Reeves argue that 'a cyber *levée en masse* combatant category increases "confusion and uncertainty as to the distinction between legitimate military targets and persons protected against direct attack" and therefore acts in direct opposition to this well-established principle. Whether due to the irresolvable distinction problem, or because of a complete dissimilarity between a traditional *levée en masse* and the cyber variant, it is untenable to maintain this combatant category in cyber warfare.' They instead suggest an alternative concept of 'irregular cyber troop', which 'require to comply with a modified version of criteria for other irregular troops, such as militias, volunteer corps or organized militia movements'. (David Wallace and Shane R. Reeves, 'The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare ' 89 International Law Studies 646 661-662)

approach of the adversary army in cyberspace as well. The question then arises as to whether a stand-alone cyber *levée en masse* could be also accepted as an IAC. Would *levée en masse* only in or through cyberspace be possible without kinetic invasion of other states and corresponding resistance? Cyber *levée en masse* should only be allowed when repelling kinetic invasion of territory by adversary armed forces in a traditional sense. It is not permitted in the face of invasion that is only composed with cyber operations. Considering that the concept of *levée en masse* historically started from exceptional situation and allowed temporarily until occupation by invading forces or complete repelling, there is no reason to especially extend the application of *levée en masse* in cyberspace. Thus, cyber *levée en masse* should be still permitted in the limited situation of a conventional kinetic invasion. In this regard, the situation where cyber *levée en masse* appears is always classified as an IAC and its characterisation is different from stand-alone international cyber armed conflicts.

2.4. Cyber Outsourcing as Irregular Armed Forces?

Outsourcing of cyber operations is easier than that of kinetic ones because of the unique characters of cyberspace. Internet security companies such as PMSCs can be hired by states for cyber operations. What matters here is to distinguish cyber attacks having military purpose carried by outsourcers from other cyber operations outsourced for ordinary maintenance and repair of computer network system or security of network system. The question then arises as to whether a group of cyber outsourcers conducting cyber hostilities could be also regarded as irregular armed forces similar to those examined above.

Assuming a group of employees from private cyber security company who continuously takes a task of military cyber operations (not mere war supporting and sustaining efforts), would it be qualified as irregular cyber armed forces as long as satisfying the conditions of article 4A(2) of Geneva Convention III or the attribution test for being a state-sponsored group? Would it be regarded as cyber mercenary on the ground that they get paid by a hiring state party to the conflict? If such a group neither qualifies as irregular armed forces nor a state-sponsored group, whose activities attribute to a party state to the conflict in the end, that group would be separately considered in terms of classification of the concerned conflict. There could be simultaneously and separately NIAC between one state and that organised cyber group along with IAC between two state parties. Organised armed groups belonging to neither of the state parties to the conflict could also position at the same side with one state of the concurrent IAC. Cyber operations carried out by the employees of PMSCs based on the contract with and subordination to a hiring state must be attributed to that state. Employees assigned from private company could be regarded as cyber mercenaries under certain circumstances as long as there are not newly established norms and rules in international law.[94] However, the existence of those individuals or PMSCs as cyber mercenaries does not have any effect on classification

[94] 'Mercenaries' are defined as any person who a) is specially recruited locally or abroad in order to fight in an armed conflict; b) does, in fact, take a direct part in the hostilities; c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that party; d) is neither a national of a party to the conflict nor a resident of territory controlled by a party to the conflict; e) is not a member of the armed forces of a party to the conflict; and f) has not been sent by a stat which is not a party to the conflict on official duty as a member of its armed forces. (Additional Protocol I, art 47(2)); Article 47(1) of the AP I reflecting a customary international law denies 'the right to be a combatant or a prisoner of war' for a mercenary. Rule 90 of the *Tallinn Manual* 2.0 stipulates that 'mercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status.' (Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 412) A 'hacker for hire' who meets the above-mentioned six criteria, even if operating alone and far from the battlefield would be a mercenary for the hiring state. (ibid 413)

itself. Their military cyber operations would be subject to the rules of direct participating in hostilities (DPH).

III. Whether Intensity Matters in International Cyber Armed Conflict

For an IAC to exist, there must be a resort to armed forces involving at least two states.[95] The threshold for an international armed conflict is very low and does not require a certain intensity or duration.[96] The existence of an IAC is to be determined by the facts, not the subjective intent of the belligerents.[97] Pursuant to the common article 2 of the Geneva Conventions, the Conventions apply to 'all cases of declared war, or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognised by one of them'.[98]

---

[95] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* (Jurisdiction) ICTY (2 October 1995) para 70; *Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić, and Esad Landžo* para 184. ('The existence of armed force between states is sufficient of itself to trigger the application of international humanitarian law'); Be that as it may, there are practical attempts to apply the intensity criterion restrictively and not to regard small-scale military confrontations between states as a triggering event for an IAC. (Masahiko Asada, 'The Concept of "Armed Conflict" in International Armed Conflict' in Mary Ellen O'Connell (ed), *What Is War?: An Investigation in the Wake of 9/11* (Martinus Nijhoff 2012) 60-62) According to this approach, a considerable number of isolated or sporadic inter-state exchanges of fire being expressed as 'border incidents', 'clashes', or other types of armed provocation do not denote IAC due to the insufficient intensity of hostilities thereof. (ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (31st International Conference of the Red Cross and Red Crescent, 2011) 7)

[96] The ICRC takes a more policy-oriented position that 'the absence of a requirement of threshold of intensity for the triggering of an IAC should be maintained because it helps avoid potential legal and political controversies about whether the threshold has been reached based on the specific facts of given situation. There are also compelling protection reasons not to link the existence of an IAC to a specific threshold of violence.' (ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* 7)

[97] 'Any difference arising between two states and leading to the intervention of members of the armed forces is an armed conflict within the meaning of article 2, even if one of the parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.' (Pictet, *The ICRC, Commentary III on the Geneva Convention of 12 August 1949* 23)

[98] Geneva Conventions I - IV, art 2

Literally, the provision does not seem to consider the intensity of IAC. Whenever there is armed fire between states, the situation refers to an IAC. If a declaration of war[99] *per se* is sufficient to bring into force the Geneva Conventions, it is clear that the requirement of intensity is not needed to determine the status of an armed conflict initiated in this way.[100] 'Purely' declared war has not appeared since World War II in practice and formal declarations of war nowadays occur only very rarely.[101] A state of IAC also exists in the absence of hostilities in cases of belligerent occupation.[102] In conclusion, as a matter of law, in the course of assessment of IAC, the intensity requirement is only dependent on factual existence of hostilities and not necessary to be considered separately.

Put it in the cyber context, in case of cyber attack unaccompanied with other kinetic hostilities,[103] the question of whether the criterion of intensity is still unnecessary in the process of characterising inter-state cyber conflicts. However, there is no reason

---

[99] 'The essence of a declaration of war is an explicit affirmation of the existence of a state of war between belligerents.' (*Eritrea-Ethiopia Claims Commission Partial Award: Jus Ad Bellum* International Arbitral Awards (19 December 2005) 467 para 17); Convention (III) Relative to the Opening of Hostilities (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat. 2259 (Hague Convention III), art 1

[100] Anthony Cullen, *The Concept of Non-international Armed Conflict in International Humanitarian Law* (CUP 2010) 132; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 120-122.

[101] Dieter Fleck (ed) *The Handbook of International Humanitarian Law* (2nd edn, OUP 2008) 49 (for instance, Iran-Iraq War in 1980-1988, Pakistan-India War in 1965, Arab states in both 1948 and 1967); It should be noted that declaration of war can still be the beginning of war in the technical sense to date in case that actual hostilities follow it. (Yoram Dinstein, *War, Aggression and Self-Defence* (6th edn, CUP 2017) 32-35)

[102] Geneva Conventions I-IV, art 2(2); Roscini, *Cyber Operations and the Use of Force in International Law* 141-147.

[103] In case that cyber attacks are ensuing kinetic hostilities among states, it is not problematic in identifying the conflicts as an IAC. Cyber operations may be an integral part of a wider operation that constitutes an attack. A cyber operation may be used to disable defences at a garget that is subsequently kinetically attacked. LOAC on attacks applies fully to such cyber operations. (Michael N. Schmitt, 'Cyberspace and International Law: The Penumbral Mist of Uncertainty' 126 Havard Law Review Forum 176) This thesis limitedly aims to examine how to classify stand-alone cyber armed conflicts.

why the factors in kinetic context cannot be utilised in the cyber context as long as cyber attack is defined to bring about violent consequences. It should be also noted that a declared cyber war is unrealistic because it is scarcely reconcilable with the surprise and plausible deniability factors that constitute two of the main advantages of cyber operations.[104] Violent cyber operations conducted in the situation of belligerent occupation would be governed by the rule of IAC even without resistant cyber operations.[105] When there are cyber operations amounting to attack in or through cyberspace, an IAC would exist, even if short and limited in scope.[106]

On the other hand, the starting point of an international cyber armed conflict refers to the initial time of cyber attack. A given situation is supposed to be divided into two prongs: one is one-time scheduled setting of activation of malicious warm for cyber attack;[107] the other is being kept in control and monitored by an attacking state. In case of the latter, a cyber attack would be initiated with the installation of malware in the adverse state's networks because an attacking state has been continuously engaged in the cyber hostilities. The scheduled time would be the starting point of a cyber attack for the former case because a cyber attack is set to be actually launched at the appointed time.

---

[104] Roscini, *Cyber Operations and the Use of Force in International Law* 122.

[105] By analogical application of the common art 2 to the Geneva Conventions.

[106] Laurie R. Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015) 82.

[107] For example, on 17 and 18 December 2016, 'a power distribution station near Kiev was switched off and the Northern part of the city was cut off electricity for an hour' in Ukraine. In this cyber operation, malware programme dubbed 'Industroyer' or 'Crash Override' was infiltrated into the control system of electric power grid. Industroyer/Crash Override, which as a variation of Stuxnet, could be programmed to activate without operator's control even when the network is disconnected from the Internet. (Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' 112 AJIL 583 624-625)

IV. Conclusions

The existing IHL framework of classification in kinetic space, the criterion of actors is also applicable to classifying cyber armed conflicts. On the premise of the bifurcated IAC – NIAC structure of IHL, the issue as to whether the concerned conflict occurs between states take precedence over all other issues in classification.

In terms of the criterion of actors, state armed forces including regular and irregular members are comparatively well-established through a long history of the LOAC. As information and communication technologies (ICT) have been developed and the security risk surrounding the computer network systems have simultaneously increased, nation states tend to separately organise special cyber units of armed forces or specialised organs in governments, which are fully put on the charge of cyber tasks. In addition, states have established cyber security policies, military strategies, and long-term national plans for the furtherance of their cyber capacity and capabilities over civilian (private) as well as military (public) sectors.

The conditions of cyber combatant status, especially for the members of irregular armed forces such as cyber militia, voluntary cyber corps, *levée en masse* participants, and other organised groups, would be reconsidered to adapt to the inherent characteristic of high-speed and closely intertwined networks in cyberspace. When those members meet the conditions of cyber combatants under article 4(2) to the Geneva Convention III, their cyber militia, volunteer corps of hackers, and other organised groups of hackers are regarded as state-affiliated and irregular armed forces.

Next, attribution was discussed in classifying international cyber armed conflicts, as it has been also controversial in some kinetic context. Attribution tests have been debated by international courts and tribunals in cases, which investigated state responsibility or individual war crimes in armed conflicts. According to the effective control test held by ICJ, attribution to a state for state responsibility, punishment of war crimes, and classification of armed conflicts becomes consistent. However, there are other opinions such as ICTY that the attribution test can differ in respective areas of international law. The attribution test takes into account the object and purpose of the respective area of law. It should be considered which test is more suitable for the object and purpose of classification of cyber armed conflicts. Currently, there are no treaty laws, state practice, and sufficient discussion about this issue. It is only possible to analogically apply a more suitable test to the cyber context or to develop a new theory for characterising cyber armed conflicts. When a group of hackers conducts cyber attacks under the effective control of a state, the cyber attacks could be attributed to that state. Then, the concerned conflict comes to be an IAC (or internationalised).

In characterising an international cyber armed conflict, the confronting actors must be identified. When a group of hackers is state-affiliated as regular or irregular state armed forces, the concerned cyber conflict between that group and other states is classified as IAC. When the hacker group is proven to conduct cyber attacks against one state on behalf of other states on the basis of attribution test, the concerned conflict is classified as IAC. With regard to the criterion of intensity, when the forgoing cyber hostilities occur between states, an IAC is deemed to exist.

Chapter 4 – Non-International Cyber Armed Conflict

I. Introduction

As seen in chapter 3, the distinction between international armed conflict (IAC) and non-state armed conflict (NIAC) remains despite the argument of partial convergence of IAC and NIAC in international humanitarian law (IHL). On this assertive premise, the actors of IAC and NIAC are quite distinguished. The criterion of actors as the first step to assess the existence of an armed conflict is important in determining the character of the concerned situation by excluding an IAC. States or state-affiliated actors are identified based on their status and connection to states in IAC, whereas in order to recognise an armed group that triggers the application of IHL, the threshold of 'organisation' in NIAC requires more complex considerations. It may not be irrelevant to state attitudes towards recognising the actions of non-state actors as giving rise to the applicability of IHL. The difficulties of establishing the existence of NIAC would be intensified in the cyber context due to its special characteristics such as easy access and anonymity.

The definition of non-international armed conflict (NIAC) as 'protracted armed violence between governmental authorities and organised armed groups or between such groups within a state' is broadly accepted.[1] A NIAC is also characterised based on the two criteria of 'actors' and 'intensity'. According to the definition phrase of

[1] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* (Jurisdiction) ICTY (2 October 1995) para 70.

NIAC, ‘organised armed group’ is a new concept for the criterion of actors to be analysed and ‘protracted armed violence’ refers to the intensity of NIAC.

The existence of an organised armed group should be confirmed for the existence of an armed conflict *per se*. This is particularly important for considering actors in the cyber context where they are likely to be acting in looser networks, if in an organised structure at all. In other words, the question arises as to whether in fact any group acting in cyberspace – only organised online and exclusively engaged in cyber operations with members located in different states – could be said to meet the threshold of ‘organisation’ for the purpose of IHL. It is also questionable that these groups should satisfy higher threshold to be an organisation or have a different or specific qualification in cyberspace.

While the criterion of intensity has comparatively less importance in characterising IAC, it can be said that the ‘intensity’ assessment is of more significance in determining the existence of NIAC. Internal disturbances, such as riots, that have a potential to deteriorate into a NIAC can be more complicated and diverse. It could develop into a NIAC[2] or an IAC.[3] Otherwise, it would stay as merely domestic matter. Internal conflicts have increased in recent decades and this tendency has provoked more active debates surrounding the intensity criterion. However, compared to the other criterion ‘actors’, the analysis of intensity has not yet sufficiently unfolded in

[2] When the intensity of internal disturbances reaches the level of a NIAC, provided the actors requirement as between a government and an organised armed group or between groups within a state is satisfied, the concerned internal disturbances comes to a NIAC.

[3] When other states are newly involved in the internal disturbances on the side of an organised armed group, the concerned internal disturbances may develop into an IAC. On the other hand, if other states get involved in the internal disturbances with the consent of government on the side of state, the concerned internal disturbances may not be internationalised.

both state practice and academic debates.[4] In the same context, although internal conflicts would occur in cyberspace in a similar or easier way, the discourse about the extent to which, and the conditions under how, a cyber conflict could be of the intensity to attain the level of a NIAC has not developed yet. It is necessary to consider the intensity criterion in cyberspace with a more comprehensive approach, connected to a case-by-case analysis as well as organic interpretation considering the actors requirement for qualifying as a NIAC.

II. Organised Armed Group

1. Organised in Cyberspace

1.1. General Understanding

The legal character of the concerned group as 'organised' should be identified in order to ascertain the existence of NIAC.[5] In the absence of any state practice to the contrary, classifying cyber operations as a NIAC would mean that the IHL criteria would also apply in order to determine whether a certain group qualifies as a party to a conflict: the groups in question must be a collective entity, able to engage in sufficiently intense violence against the adversary, and capable of respecting basic

[4] Details of intensity assessment for kinetic armed conflicts have been suggested in international courts and tribunals such as International Criminal Tribunal for the Former Yugoslavia (ICTY), International Criminal Tribunal for Rwanda (ICTR), International Criminal Court (ICC), Special Court for Sierra Leone (SCSL) and so on. The cases that those jurisprudence dealt with follow somewhere necessary in this chapter.

[5] *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (Judgement) ICTY IT-03-66-T (30 November 2005) para 89; Monika Hlavkova, 'Reconstructing the Civilian/Combatant Divide: A Fresh Look at Targeting in Non-International Armed Conflict' Journal of Conflict & Security Law 1 9.

norms of IHL.[6] Logically, a group already meeting these qualities in a kinetic armed conflict would also qualify as an organised armed group for the purposes of engaging in non-international cyber armed conflict. Organisation only grouped in cyberspace is more confusing in that individual actors are physically invisible, remote, and largely intangible. The very characteristic of anonymity in cyberspace brings about the result that the more anonymous in operations, the more luring for non-state actors who want to be involved in armed conflict situation.[7] Prior to looking into cyber organisation, it should be noted that the issues in technologies such as tracing and proving cyber attacks are common in cyberspace. In this regard, those technical issues are excluded in legally analysing and examining structural characteristics of an organised armed group.

There would be two compositions of objective and subjective aspects in considering organisation of an armed group. An objective aspect refers to the existence of individuals and a certain level of cohesion among them through some structures or their manoeuvre. A subjective aspect refers to intention of that group of individuals. The first question is whether the intention or purpose of a group should be required or limited to some extent or kind. It is worth noting the research of the International Committee of the Red Cross (ICRC) about armed groups – any armed group, distinct from and not operating under the control of the state or states in which it carries out military operations, and which has political, religious, or military objectives. The ICRC observed: 'amongst armed groups, the distinction between politically-motivated action and organised crime is fading away. All too often the political objectives are

[6] Tilman Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law* (OUP 2018) 104-105.

[7] Jack Goldsmith, 'How Cyber changes the Laws of War' 24 EJIL 129.

unclear, if not subsidiary to the crimes perpetrated while allegedly waging one's struggle. Are we dealing with a liberation army resorting to terrorist acts, or with a criminal ring that tries to give itself political credibility? Are we dealing with a clan-oriented self-defence militia relying heavily on criminal funding, or with a Mafia-like gang whose constituency is strongly intertwined with ethnic communities?'[8] If so, putting a political intention into subjective element of the definition of armed groups, it becomes more difficult to identify the character of a given operation.[9] Some armed groups that stated political purposes could take criminal operations to achieve them and *vice versa*. In this regard, organised armed groups not only in a physical ground but also in cyberspace are not identified on the basis of their political purpose in reality. As a result, the existence of cyber organised groups must be confirmed based on their objective structures.

Dissident cyber armed forces can be thought of first because article 1(1) of the Additional Protocol (AP) II stipulates that dissident armed forces and other organised armed groups are the parties to NIAC. Dissident armed forces refer to the former military units that break away from state armed forces to stand against the incumbent government. When insurgency or rebellion occurs in a state, there could be small units of state forces to stand by the insurgent side.[10] In many situations of kinetic

[8] International Council on Human Rights Policy, *Ends & Means: Human Rights Approaches to Armed Groups* (2000) 5-8; ICRC, *Holdings Armed Groups to International Standards: An ICRC Contribution to the Research Project of the ICHRP* (1999) 2-3.

[9] International Council on Human Rights Policy, *Ends & Means: Human Rights Approaches to Armed Groups* 6.

[10] For example, in *Libya*, after the civil war broke out in 2011, part of the government forces turned their back the-then Gaddafi government and stood by the rebellion group side. Later, in the second civil war, armed actors in *Libya* showed very complicated features and state security forces were divided with some of them combined with opposition groups. '*Libya* does not have a straightforward delineation of State security forces and opposition forces. Instead, it has a complex set of armed actors, with varying degrees of association with the State and each other.'(Human Rights Council,

NIAC, dissident armed forces take an important role in insurgency in that they could sustain comparatively well-organised command and control structure and their members are well trained and equipped.[11] Therefore, there is little demand to consider the structure and membership of dissident armed forces to recognise.[12] In the case of non-international cyber armed conflict, we can also think of ex-cyber units of state armed forces,[13] which disengaged part of cyber units of state armed forces mentioned before.[14] If this cyber unit takes part on the side of an insurgent party to the internal conflict, they are regarded as dissident cyber armed forces in terms of classification. However, the fact of merely having been members of state armed forces is not sufficient to qualify individuals as members of a dissident armed force. Since dissident armed groups should also be characterised as organised armed groups, breakaway units from a states' military forces must retain some degree of their original organised structure.[15] This may also apply to dissident cyber armed forces.

It is necessary for an 'organised armed group' to have a command and control structure to 'enable them to carry out sustained and concerted military operations and

---

Investigation by the Office of the United Nations High Commissioner for Human Rights on Libya: detailed findings (A/HRC/31/CRP.3 23 February 2016))

[11] Yoram Dinstein, *Non-International Armed Conflicts in International Law* (CUP 2014) 40.

[12] 'Although members of dissident armed force are no longer members of state armed forces, they do not become civilians merely because they have turned against their government. At least to the extent, and for as long as, they remain organised under the structures of the state armed forces to which they formerly belonged, these structures should continue to determine individual membership in dissident armed forces as well.'(Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) 32); This analysis elicited no significant objection from the international experts during drafting process, whereas other aspects of the Interpretive Guidance arouse controversies.

[13] See, Chapter 3 – International Cyber Armed Conflict II. State and State-Affiliated Actors 1. Cyber Units of State Armed Forces

[14] Sandesh Sivakumaran, *The Law of Non-International Armed Conflict* (OUP 2012) 170, 172.

[15] Ibid 170.

to implement' IHL.[16] So, members of a group in the operational details of violence that they cause are necessarily pragmatic to identify a NIAC.[17] A command and control structure in cyberspace would be different from that of kinetic space. Non-state actors in cyberspace do not necessarily possess a physical connection among themselves; they could be completely strangers or even have no perception of each other's existence. The links among non-state actors in cyberspace can be established in a scattered and decentralised manner. For instance, as seen in Georgian cyber-attacks, where one website published a list or uploaded their own cyber-attack programmes which were dispersed anonymously.[18] On this point, it is problematic whether or not those cyber-actors could be regarded as 'organised' in terms of IHL.

1.2. Structure of Organisation

The organisation of armed groups could be analysed with both structural and temporal approaches. In terms of internal structure of a group, it seems to easily draw hierarchical command and subordinate chains.[19] This vertical structure is more common and broadly appears in many groups including dissident cyber armed forces.

---

[16] Additional Protocol II, art 1(1); The ICRC Commentary about this article explains as follows: 'the existence of a responsible command implies some degree of organisation of the insurgent armed group or dissident armed forces, but this does not necessarily mean that there is a hierarchical system of military organisation similar to that of regular armed forces. It means an organisation capable, on the one hand, of planning and carrying out sustained and concerted military operations, and on the other, of imposing discipline in the name of a *de facto* authority.' (Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC / Martinus Nijhoff 1987) para 4463); *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* para 89.

[17] Peter Margulies, 'Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"' 89 International Law Studies 54 62-63; *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* para 90.

[18] Eneken Tikk, Kadri Kaska and Liis Vihul (eds), *International Cyber Incidents: Legal Considerations* (CCDCOE 2010); Andreas Hagen, 'The Russo-Georgian War 2008' in Jason Healey (ed), *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (A CCSA Publication 2013)

[19] Sivakumaran, *The Law of Non-International Armed Conflict* 172.

Some indicators of organisation have been suggested in international jurisprudence. In the *Limaj* case, assessing the character of the Kosovo Liberation Army (KLA), the Trial Chamber of the ICTY held that 'some degree of organisation by the parties will suffice to establish the existence of an armed conflict. This degree need not be the same as that required for establishing the responsibility of superiors for the acts of their subordinates within the organisation, as no determination of individual criminal responsibility is intended under this provision of the Statute.'[20] The Chamber concluded that the KLA was an organised armed group,[21] and a subsequent determination consistent with this in other cases examining the same issue was held.[22] In the *Haradinaj* case, the ICTY surveyed all previous judgements relevant to the issue of organisation prior to concluding that no single factor can be ruled out as a 'determinative' one in assessing the degree of organisation. Rather, the Trial Chamber suggested a holistic approach. Factors that indicate organisation were recognised as follows: 'the existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; its ability to plan, coordinate, and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and use military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords'.[23]

---

[20] *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* para 89.

[21] Ibid para 90-134. (There were a variety of factors in estimating the degree of organisation such as the existence of a general staff and headquarters, designated military zones, adoption of internal regulations, the appointment of a spokesperson, coordinated military actions, recruitment activities, the wear of uniforms, and negotiations with the other side.)

[22] Jean-Jacques Fresard, *The Roots of Behaviour in War - A Survey of the Literature* (2004) para 16-25.

[23] *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (Judgement) ICTY IT-04-84-T (3 April 2008) para 60.

Herein, it is noteworthy that all these analyses have been done in an inductive way based on empirical fact-finding. The forgoing indicia extracted in kinetic cases could be put in the cyber context to identify cyber organisations which takes similar structure.

A group in question should exhibit a certain degree of structure, but this structure need not necessarily be hierarchical. Groups could be formed in a horizontal way in both kinetic and cyberspace.[24] For instance, there could be some guerrillas[25] or groups that carry on the shared goal with distributed resources and power to the units or individuals.[26] In addition, there are some cases that small groups with loose ties or individuals are affiliated with an organised armed group such as Al-Qaeda.[27] Such a horizontal structure would be more likely in the case of virtually organised groups. The question then arises as to what degree of cohesion is required to be assessed as organised among individual actors dispersed over cyber networks. This assessment is closely related to the way of cyber operations conducted by those individual actors in or through cyberspace.

How can a system of command and control be identified in the context of cyber groups? The dynamic of online command and control system needs to be observed and reconsidered from the perspective of IHL. For example, if individuals meet in the

[24] Margulies, 'Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"' 66-75; Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law* 75-85.

[25] Sivakumaran, *The Law of Non-International Armed Conflict* 172-173.

[26] Ibid 173.

[27] Peter Margulies and Matthew Sinnot, 'Crossing Borders to Target Al-Qaeda and Its Affiliates: Defining Networks as Organised Armed Goups in Non-International Armed Conflicts' 16 YBIHL 319 325.

same chatroom, can they be regarded as a group? For certain members to have a position of commander, what do they play a role in cyberspace? Do they take responsibility for who can enter and who can participate in the chatroom i.e. does a member decide who is allowed into the chatroom and who can be excluded? Other individuals who access the chatroom, how do they behave as members of the group? Rid hypothesises that 'internet-driven subversion is characterised by lower levels of organisational control.'[28] He gives an example of Anonymous which has high membership mobility, a loose and largely leaderless movement of activists.[29] Anonymous became visible to the larger public since 2008. About the question 'on what role hierarchy and internal authority play (if any) within the cyber group', there has been research about the internal structure of cyber groups who conduct offensive cyber operations representing Anonymous. According to the research, the Internet Relay Chat (IRC) servers were used to provide a peer-to-peer, instant messaging service that creates a hub for many Anonymous members to gather and coordinate their attack.[30] Investigation over the communications of IRC showed that there were some privileges, which are not all equal, observable within it.[31] 'The obvious question arises if one conceptualises Anonymous IRC as a classic hierarchical structure of command and control, how much influence could such small numbers of privileged nicks have over the wider community?'[32] One commentator concluded that the privileged nicks look like 'showmen attempting to attract support from an ever

[28] Thomas Rid, *Cyber War Will Not Take Place* (Hurst 2013) 115. ('Launching a subversive 'start-up' has become easier – but technology has a darker flipside for those attempting to undermine established powers.')

[29] Ibid.

[30] Stewart K. Bertram, 'Authority and Hierarchy within Anonymous Internet Relay Chat Networks' 6 Journal of Terrorism Research 15 15.

[31] Ibid 17-18.

[32] Ibid 23.

changing crowd, rather than commanders leading an army of followers and the internal structure of Anonymous is neither completely hierarchy nor a fully leaderless group. Additionally, it is incorrect to assume that all privileged members are ideologically aligned; instead, at any given time there are a multitude of privileged individuals advocating different (if not competing) causes within the IRC.'[33] Anonymous does not have 'a stable and identifiable membership'.[34] It also showed that high membership mobility inhibits the creation of hierarchy within a hyper-networked group like Anonymous.

To be organised, a group should be able to act in a coordinated fashion, albeit not to the extent of the regular armed forces in kinetic conflicts. This requirement encompasses the ability to plan and execute group activities, collect and share intelligence, communicate among members, de-conflict operations, and provide logistic support to operations. That is to say, the merely collective and accidental sum of actions against the adversary party does not suffice in characterising an 'organised' armed group. According to this standard, the above-mentioned Anonymous can be regarded as merely collective cyber operations or looser level of assemblage among individual users. Among the possibly various types of cyber warriors grouping, when a group of individuals simultaneously conduct cyber operations in a collective way in or through cyberspace, they may not be regarded as 'organised'. To cooperatively operate in the cyber context, the questions arise as to whether certain members necessarily provide the indispensable resources such as malware or instructions on how to obtain or activate it to enable a cyber-attack to happen. For instance, do they

[33] Ibid 24.

[34] Russell Buchan, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' 15 Chinese Journal of International Law 741 748.

identify vulnerabilities in the target's computer systems and networks and offer the information to others? Or do they coordinate when attacks should happen and at what frequency and intensity?

On this point, the *Tallinn Manual* 2.0 says as follows: 'the more difficult case is that of an informal grouping of individuals who operate not cooperatively, but rather 'collectively', that is simultaneously but without any intended coordination. For instance, acting with a shared purpose, they access a common website which contains tools and vulnerable targets, but do not organise their cyber attacks in any fashion.'[35] The major view of the working group of the Manual took the position that 'an informal grouping of individuals acting in a collective but otherwise uncoordinated fashion cannot comprise an organised armed group.'[36] In order to constitute an organised armed group, it must be 'a distinct group with sufficient organisational structure that operates as a unit'.[37] The other view was submitted that 'whether an informal group meets the organisation criterion would depend upon a variety of content-specific factors, such as the existence of an informal leadership entity directing the group's activities in a general sense, identifying potential targets, and maintaining an inventory of effective hacker tools.'[38]

In case of Anonymous, certain members have taken the privilege of pointing at targets and offering information of their cyber vulnerabilities and methods of cyber attacks.

---

[35] Michael N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 390.

[36] Ibid.

[37] Ibid 390-391.

[38] Ibid 391.

Leading members provide some advice and guidance to other members.[39] However, this feature does not seem to be a command and control chain as seen in organised armed groups in terms of IHL. Influences and authorities of privileged members over other members within Anonymous are not sufficient. The opportunities of members to contact each other is entirely dependent on their mutual willingness to logon to the discussion board, which clearly inhibits the authority of privileged members over other members and disciplinary internal structure.[40]

Another temporal approach to examine an organised armed group looks at how long a group needs to persist in order to be regarded as organised. In kinetic conflicts, there is either a perpetually organised armed group or a group that is transitory or *ad hoc* in nature. To establish internal structures for commanding and disciplining its members to conduct operations cooperatively, it unavoidably takes a certain period of time to become organised in the kinetic context.[41] Cyber organised armed groups, such as a hacktivist group, can exist on the *ad-hoc* basis to diffuse the same propaganda or to achieve shared goals. On the other hand, there would be a consistent group that endures over time but its membership is transient. In this case, if the internal structure of a group stands still as 'organised', only high membership mobility (transient membership) cannot hinder the group from being organised. Cyber operations conducted by hackers' group would last for a number of hours or days, but those cyber operations could be constitutive of non-international cyber armed conflict as long as the operations are sufficiently intense. If this group exists only during those

[39] Buchan, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' 749.

[40] Ibid 748.

[41] This duration factor can also have an effect on the criterion of 'intensity' of non-international (cyber) armed conflict. See, III. Intensity of Non-International Cyber Armed Conflict 1. Composition of Intensity 1.2. Duration

cyber operations, the organisation would then be confirmed in a stricter way because a short duration also influences the cohesion among its members.[42] On balance, the factor of duration can be said to be less critical in non-international cyber armed conflicts than in kinetic ones.

1.3. Capacity of Organisation

An organised group should possess the ability to respect fundamental humanitarian law and the capacity to execute sufficiently intense violence.[43] A qualified group capable of exercising some degree of control over the activities of its members, in particular, should be organised enough to comply with the LOAC.[44] However, failing to comply itself does not impede the qualification of an organised armed group.[45] This group also has to be capable to engage in sufficiently intense cyber violence in terms of IHL. Cyber organised armed groups, such as a hacktivist group, can exist on the *ad-hoc* basis with regard to a certain shared goal. Cyber operations conducted by hackers' group would last for a number of hours or days, but those cyber operations could be constitutive of non-international cyber armed conflict as long as the

[42] As a regional organisation, the Inter-American Commission on Human Rights (IACHR) characterised an engagement of Argentina's armed force with organised, armed militants that lasted thirty hours and resulted in casualties and property destruction as an armed conflict. (*Juan Carlos Abella v. Argentina* Inter-American Commission on Human Rights, Case 11.137 (18 November 1997) <http://www.cidh.oas.org/annualrep/97eng/Argentina11137.htm> accessed 31 October 2018 para 154-156)

[43] Additional Protocol II, art 1(1)

[44] Ibid.

[45] Andrew Clapham, 'Focusing on Armed Non-State Actors' in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (OUP 2014); Cedrin Ryngaert and Anneleen Van de Meulebroucke, 'Enhancing and Enforcing Compliance with International Humanitarian Law by Non-State Armed Groups: an Inquiry into some Mechanisms' Journal of Conflict & Security Law.

operations are sufficiently intense.[46] Because of this, the factor of duration could be considered less critical in non-international cyber armed conflicts than in kinetic ones.

In conclusion, the standards to confirm the existence of a cyber 'organised' group would be altered in the context of non-international cyber armed conflict. A cyber organised group could be established in both continuous and *ad hoc* bases with even a very shorter duration compared to an organised group in kinetic space if its individual actors cooperatively conduct hostile cyber operations with a certain level of internal structure.

2. Armed in Cyberspace

The next criterion of an organised armed group to be examined is 'armed'. The term 'armed' literally means that someone possesses arms. A group is also armed when it has the capacity to carry out 'attacks', which is defined as 'acts of violence against the adversary, whether in offense or in defence'.[47] Whether a group is 'armed' depends upon whether it conducts attacks that produce 'violence'. It can be said that the meaning of both cyber weapons and cyber attacks are essential to understand 'armed'

[46] Michael N. Schmitt, 'Classification of Cyber Conflict' 17 Journal of Conflict & Security Law 245; Goldsmith, 'How Cyber changes the Laws of War'.

[47] Additional Protocol I, art 49; Such acts for attacks should be come out of the group's intentions, not those of individual members. This is inferred from the fact that while many members of armed forces do not carry out combat functions, the armed forces as a whole entity are regarded as 'armed' under the LOAC. Article 43(2) of AP I identifies 'members of the armed forces' as 'combatants … [who] have the right to participate directly in hostilities,' not as individuals who do so participate. Put it in a reverse way, the mere fact that a part of group's members participate in hostilities does not render the group 'armed'. On the other hand, some organised groups such as Hamas in *Palestine* and Hezbollah in *Lebanon* are comprised of both armed and non-armed wings. To achieve a certain political purpose, some entities not only act as political parties but also have military wings. In this case, it is generally accepted that when the group in question consists of subgroups, only those that engage in hostilities qualify as organised armed groups. Individuals who play roles in both wings, for instance the overall leader, would be regarded as members of the armed subgroups, in spite of their coexisting non-hostile role.

in the cyber context. Cyber attack has been defined as a cyber operation, whether in offence or in defence, that brings about violent consequences against the adversary.[48] The other crucial question here is whether a group that possesses cyber weapons can be regarded as 'armed'. The definition of cyber weapons needs to be clarified because cyber attacks do not use arms in the conventional sense.

We easily recall the definition of weapon from gun, knives and tanks; devices which have violent damaging effect on people and objects. In this regard, 'one might define a weapon generically as a capability that can be applied to a military objective or an enemy combatant with the aim of either destroying or reducing the military effectiveness of the objective or incapacitating the combatant to the extent that he (or she) is rendered incapable of further effective combat.'[49] Then, the question arises as to what cyber weapons are and whether it falls under the scope of IHL.[50] When a hacker breaks into the firewall of military computer network system of the adversary, would it be qualified as cyber attack? And would the malware programme or code used by that hacker in a given cyber operation be regarded as cyber weapon? Finding answers to these questions leads to the meaning of 'armed' in cyberspace.

---

[48] See, Chapter I – Introduction III. Terms and Definition 2. Cyber Operations 2.1. Cyber Attack; Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' 96 IRRC 189; Oona A. Hathaway and others, 'The Law of Cyber-Attack' 100 California Law Review 817.

[49] Steven Haines, 'The Developing Law of Weapons' in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (OUP 2014) 276.

[50] Article 36 of the AP I offers the clue as to cyber weapon. The so-called Martens Clause was first enacted in the Hague Convention II with Respect to the Laws and Customs of War in Land of 1899 (Hague Convention II) and also stipulated in article 1(2) of the AP I. The International Court of Justice (ICJ) affirmed the Martens Clause as customary international law and the fundamentals of estimation of new weapons and methods. (*Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 para 78) Put it another way, a weapon, if it is determined *per se* to infringe the principles of humanity or the dictates of public conscience, would be against the Martens Clause. Hence, cyber weapon as a new type of weapon must conform with the Martens Clause and other rules of IHL.

There are conceptually two types of weapons: one which was originally designed to be arms such as guns, bombs, missiles, and tanks; the other are those which are originally neutral but depending on their usage transform into weapons. For example, there are some specifically identified weapons that have separate treaties about those such as chemical weapons and nuclear weapons.[51] Chemical substances and nuclear energy themselves are not necessarily designed to be weapons but could be weaponised by specific ways or by intention to use, and thus fall under the scope of IHL. More recently, the use of drones in the battlefield are also at issue in the same context.[52] A drone could be used in various ways such as commerce,[53] espionage[54] or

[51] Walter Krutzsch, Eric Myjer and Ralf Trapp (eds), *The Chemical Weapons Convention: A Commentary* (OUP 2014) 74-82;

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Use (adopted 13 January 1993, entered into force 29 April 1997) 1974 UNTS45 (The Chemical Weapons Convention, CWC), art II: Definition and Criteria

For the purpose of this Convention:

1. 'Chemical Weapons' means the following, together or separately:

(a) Toxic chemicals and their precursors, except where intended for purposes not prohibited under this Convention, as long as the types and quantities are consistent with such purposes;

(b) Munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals specified in subparagraph (a), which would be released as a result of the employment of such munitions and devices;

(c) Any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in subparagraph (b).

[52] Michael N. Schmitt, 'Drone Attacks under the Jus ad Bellum and Jus in Bello: Clearing the 'Fog of Law'' 13 YBIHL 311; Christof Heyns and others, 'The International Law Framework Regulating the Use of Armed Drones' 65 ICLQ 791; Steven J. Barela, *Legitimacy and Drones: Investigating the Legality, Morality and Efficacy of UCAVs* (Routledge 2016); Michael N. Schmitt, 'Drone Law: A Reply to UN Special Rapporteur Emmerson' 55 Virginia Journal of International Law 14; Jelena Pejić, 'Extraterritorial Targeting by Means of Armed Drones: Some Legal Implications' 96 IRRC 67.

[53] Matt Burgess, 'DHL's Delivery Drone Can Make Drops Quicker Than A Car' *WIRED* (10 May 2016) <https://www.wired.co.uk/article/dhl-drone-delivery-germany> accessed 5 November 2018; Alex Hern, 'DHL launches first commercial drone 'parcelcopter' delivery service' *The Guardian* (25 September 2014) <http://www.theguardian.com/technology/2014/sep/25/german-dhl-launches-first-commercial-drone-delivery-service> accessed 8 Febuary 2015.

[54] Mark Mazzetti, 'New Terror Strategy Shifts C.I.A. Focus Back to Spying' *The New York Times* (23 May 2013) <http://www.nytimes.com/2013/05/24/us/politics/plan-would-orient-cia-back-toward-spying.html?emc=tnt&tntemail0=y&_r=0> accessed 8 Febuary 2015.

even for leisure[55] whereas it is simultaneously a novel and powerful weapon in actual hostilities.[56] Put it in the cyber context, specially designed malware programme or a weaponised code for cyber attacks, which bring about violent effects, can be cyber weapons.[57] It can be more difficult to imagine the weaponisation of computer programs and codes than that of guns, bombs or missiles, because they have to go through the process of actualising violence such as installation, infiltration, or activation.

Unfortunately, there is currently no international consensus about the definition of cyber weapons.[58] When we think of how a weaponised code is different from physical weaponry,[59] a subjective factor, such as intention or purpose of the use of a code (or programme), seems to be crucial in identifying cyber weapons. As for the subjective factor of cyber weapons, there would be two aspects: the offender's intention to threaten or cause harm to targets and the target's perception of the weapon's potential to actually cause harm.[60] For the latter, in case of cyber weapons, a weapon's utility

---

[55] Kate Murphy, 'Things to Consider Before Buying That Drone' *The New York Times* (6 December 2014) <http://www.nytimes.com/2014/12/07/sunday-review/things-to-consider-before-buying-that-drone.html?emc=edit_tnt_20141206&nlid=53442825&tntemail0=y> accessed 8 Febuary 2015; Nick Wingfield, 'Now, Anyone Can Buy a Drone. Heaven Help Us.' *The New York Times* (26 November 2014) Technology <http://www.nytimes.com/2014/11/27/technology/personaltech/as-drones-swoop-above-skies-thrill-seeking-stunts-elicit-safety-concerns.html?emc=edit_tnt_20141126&nlid=53442825&tntemail0=y> accessed 8 Febuary 2015.

[56] Shuaib Almosawa and Rod Nordland, 'Drone Strike in Yemen Said to Kill Senior Qaeda Figure' *The New York Times* (5 Feb 2015) Middle East <http://www.nytimes.com/2015/02/06/world/middleeast/senior-qaeda-figure-in-yemen-killed-in-drone-strike.html?emc=edit_tnt_20150205&nlid=53442825&tntemail0=y&_r=0> accessed 8 Febuary 2015.

[57] Russia and China argue that a specific definition needs to be established by treaty because of cyber difficulties in classifying cyber weapons as 'arms'.

[58] US Department of Defense, *Department of Defense Cyberspace Policy Reoport* (Novemeber 2011) 8; Thomas Rid and Peter McBurney, 'Cyber-Weapons' 157 The RUSI Journal 6 6-7.

[59] Rid and McBurney, 'Cyber-Weapons' 6.

[60] Ibid.

as a weapon to intimidate an adversary may be said to critically lean upon the perception of the threatened party.[61]

Then, what does violence mean in the context of cyber? Violence typically means death or injury to people or damage to physical property. However, given society's dependence upon cyberspace in the Internet Age, the question arises as to whether violence can be interpreted to mean destruction or harm to the normal functions in critical infrastructures. For example, the code of NotPetya that Russian hackers infiltrated into the systems including Ukraine's spread automatically, rapidly, and indiscriminately.[62] It has been often said as 'the most devastating cyber attack in history' in the press.[63] The release of NotPetya showed that a weaponised code could disrupt a nation: 'at least four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency' were hit and the Ukrainian minister of infrastructure announced, 'the government was dead'.[64] According to the consequential approach about cyber attack corresponding to a kinetic attack, this case never refers to cyber attack in terms of IHL. Moreover, most of cyber incidents, which increasingly occurs to cause massive disruptions over both online and offline

[61] Ibid.

[62] About the overall legal review of NotPetya, Michael Schmitt and Lieutenant Colonel Jeffrey Biller, 'The NotPetya Cyber Operation as a Case Study of International Law' EJIL: Talk! <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/> accessed 15 July 2017; NotPetya, named from its resemblance to the precedent ransomware Petya, appeared in 2016 to extort victims to pay for a unlock key of their files, whereas the ransom message of NotPetya was proven fake and it was only disruptive. (Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' 112 AJIL 583 628-631, 657)

[63] Andy Greenberg, 'The Untold Story of Notpetya, The Most Devastating Cyberattack in History' WIRED <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 22 October 2018.

[64] Ibid.

such as DDoS by Botnets, would not be included in cyber attacks. Such attacks may not cause violence strictly speaking but they do cause destruction and harm that could result in harsher chaos or broader effects in one state. Nonetheless, the majority still view cyber attacks as a corresponding attack which brings about physically violent consequences. However, it cannot be exclusively said that this definition of violence will never be recalibrated to include cyber attacks that produce online destructive effects. If novel demand or necessity to protect humanity would be found in such massively disruptive incidents, a more inclusive interpretation about cyber attack could be encouraged in state practice.

It is obvious that the rules of IHL should be applied to cyber weapons, apart from the fact that the definition of cyber weapons has not yet been confirmed. The discourse for defining cyber weapons will continue through state practice concerning cyber operations. For the purposes of this thesis, it follows the definition of the *Tallinn Manual* 2.0: 'cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack.'[65] To date, this definition seems to be comparatively more updated and authoritative. When an organised group is facilitated

[65] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 452; ibid 452-453.

Rule 103 – Definition of means and methods of warfare

For the purposes of this Manual:

(a) 'means of cyber warfare' are cyber weapons and their associated cyber systems; and

(b) 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted.

with these cyber weapons to carry out cyber attacks, that group refers to a cyber organised armed group.

Going back to the incidents of NotPetya, there are two issues to pick up from the angle of IHL: whether it is a cyber weapon and whether the incidents which occurred in Ukraine were cyber attacks in terms of LOAC.[66] The NotPetya malware can be regarded as a weaponised code, cyber weapon in that it is 'foreseeably and likely risks causing consequences at the attack level'.[67] Strictly interpreting, the incidents in Ukraine cannot qualify as cyber attacks because there were only widespread disruptions not physically violent consequences.[68] However, there is a growing sense that a cyber operation creating massive disruption, but without unleashing violence or destruction, would be regarded as a cyber attack. This issue is also very closely related to the intensity of a cyber armed conflict in the following section.

III. Intensity of Non-International Cyber Armed Conflict

The requirement that a given violent situation has to meet a certain level of intensity could be interpreted in different ways. First of all, the question arises as to whether intensity is to be measured in relation to the damage caused or the intensity of the operation itself. The former is called a 'consequence approach' that is based on the

[66] After getting answers of these questions, it could be examined whether the intensity of incidents occurring in *Ukraine* reached the level of NIAC, or whether the incidents can be classified as IAC, if the incidents was attributable to Russia.

[67] Schmitt and Biller, 'The NotPetya Cyber Operation as a Case Study of International Law'.

[68] MARSH, 'NotPetya Was Not Cyber "War"' (August 2018) <https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/NotPetya-Was-Not-Cyber-War-08-2018.pdf> accessed 5 November 2018; Danny Palmer, 'NotPetya Malware Attack: Chaos But Not Cyber Warfare' *ZDNet* (16 August 2018) <https://www.zdnet.com/article/notpetya-malware-attack-chaos-but-not-cyber-warfare/> accessed 5 November 2018.

number of incidents of violence or the consequent number of deaths, injuries, or damage to property.[69] The latter approach refers to that the intensity could be assessed against the number of persons involved in the operations and the military resources used; 'equally, it could involve consideration of the geographic spread of the violence or its duration.'[70] This approach seems not to be adopted in that the aggrieved party or the third parties could not precisely measure the intensity of the concerned operations, which are only apparent to the aggrieving party. By this approach, the intensity of armed conflict comes to mostly depend on the aggrieving party's operational intention and purpose. In conflict situations, the concrete details of military operations are not easily revealed to the outside. Other parties, except the aggrieving party, can only speculate about the means and methods taken by the aggrieving party. For example, in the case of terrorist attacks, the terrorists may officially proclaim their premeditated explosion and shooting, however, the exact extent of damage cannot be premeditated by the attackers. Instead, the aggrieved party can estimate the conclusive scale and details of damage from the attack.

The logic underlying the criterion of intensity is similar with that of cyber attack as examined in the introductory chapter because both concepts take commonly consequence-based approach.[71] This is also because the violent and destructive effect of a cyber attack directly leads to how intense the concerned conflict is. In other words, a very powerful cyber attack could meet the intensity level of NIAC,

[69] Sivakumaran, *The Law of Non-International Armed Conflict* 167.

[70] Ibid.

[71] See, Chapter 1 – Introduction III. Terms and Definitions 2. Cyber Operations 2.2. Cyber Attack

extremely saying, but accumulated violent effects of cyber attacks would ordinarily reach the required level of intensity for NIAC.

1. Composition of Intensity

1.1. Gravity

Intensity can be analysed in its two constituent parts: gravity and duration.[72] The gravity aspect of intensity is understood as a sense of magnitude in the concerned confrontation.[73] The Appeal Chamber of ICTY in its *Tadić* case stated that 'there has been protracted, large-scale violence between the armed forces of different states and between governmental forces and organised insurgent groups.'[74] The Tribunal continuously used the term of 'large-scale' in confirming the existence of a NIAC.[75] The ICTY Trial Chamber determined that the criterion of protracted armed violence was interpreted in practice, including by the *Tadić* Trial Chamber itself, as referring more to the intensity of the armed violence than to its duration.[76] However, the International Criminal Court (ICC) Pre-Trial Chamber noted that the reference of 'protracted armed conflict between … organised armed groups' in the article 8(2)(f) of the Rome Statute of ICC 'focuses on the need for the armed groups in question to

[72] Eric David, 'Internal (Non-International) Armed Conflict' in Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law In Armed Conflict* (OUP 2014) 356-358.

[73] Ibid 356-357; Sivakumaran, *The Law of Non-International Armed Conflict* 167-170.

[74] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* para 70.

[75] Ibid para 97, 100, and 106.

[76] *Prosecutor v. Dusko Tadić* (Judgement) ICTY IT-94-1-T (7 May 1997) 193-196.

have the ability to plan and carry out military operations for a prolonged period of time'.[77] It is also considered a time-based criterion.

The aspect of gravity has been also found in the area of *jus ad bellum*. In the *Military and Paramilitary Activities In and Against Nicaragua* case, the ICJ held that 'as regards certain particular aspects of the principle in question, it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms'.[78] In assessing whether a particular hostile action directed at a state amounts to the level of an armed attack, the ICJ has examined the scale and effects of the concerned act.[79] Later, it reaffirmed that to constitute an armed attack a 'most grave' form of the use of force is required.[80] In the resolution on the *Definition of Aggression*, the United Nations (UN) General Assembly required an attack to be of 'sufficient gravity' before it is considered an armed attack.[81] The 2010 Review Conference of the Rome Statue of the ICC adopted a definition of the crime of aggression and referred to the character, gravity, and scale of an act of aggression as constituents of a manifest violation of the UN Charter.[82]

---

[77] *The Prosecutor v. Thomas Lubanga Dyilo* (Decision on the Confirmation of Charges) ICC-01/04-01/06, Pre-T Ch I (29 January 2007) para 234.

[78] *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14 para 191.

[79] Ibid 195.

[80] *Oil Platforms (Islamic Republic of Iran v. United States of America)* (Merits) [2003] ICJ Rep 161 para 64.

[81] UNGA Res 3314 (XXIX) (14 December 1974)

Article 2

The first use of armed force by a State in contravention of the Charter shall constitute *prima facie* evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.

[82] ICC Assembly of States Parties, Review Conference (Kampala) (Resolution RC/Res.6 11 June 2010) 18.

On the basis of the foregoing, the aspect of gravity is assessed in conflict situations for both 'attack' (or the existence of an armed conflict, *jus in bello*) and 'armed attack' (*jus ad bellum*).[83] However, it should be noted that each definition of gravity is different in its detailed intensity and how it applies to within each of fields. Gravity in terms of *jus in bello* is used to assess whether the concerned conflict is intense enough to reach the level of NIAC, whereas gravity in terms of *jus ad bellum* is used to distinguish an armed attack as the most grave form of use of force to justify self-defence.

1.2. Duration

In the *Tadić* formula, 'protraction' from the phrase 'protracted armed violence' could be interpreted as referring to the aspect of duration for the intensity criterion. Duration alone cannot be determinative because there could exist a prolonged but very low intensity conflict situation in reality. This type of situation does not seem to be regarded as an armed conflict due to its lack of intensity. On the contrary, the conflict situation with sufficiently grave intensity lasting a very short period of time can be regarded as an armed conflict. In conclusion, it can be said that the gravity factor is more critical for intensity, whereas duration is a complementary factor to the intensity assessment.

The Inter-American Commission on Human Rights (IACHR) characterised an engagement of Argentina's armed force with organised, armed militants that lasted

[83] Charter of the United Nations, art 51

thirty hours and resulted in casualties and property destruction as an armed conflict. It is based not only on duration but also on other aspects of the concerned situation.[84] Thus, 'as duration is an aspect of the intensity of violence, violence of a relatively brief duration may still amount to a NIAC provided that other indicators suggesting intensity are present to a significant degree.'[85]

The international jurisprudence has counted on indicative factors relevant for assessing the intensity criterion, none of which are, in themselves, essential to establish that the criterion is satisfied. These indicative factors include the number, duration, and intensity of individual confrontations,[86] the geographical spread of the conflict,[87] the type of weapons and other military equipment used,[88] the deaths, injuries, and damage caused by the conflict,[89] and the number of civilians fleeing combat zone. The involvement of the UN Security Council may also be a reflection of

[84] *Juan Carlos Abella v. Argentina* Case 11.137 (18 November 1997) <http://www.cidh.oas.org/annualrep/97eng/Argentina11137.htm> accessed 31 May 2018 para 147, 154-156; This duration was before considered for the other criterion of 'organised' armed group.

[85] International Law Association Use of Force Committee, *Final Report on the Meaning of Armed Conflict in International Law* (2010) 30.

[86] *Prosecutor v. Dusko Tadić* para 565-566; *Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić, and Esad Landžo* (Judgement) ICTY IT-96-21-T (16 November 1998) para 189; *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* ICTY IT-02-54-T (16 June 2004) para 28; *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* para 135-167; *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (Trial Judgement) para 49; *Prosecutor v. Ljube Boškoski, Johan Tarčulovski* (Judgement) ICTY IT-04-82-T (10 July 2008) para 216-234; *Prosecutor v. Ljube Boškoski, Johan Tarčulovski* (Judgement) ICTY IT-04-82-A (9 May 2010) para 22; *The Prosecutor v. Thomas Lubanga Dyilo* para 235.

[87] *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* para 29; *Prosecutor v. Ljube Boškoski, Johan Tarčulovski* (Trial Judgement) para 216-234, 243; *Prosecutor v. Ljube Boškoski, Johan Tarčulovski* (Appeal Judgment) para 22.

[88] *Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić, and Esad Landžo* (Trial Judgement) para 188; *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* para 30-31; *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (Trial Judgement) para 135-167; *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (Trial Judgement) para 49; *Prosecutor v. Ljube Boškoski, Johan Tarčulovski* (Appeal Judgement) para 22.

[89] *Prosecutor v. Dusko Tadić* (Trial Judgement) para 565-566; *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (Trial Judgement) para 135-167; *The Prosecutor v. Thomas Lubanga Dyilo* para 235.

the intensity of a conflict.[90] When the Security Council has released a series of resolutions over one conflict, it is easy for the international community to recognise the concerned situation exceeding a certain level of intensity. However, along with the Security Council's resolutions, more factors are required to prove the satisfaction of intensity criterion to constitute an armed conflict. It is necessary to examine to what level of violence should be conducted in the concerned hostilities to qualify as a NIAC.

2. Intensity Assessment of Non-International Cyber Armed Conflict

2.1. Substantive Contents of Intensity in Cyber Conflict

A cyber conflict could reach a sufficient level of intensity to satisfy the threshold of a NIAC, like a kinetic one. The question is then what degree of intensity is required for being a non-international cyber armed conflict. As long as it takes the consequence approach in assessing intensity, there would be no difference in the conclusive damage or injuries resulted from between kinetic and cyber attacks. In this regard, no specific reason is found to differentiate the intensity level of non-international cyber armed conflict from that of kinetic one. The evidence or analysis of such intensity could differ from those of a non-international kinetic armed conflict.[91]

[90] *Prosecutor v. Dusko Tadić* (Trial Judgement) para 567.

[91] Laurie R. Blank, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015) 83.

It is the same as in cyberspace that sporadic cyber incidents, even if those directly bring about physical damage or injury, do not constitute a NIAC.[92] International case law has suggested a variety of indicia: 'the gravity of attacks and their recurrence;[93] the temporal and territorial expansion of violence and the collective character of hostilities;[94] whether warriors parties were able to operate from a territory under their control;[95] an increase in the number of government forces;[96] the mobilisation of volunteers and the distribution and type of weapons among both parties to the conflict;[97] the fact that the conflict led to a large displacement of people;[98] and whether the conflict is the subject of any relevant scrutiny or action by the Security Council.'[99] But as for cyber conflicts, it should be noted that cyber operations alone could trigger a NIAC in only rare cases in terms of the intensity threshold.[100]

[92] 'Similarly, cyber operations that incite incidents such as civil unrest or domestic terrorism do not qualify as NIACs. For instance, the calls that appeared on the Internet for riots by the Russian minority in Estonia in 2007 cannot be regarded as meeting that threshold.' (Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 387)

[93] *Prosecutor v. Mile Mrkšić, Miroslav Radić, Veselin Šljivančanin* (Judgement) ICTY IT-95-13/1-T (27 Septemeber 2007) para 419; *Procesutor v. Enver Hadžihasanović, Amir Kubura* (Judgement) ICTY IT-01-47-T (15 March 2006) para 22; *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (Trial judgement) para 135-167.

[94] *Procesutor v. Enver Hadžihasanović, Amir Kubura* (Trial judgement) para 22**;** *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* para 28-29.

[95] *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* para 29; *Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić, and Esad Landžo* (Trial judgement) para 187.

[96] *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (Trial judgement) para 146, 159 and 164-165; *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* para 30.

[97] *Prosecutor v. Mile Mrkšić, Miroslav Radić, Veselin Šljivančanin* (Trial judgement) para 39-40, 407-408; *Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal* para 31.

[98] *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (Trial judgement) para 49.

[99] *Prosecutor v. Mile Mrkšić, Miroslav Radić, Veselin Šljivančanin* (Trial judgement) para 420-421; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 388.

[100] Robin Geiss, 'Cyber Warfare: Implications for Non-International Armed Conflicts' 89 International Law Studies 627 634.

The international group of experts for the *Tallinn Manual* struggled with the question of 'whether non-destructive cyber operations conducted during civil disturbances or in connection with other acts of violence not qualifying as a NIAC can tip the scale and cause the hostilities to rise to the level of an armed conflict'.[101] For instance, assume an organised armed group has orchestrated civil disturbances. Although destruction of property is involved, such destruction is insufficiently severe to meet the intensity criterion for NIAC. But when cyber operations are added, the overall violence level could exceed the intensity bar for being a NIAC. The international group of experts achieved no consensus as to whether non-destructive but severe cyber operations satisfy the intensity criterion.[102]

From the view of the author, since a non-destructive cyber operation cannot be admitted as a cyber attack meaningful in terms of LOAC, a non-destructive cyber operation in and of itself cannot make it for intensity to qualify as a NIAC.[103] However, when it comes to the case that non-destructive cyber operations being conducted during other acts of violence not referring to a NIAC, those cyber operations could intensify the civil disturbance situation, then progress it to a NIAC. Assuming the situation in which massive cyber operations against computer networks or systems that sustain critical national infrastructure, such as power stations, dams, or public transportation system, those cyber operations cause massive disruption in its normal function and lead to mayhem in society. When those cyber operations are accompanied with physically violent acts, the blocking of functions and services and

[101] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 388-389.

[102] Ibid.

[103] Non-destructive cyber operation would refer to 'network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, data theft, and the defacement of important governmental website, etc.'. (ibid 388)

social mayhem could be used to contribute to other kinetic attacks and potentially offer military advantages to the adversary party. Hence, the destructive character is indispensable for independently conducted cyber operations to qualify as a NIAC, whereas non-destructive cyber operations accompanying other acts of violence could at least play a role of increasing the whole intensity of the concerned conflict situation.

Violence caused by cyber operations must also be protracted to qualify a situation as a NIAC.[104] However, the meaning of protraction (or duration) in terms of intensity in cyberspace needs to be reconsidered. A cyber operation needs not to be as continuous as in kinetic armed conflicts. 'Frequent, albeit not continuous, cyber attacks occurring within a relatively defined period may be characterised as protracted.'[105]

2.2. Determination of Temporal Scope of Cyber Armed Conflict

Once a given armed clash situation is assessed as to whether its intensity reaches the required level for being an armed conflict, the question arises as to whether the character of the concerned conflict would last, even if its intensity later comes down below the required level. This is especially so given that 'failed and failing states are often associated with 'low-intensity conflicts' in which fluctuating levels of violence and sporadic outbreaks of hostilities predominate over sustained combat operations and large-scale military operations.'[106] On the point of fluctuating intensity level, the

[104] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* para 70.

[105] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 389.

[106] Robin Geiß, 'Armed Violence in Fragile States: Low-intensity conflicts, spillover conflicts, and sporadic law enforcement operations by third parties' 91 IRRC 127 135.

ICTY in the *Tadić* case clarified that 'IHL applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved.'[107] In other words, once the required level of intensity is satisfied, the concerned armed conflict would sustain its legal character until the whole armed conflict situation has ceased, regardless of its fluctuating intensity level. While this point does not seem controversial, it is important to discern the temporal point at which a given armed confrontation situation intensifies and meets the level of intensity for a NIAC. Once its intensity reaches the level of NIAC, lowered intensity thereafter does not influence on the classification of NIAC.

Duration not only implies the intensity level of a given conflict but also brings about reinforcement of the internal structure of an organised armed group. In a cyber attack, duration relates to the lapse of time between the installation of malware and its activation. The question arises as to when a cyber attack would be regarded to start and to reach the intensity level of non-international cyber armed conflict. A lag can generally be assumed between the implantation of malware into the target of computer network system and its actual activation. In this case, even assuming that the activation causes violent effects corresponding to a cyber attack, the question still remains as to at which point the concerned cyber conflict reaches the intensity level of a non-international cyber armed conflict. There would be time gap between the occurrence of cyber attack and the existence of a non-international cyber armed conflict.

[107] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* para 70.

From the stance of the aggrieved party, if it recognises the silent invasion of its computer systems in terms of defensive capability, the aggrieved party may counter-attack against the launching system of the adversary. If so, then there are several issues to be solved. First, not yet qualifying a cyber attack under the LOAC, is whether or not the aggrieved party recognising a suspicious invasion of some programme can set a so-called counter-attack or countermeasure against the launching party. Second, if it is permissible, it follows to what extent the counter-attack or countermeasure can be allowed by comparison with the initial invasion.

Returning to individually conducted cyber operations, in case that there is a lapse of time between the installation of malware and its activation, the conflict would be regarded as starting at the point of activation and generating violent effects. Thus, the period of time in between is not covered by the LOAC but instead could be subject to other relevant laws. In a non-international cyber armed conflict, protraction of a cyber operation is also not the requirement of intensity criterion as mentioned above. However, as circumstances require, the duration factor could be complementarily considered for the intensity criterion.

Next, given all other requisite requirements satisfied, it is also problematic when the planted malicious programme has gradually and slowly been activated and then brings about material damages to people or objects of the aggrieved party. The point differs in that after the activation of malware, there could be another considerable lapse of time in between the activation and reaching the intensity level for qualifying as a NIAC. This closely relates to the aforementioned duration issue. Assume the situation

where the activated malicious programme planted in the adversary's system and slowly expands its destructive effects over populations or objects. In spite of activation, the violent effects steadily intensify and then the overall situation at a certain point of time exceeds beyond the intensity bar of a NIAC. In this case, during the period of time between activation and reaching the intensity criterion of NIAC, the concerned situation could be classified as an internal cyber disturbances and tensions.

As seen in the previous chapter, no sooner a cyber attack is admitted between states, an international cyber armed conflict exists because the required intensity is relatively very low.[108] The starting point of international cyber armed conflict is then divided into two prongs of a one-time scheduled setting of activation and being kept controlled and monitored by an attacking state.

To put this in a non-international cyber armed conflict context, the question also arises as to whether this interpretation is identically applicable. It is rarely possible for a cyber attack to qualify as a non-international cyber armed conflict, which is different from an international cyber armed conflict. As mentioned above, the lapse of time, likely being characterised as internal cyber disturbances and tensions between a cyber attack and the point of reaching the required intensity for a non-international cyber armed conflict, would be variable on a case-by-case basis. During this period of time, there would not be a clear and meaningful distinction between automatically

[108] See, Chapter 3 – International Cyber Armed Conflict III. Whether Intensity Matters in International Cyber Armed Conflict

scheduled activation and continuous being controlled by the aggrieving party in terms of classification of the concerned cyber conflict.

A non-international cyber armed conflict would have more diversity in its forms and progress in practice. It would be simultaneously more difficult to trigger a non-international cyber armed conflict by means of mere cyber attacks. Recalling the states' reluctance to admit the existence of NIAC regulated by IHL in their territories, such a two-pronged approach seems to be more or less instrumental and schematic away from the reality. However, it is helpful to analyse as much as we can to be prepared for predictably upcoming internal cyber conflict situation. For the time being, it would be better to keep an eye on how the real incidents and state practice would unfold than to promptly answer this issue.

IV. Conclusions

The issue of a non-international cyber armed cyber conflict starts from whether cyber operations, without any accompanying kinetic military operations, could trigger a non-international armed conflict in terms of IHL. Considering the relatively higher threshold required for a NIAC, a stand-alone non-international cyber armed conflict seems to occur in rare cases.[109] Nonetheless, the international community have witnessed the possibility of appearance of sophisticatedly organised cyber groups that are capable of operating cyber attacks against states or between themselves. As seen above, there have been increasing internal cyber disturbances and tensions not being

[109] Michael N. Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 87.

armed conflicts such as massive disruptions and paralysis of critical infrastructures including electric grids, public transportations, banking systems, and other governmental functions in or through cyberspace.[110]

Clarifying the classification of non-international cyber armed conflict is necessary to get ready for distinguishing a NIAC from the lower level of cyber incidents. As to the criterion of actors, cyber organised armed groups should take an internal command structure to the extent to carry out sustained and concerted cyber operations.[111] This could be different in virtualised cyberspace. The characteristics of anonymity and invisibility in cyberspace allow an organisation to take cyber attacks as well as to gather together in a cooperative way while non-acquainted with each other. The required internal command structure could be established through a mere website to share a certain goal, and to distribute the means and methods of cyber attacks among individual cyber warriors. Such internal structure of cyber organisation could be of less command chains and more horizontal compared to that of kinetically organised group. At the same time, a cyber organisation can be sustained only for a very short period time or intermittently when it is necessary to work on the ground of the high-speed character of cyber attacks. For a cyber organisation to be armed in or through cyberspace, it should possess weaponised codes or malware programmes that can cause some violent consequences to the extent to qualify that use as a cyber attack. These cyber weapons can be defined as cyber means originally designed, or intentionally used, to cause either human injury or death or damage or destruction of

[110] Additional Protocol II, art 1(2)

[111] Additional Protocol II, art 1(1)

objects. Cyber weapons also need to comply with the Martens Clause and to be reviewed by the rules of IHL.

Next, the question relating to the criterion of intensity would be whether the indicators for assessing intensity could be generalised or more objectified. The assessment of the intensity level of armed conflict has developed on a case-by-case approach. Through the accumulated case studies of non-international kinetic armed conflicts in international jurisprudence, it has been proven that the assessment standards of intensity are not easy to schematise due to various spectra of NIACs even in the kinetic context. Under these circumstances, the intensity of non-international cyber armed conflict cannot help being examined for the present based on the analyses of that of non-international kinetic armed conflict because of the lack of state practice and discourse surrounding it. Analogical and hypothetical approach for the time being seems the only way to look into these relevant issues. However, this does not indicate the lack of its importance. If strictly applying the requirements of non-international kinetic armed conflict to cyber context as they are, it would be quite difficult to classify non-international cyber armed conflict in practice. When a cyber organised group especially incurs massive disruption of critical infrastructures by using cyber means, it is not classified as NIAC under the existing IHL. Instead, if they locate in the territory of victim state, the group is subject to domestic jurisprudence of the state. Otherwise, it could be extended to the issue of state responsibility between the territorial state where the group locates, and the victim state based on the obligation to prevent transboundary harmful cyber operations.[112] On the other hand,

[112] Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' 21 Journal of Conflict & Security Law 429.

there simultaneously remains a growing concern about whether such a characterisation of this situation is valid.

Chapter 5 – Transnational Cyber Armed Conflict?

I. Introduction

Territorial borders exist, which delineate areas governed by different legal systems. That is to say, territorial borders drawn in kinetic space (between nation states or other political entities) correspond to the 'law space'.[1] However, this correspondence is radically undermined in cyberspace. The rise of global computer networks has jeopardised the power of sovereign states not only to exert control over the Internet including individuals' online behaviours but also to defend intrusive access from other states.[2] Cyberspace features anonymity and active participation of individuals. Cyberspace can by nature provide a far easier way of grouping and connecting among people regardless of their factual acquaintances or territorial borders. So, there is a view of that 'the Internet was designed without any contemplation of national boundaries. The actual traffic in the Net is totally unbound with respect to geography', proclaimed by Vinton Cerf, who is recognised as one of the fathers of the Internet

[1] David R. Johnson and David Post, 'Law and Borders - The Rise of Law in Cyberspace' 48 Stanford Law Review 1367 1368.

[2] About 'when geographic boundaries for law make sense', David R. Johnson and David Post suggested the following four aspects for the development and enforcement of legal rules: 1) power – control over physical space, and the people and things located in that space, is a defining attribute of sovereignty and statehood; 2) effects – the correspondence between physical boundaries and 'law space' boundaries also reflects a deeply rooted relationship between physical proximity and the effects of any particular behaviour; 3) legitimacy – generally accepted notion that the persons within a geographically defined border are the ultimate source of law-making authority for activities within that border, in other words, it can be said as 'consent of the governed'; 4) notice – physically boundaries are also appropriate for the delineation of 'law space' in the physical would because they can give notice that the rules change when the boundaries are crossed. (ibid 1369-1370)

credited with designing much of its structure.[3] On the other hand, Cyber disturbance, rebels or cyber attacks are more enticing to those non-state actors – who are willing to stand against their own government or external entities including other states, international organisations, different ethnic or religious groups – due to the cost-effective benefit and easy access of cyberspace.[4]

The fundamental question arises on this point as to whether territoriality or conceptualised geography in the existing international law can still identically apply to cyberspace. It is the first issue whether the borderless character of cyberspace could be respected as it is in the era of cyber armed conflicts in terms of international humanitarian law (IHL). The governance and regulability over cyberspace would be first considered.

In researching classification of cyber armed conflicts in IHL, the main issue in relation to geography would be of whether a so-called transnational armed conflict (TAC, or extraterritorial armed conflict) is necessary as the new third category of an armed conflict.[5] The argument of TAC to date has been developed in kinetic context.

---

[3] Lisa Guernsey, 'Welcome to the World Wide Web. Passport, Please? ' *The New York Times* (15 March 2001) Technology <http://www.nytimes.com/2001/03/15/technology/15BORD.html> accessed 21 September 2015.

[4]Andreas Paulus and Mindia Vashakmadze, 'Asymmetrical War and the Nothing of Armed Conflict - A Tentative Conceptualization' 91 IRRC 95.

[5] Roy S. Schöndorf, 'Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?' 37 New York University Journal of International Law and Politics 1 3 (This article focused on one type of such non-traditional conflicts: 'extra-state hostilities which is defined as 'ongoing hostilities between a state and a non-stat actor that take place, at least in part, outside the territory of the state'.); Djemila Carron, 'Transnational Armed Conflicts' 7 Journal of International Humanitarian Legal Studies 5; Claus Kreß, 'Some Reflections on the International Legal Framework Governing Transnational Armed Conflcits' 15 Journal of Conflict & Security Law 245; Marco Milanovic, 'The Applicability of the Conventions to 'Transnational' and 'Mixed' Conflicts' in Andrew Clapham, Paola Gaeta and Marco Sassòli (eds), *The 1949 Geneva Convnentions: A Commentary* (OUP 2015); Tamás Hoffmann, 'Squaring The Circle? International Humanitarian Law And Transnational Armed Conflicts' in Académie de Droit International de La Haye (ed), *Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts (Law Books of Academy)* (Brill 2010)

As seen through the previous chapters, the conditions to be considered are the 'actors' who actually participate in hostilities, and the 'intensity' of which hostilities occur in the field. There seems, in principle, no room to consider the geographical aspects of an armed conflict in order to classify the concerned conflict. However, the existing bifurcation of international armed conflict (IAC) and non-international armed conflict (NIAC) in the law of armed conflict (LOAC) has been challenged with another aspect of geography. There is no reason to develop a different framework of classification in cyberspace than that in kinetic space. TAC as a newly suggested category of armed conflicts should not exclude its application to cyberspace, if it is accepted. Thus, the issue of whether TAC could be accepted would be examined on the ground that the existing argument of TAC should be valid in both kinetic and cyber contexts.

II. Spatial Conceptualisation for Cyber Armed Conflict

Ahead of looking into the geographic aspects challenging the classification of armed conflicts in IHL, the encompassing meaning of geography and territorial sovereignty in cyberspace is herein considered. In order to know whether the traditional concepts of territorial sovereignty and jurisdiction could be implemented in cyberspace as in physical space, these questions follow: cyberspace as virtualised reality, is it a 'territory' which belongs to, or can be captured by, one state's sovereignty? Would a state be capable or eligible to take overall control over a portion of cyberspace? Otherwise, would the premise of sovereignty be challenged in cyberspace? If not, how could the control over cyberspace allocated among sovereign states? Then, what is the accurate legal nature of cyberspace in international law? All of these questions refer to spatial reconceptualisation for characterising cyber armed conflicts.

1. Sovereignty in Cyberspace

Territorial sovereignty means that a state exerts full and exclusive control over its territory.[6] A state is entitled to internal sovereignty: to exercise jurisdiction over persons and objects located within its territory pursuant to domestic legislation and to enforce those laws. A state also holds external sovereignty so as to not be intervened upon by other states within its territory. The International Court of Justice (ICJ) in its *Corfu Channel* case confirmed that 'between independent states, respect for territorial sovereignty is an essential foundation of international relations.'[7] To date, territorial sovereignty is understood to encompass all the dimensions over which state is able to access and to take control, such as land, air, sea and internal waters.[8] Comparatively recently, cyberspace has given rise to controversy about whether or not it is fully subject to the exercise of territorial sovereignty.

Facing the situation that cyberspace is now commonly described as a 'new domain of warfare' (new battlefield), the borderless character of cyberspace requires reconsidering spatial (geographical) concepts relevant to cyber armed conflicts in IHL.[9] There have been at least two competing theories in lieu of state sovereignty:

---

[6] *The Case of the S.S. Lotus (France v. Turkey)* 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7); *Island of Palmas (or Miagnas) (The Netherland v. The United States America)* PCA Case No. 1925-01 2 R.I.A.A. 829, 838.

[7] *Corfu Channel case* (Merit) [1949] ICJ Rep 4 35.

[8] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UNGA Res 2131 (XX) (21 December 1965)

[9] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (October 2010); US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (2011); The Ministry of Foreign Affairs of Russian Federation, *Convention on International Information Security* (22 September 2011) <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666> accessed 23 October 2018; The Ministry of Foreign Affairs of Russian Federation, *Draft United Nations Convention on Cooperation in Combating Information Crimes* (2018); German Federal Ministry of Interior, *Cyber Security Strategy for Germany* (February 2011)

first, that cyberspace could be regarded as immune from state sovereignty; and second, that cyberspace could be regarded as a global common comparable with outer space or deep sea. There is another view that the existing rule of state sovereignty can apply to different aspects of cyberspace and states can project or extend their sovereignty.

There are those who regard cyberspace as one of the global commons. The preliminary question then arises as to how the 'global commons' have been defined in international law.[10] There is no universally confirmed definition of global commons but two international governmental organisations, the United nations (UN) and the Organisation for Economic Co-operation and Development (OECD), have defined 'global commons' as 'natural assets outside national jurisdiction such as the oceans, outer space, and the Antarctic'.[11] Through analysing the common aspects for them to qualify as the global commons, it would be clear whether cyberspace could be regarded as one of them.

It should first be noted that there are international treaties governing the respective natural assets: the United Nations Convention on the Law of the Sea,[12] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies,[13] and the Antarctic Treaty.[14]

---

[10] Surabhi Ranganathan, 'Global Commons' 27 EJIL 693.

[11] Organization for Economic Co-operation and Development, Glossary of Statistical Terms, *Global Commons*, <http://stats.oecd.org/glossary/detail.asp?ID=1120> accessed 5 April 2017; United Nations Statistics Division, Global Commons Definition, <http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573> accessed 5 April 2017.

[12] United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 3, art 3.

[13] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (adopted 27 January 1967, entered into force 10 October 1967) 610 UNTS 205, art 2

Each of these treaties addresses specific permissible uses and prohibitions for the natural assets falling under their scope.[15] Each of the treaties, which bounds, or defines, areas of sovereignty and thus areas that constitute the global commons, also addresses the issue of sovereignty.[16] States could not realistically expect to exercise sovereignty over these areas when they established these treaties[17] even if a nation wanted to assert its sovereignty over the entirety of these natural assets. Nonetheless, it could not be asserted whether the areas where a state could reasonably exert sovereignty would end up as part of global commons.

The requirements to be global commons are not literally limited to 'natural assets outside state jurisdiction'.[18] Rather, it would be proper to accept global commons as the concept that includes the foregoing characteristics. In addition, global commons do not mean the absence of sovereignty but the presence of a shared global sovereignty.[19] On the basis of this understanding, it is unlikely that cyberspace qualifies as a global common.[20] There seems no shared ideas to date that state sovereignty should be limited to some extent or shared among states in cyberspace.

Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty…

[14] The Antarctic Treaty (adopted 1 December 1959, entered into force 23 June 1961) 402 UNTS 71.

[15] Patrick W. Franzese, 'Sovereignty in Cyberspace: Can It Exist?' 64 The Air Force Law Review 1 16.

[16] Ibid.

[17] Ibid 17.

[18] Ranganathan, 'Global Commons' 693. (''Global commons', which may include spaces beyond national jurisdictions, essential resources and concerns such as biodiversity conservation and climate change, are the focus of much international interest from a governance perspective. The proposition that they must be subjected to global regulation rarely creates controversy, although disputes arise when we turn to specific issues: how to identify global commons and which rules, principles and standards to embrace for their regulation.')

[19] Duncan B. Hollis, 'Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (OUP 2015) 136; Franzese, 'Sovereignty in Cyberspace: Can It Exist?'.

[20] Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' 89 International Law Studies 123 125-126.

The argument that cyberspace should be free from governmental influence or state sovereignty arose from the fact that virtual space appears to be potentially extremely democratic and accessible. The one statement that embodies this concept was made by John Perry Barlow, a co-founder and co-chair of the Electronic Frontier Foundation, which is dedicated to protecting 'digital freedom'.[21] A 'Declaration of the Independence of Cyberspace' was written by Barlow in response to the 'Telecommunications Act of 1996', passed in the United States, and proclaimed that 'governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.'[22] This statement proclaims the tendency to deny official and dominating governance of governments over cyberspace and the desire to preserve cyberspace as the remaining place of full equality and democracy. In short, the argument is that international law, sovereignty, and jurisdiction should not extend to cyberspace.

The idea that cyberspace is free from state sovereignty also proved hardly acceptable in reality, even though the argument of free flow of information remains.[23] First of all, cyberspace ought to be controlled for it to exist and function. It is founded on a 'physical structure' that is territorially located and thus logically falls under the purview of that state on which the physical asset is based. To that extent, cyberspace

[21] Electronic Frontier Foundation, <https://www.eff.org/about/board> accessed 12 July 2018; <http://www.egs.edu/faculty/john-perry-barlow/biography/ > accessed 5 April 2014.

[22] Electronic Frontier Foundation, A Declaration of the Independence of Cyberspace, <https://projects.eff.org/~barlow/Declaration-Final.html > accessed 25 October 2018.

[23] Michael N. Schmitt and Liis Vihul, 'Sovereignty in Cyberspace: *Lex Lata Vel Non*?' 111 AJIL Unbound 213 217-218.

has some tangible attributes that can be regulated along with the conducts of those who operate within the domain.[24]

Second, the contents exchanged through cyberspace hold significance in the real world as well: 'while cyberspace ideally allows for the free flow of information, no cyberspace exemption shields information from the valid interests of the state where information is sent, received, or stored.'[25] For instance, most countries prohibited the production, possession, distribution, and spread of child pornography on the Internet.[26] That is to say, information accessible to the individuals located in the respective states via cyberspace is subject to the domestic laws within that state. The thought to leave cyberspace purely democratic and ungoverned in the early development of the Internet is no longer compatible with the role played by the Internet in contemporary era. Instead, much like the real world, which requires state sovereignty to regulate, protect, and punish various actors, cyberspace needs this sovereign influence as well. While the law enforcement systems to regulate cyberspace have been developing, one can be assured that states have valid interests in legitimate regulation over cyberspace.

Above all, cyberspace cannot be immune from state sovereignty as a matter of national security, which is more directly involved with the overall thesis topic. All states connect to and operate some of their critical infrastructure, such as banking, finance, chemical, energy, water, law enforcement, national defence system, and

[24] Louise Arimatsu, 'Spatial Conceptions of the Law of Armed Conflict' in Jr. Robert P. Barnidge (ed), *The Liberal Way of War* (Ashgate 2013) 185; Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2008) 181; Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' 126-127.

[25] Franzese, 'Sovereignty in Cyberspace: Can It Exist?' 13.

[26] Ibid.

public transportation, in or through cyberspace.[27] Those cyber infrastructures have, in practice, been targeted by other states or non-state actors for espionage, spying, or direct attack. Since 'the potential to cause harm in cyberspace is real and continues to grow, states never can leave cyberspace ungoverned but must find a way to exert their control and authority to reduce their vulnerability.'[28] As a result, cyberspace falls under the control of state sovereignty; a state is eager to exert its sovereign controls as a matter of law because another state may exploit cyberspace as a mean of gaining a strategic and military advantage over them. To put it conclusively, the foregoing two theories are not only logically incorrect but also non-reflective of the reality of state practice.

Lastly, the view of that the existing rule of state sovereignty can apply to cyberspace has survived. The matter of how state sovereignty is realised in cyberspace need to be examined. In so far as states are aware of their interests in cyberspace, they want to exert more and more control as new technology emerges and matures. On the one hand, some states seem to be hesitant in asserting their scope of sovereignty in cyberspace.[29] In the past, some states were actually hesitant to comment publicly upon cyber attacks since they did not want to enhance publicity on this issue especially in the situation that states' interests in cyberspace were not clearly identified and their tactics were not accordingly fully-established.[30] As one of the indicators of effective exercise of state sovereignty, states must be able to counteract with defence, reprisal, or punishment against an attack or law-breaking, whomever

[27] Ibid.

[28] Ibid 14; Tom Ginsburg, 'Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0' 111 AJIL Unbound 205.

[29] Franzese, 'Sovereignty in Cyberspace: Can It Exist?' 37-38.

[30] Richard A. Clarke and Robert K. Knake, *Cyber War* (HarperCollins Publishers 2010)

the actor is. On the other hand, in case that a state is subject to an armed attack in kinetic world, the state is eligible to take measures such as self-defence, collective self-defence, or countermeasures pursuant to international instruments including the UN Charter.[31] In case of receiving cyber attacks, rarely does a state claim that that state violated its sovereignty because the state of origin is not sufficient to establish attribution. Nonetheless, the discourse of cyber security has been publicly noticed in the international community as seen from the fact that a number of international institutions and national bodies have been intensifying their counter-capability to deal with cyber security.[32]

It is helpful to acknowledge how state sovereignty is understood in the cyber context. States have been intensifying their own sovereign power in cyberspace and building up several international standards to regulate cyber security. In the report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), the group confirmed the non-exhaustive views on how international law including state sovereignty applies to the use of Information and Communication Technologies (ICTs) by states.[33] The then-group offered recommendations about state sovereignty that 'states should not knowingly allow their territory to be used for internationally

[31] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI (UN Charter) art 51, 41 and 42.

[32] As examples, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Organisation for Security and Co-operation in Europe (OSCE), Respective National Cyber Commands and Units (see, Chapter 3), etc.

[33] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174 22 July 2015) 12.

> 27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by states of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.'

wrongful acts using ICTs; states should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account due regard for sovereignty.'[34] Therefore, it can be said that state sovereignty in cyberspace is respected in the international community, whereas it cannot be assured to what extent states have agreed on the details of state sovereignty in cyberspace.

The *Tallinn Manual* 2.0, which was co-worked by the international group of experts hosted by the CCDCOE, seems to fully accept the existing rules of sovereignty confirmed in the kinetic context.[35] Its Rule 2 stipulates internal sovereignty such that 'a state enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.'[36] Rule 3 provides external sovereignty such that 'a state is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.'[37] Rule 4 also states 'a state must not conduct cyber operations that violate the sovereignty of another state' in the cyber context.[38] There

---

28. (b) In their use of ICTs, states must observe, among other principles of international law, state sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other states. Existing obligations under international law are applicable to state use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;

[34] Ibid 7-8, para 13.

[35] Phil Spector, 'In Defense of Sovereignty, In the Wake of Tallinn 2.0' 111 AJIL Unbound 219.

[36] Michael N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 13.

[37] Ibid 16-17.

[38] 'This Rule applies in the relations between states, that is, to actions undertaken by, or attributable to, states. The International Group of Experts agreed that it does not extend to the actions of non-state actors unless such actions are attributable to a state. In other words, only states shoulder an obligation

are arguments and different state practice on this rule surrounding the legal effect of the violation of sovereignty in cyberspace.[39]

As seen through the foregoing chapters, cyber operations can amount to an armed attack, use of force, attack, or intervention of international law according to how violent they are in its effects (consequences). Cyber operations, which are mounted from outside of a state's territory, can violate that state's sovereignty below those foregoing thresholds based on 'the degree of infringement upon the target state's territorial integrity and whether there has been an interference with or usurpation of inherently governmental functions'.[40] In this case, there is controversy over whether state sovereignty is a primary rule of international law[41] or a non-binding and declaratory principle of international law.[42] If sovereignty is admitted as a primary law, the violation of state sovereignty in cyberspace brings about legal responsibility on the conducting state. There seems no reason to deny the legally binding nature of state sovereignty in cyberspace.

Be that as it may, it is sufficient herein to ascertain that state sovereignty is compatible in cyberspace because cyber operations at least amounting to the level of

---

to respect the sovereignty of other states as a matter of international law and therefore only states can breach that obligation.' (ibid 17)

[39] Lieutenant Colonel Jeffrey Biller and Michael Schmitt, 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences' EJIL:Talk! <https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/> accessed 24 October 2018; 'Some states have hesitated to confirm the principle of sovereignty as one that prohibits certain type of cyber operations. … Hesitant states appear to see the greater latitude to pursue national security objectives in cyberspace that derives from the absence of a primary rule of sovereignty as outweighing the likely costs of hostile cyber operations that might violate their sovereignty.'(Schmitt and Vihul, 'Sovereignty in Cyberspace: *Lex Lata Vel Non*?' 214)

[40] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 20.

[41] Michael N. Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' 95 Texas Law Review 1639; Spector, 'In Defense of Sovereignty, In the Wake of Tallinn 2.0'.

[42] Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' 111 AJIL Unbound 207.

attack are only relevant for the purpose of classification of cyber armed conflicts. Cyber operations below the level of use of force or intervention fall short of attack in terms of IHL. The foregoing debate shows that different interpretations and legal discussions have been underway in order to apply international law to cyberspace. In conclusion, the rules of sovereignty are respected in cyberspace and a cyber operation conducted by a state against cyber infrastructure located in other states infringes the latter's sovereignty. The concept of territorial sovereignty is also sustained in cyberspace. State practice to come will influence future attempts to establish clearer sovereignty rules in cyberspace.

2. Three Dimensions of Geography in an Armed Conflict

To understand the dynamics around geography of an armed conflict, it should be borne in mind that actual hostilities are often in a state of flux, so the whole picture of geography in an armed conflict and the ensuing application of LOAC is hardly fixed at an early stage. In terms of the legal character of an armed confrontation, the issue as to whether it arrives at the threshold of an armed conflict in the legal sense or remains at the stage of a temporal violent incident, could be gradually solved as the situation progresses.[43] Thus, it is necessary to understand that the perception of geography in an armed conflict is multifaceted and nearly incapable of defining at one go.

[43] For example, cyber attacks in Estonia in 2007 was neither accompanied by kinetic conflicts nor reached the level of an armed conflict. On the other hand, like the civil war in Syria (2011-Present), internal disturbances or riots became a NIAC in terms of IHL as situations progress. In some cases, it could just remain as non-NIAC violence such as internal disturbances in Kenya (2007-2008).

There are three dimensions of geography of hostilities (*factual, legal, and political)* used to analyse an armed conflict. First, *factual* geography refers to the actual place of which hostilities occurred in reality. Second, *political* geography means the reinterpreted version of geography which is added with policy consideration as seen in governmental reports or press, etc. Last, *legal* geography refers to the geographical scope being subject to the application of LOAC. This chapter mainly concerns *legal* geography. The implications of 'geography' in classifying cyber armed conflicts would be examined on the ground that this conceptual distinction of geography could better reflect actual features of armed hostilities. The conceptual distinction of 'geography', in particular, may be more useful in the context of NIAC because it requires more complex assessment procedures in order to be identified, whereas an IAC is comparatively easily determined based on the criterion of actors as an interstate armed conflict.

3. Deterritorialisation of Armed Conflicts

The legal bifurcation of international and non-international armed conflict starting from the very first phase to characterise an armed conflict has been entrenched through the historical progress of codification of LOAC. Under the dichotomy of IAC and NIAC, the rules relating to geographical scope are respectively set up in the relevant applicable laws. It could be said that 'the most far-reaching consequence of territorialised legal reasoning in IHL is the necessary bifurcation of LOAC that now distinguishes between international and non-international armed conflicts.'[44] It is also

[44] Louise Arimatsu, 'Territory, Boundaries and the Law of Armed Conflict' 12 YBIHL 157 170.

important that the fundamental point of geographical issues is where the battle space is in the legal sense.

Common article 2 to the Geneva Conventions and Additional Protocol (AP) I do not recognise any geographical limit in an IAC. State parties to the conflict may resort to armed forces in 'all the territory of the parties to the conflict as defined by the national boundaries', 'the high seas (including the airspace above and the sea floor)', and 'exclusive economic zone'.[45] The LOAC is, in principle, not limited to the regions where actual hostilities are being carried out but some individual rules of LOAC could have limited application in several ways. Put it another way, the *factual* geography of hostilities is not always identical to the *legal* geography of said hostilities. Setting aside other legal issues that may be raised by the incursion of hostilities to the third state such as violation of state sovereignty and possible reactions of that state, it is submitted that the legal character of IAC is sustained.

In a NIAC, the applicability of LOAC extends to the entire territory of the state concerned and is not limited to areas of actual combat or their vicinity.[46] In the *Tadić* case, the defendant argued before the International Criminal Tribunal of the Former Yugoslavia (ICTY)'s Appeals Chamber that there had been no armed conflict of any kind in *Prijedor* at the relevant time.[47] This argument assumes that an armed conflict exists only in those parts of a state (or states) where actual fighting is taking place at

[45] Jann K. Kleffner, 'Scope of Application of International Humanitarian Law' in Dieter Fleck (ed), *The Handbook of Humanitarian International Law* (3rd edn, OUP 2013) 56.

[46] Ibid 59.

[47] 'Instead, he maintained that the Serb inhabitants had assumed authority in the region without active resistance on the part of the Muslim and Croat inhabitants, so that, whatever the position may have been in other parts of Bosnia-Herzegovina, there had been neither an internal nor an international armed conflict in *Prijedor*.' (Christopher Greenwood, 'International Humanitarian Law and the *Tadić* Case' 7 EJIL 265 269)

any given time. However, it does not accord with any rules of IHL. The Appeals Chamber in *Tadić* case held that:

> …an armed conflict exists whenever there is a resort to armed forces between states or protracted armed violence between governmental authorities and organised armed groups or between such groups within a state. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring states or, in the case of internal conflicts, the whole territory under the control of a party whether or not actual combat takes place there.[48]

Also described in the decision of *Tadić* case, the determination of geographic scope of an armed conflict in order to apply LOAC depends on whether actual hostilities occur in the same territory and is estimated based on the overall range of conflict.

Assuming the situation when an internal armed conflict crosses over a border causing the conflict to straddle at least two countries, the question arises as to whether the concerned conflict still remains non-international in its classification or automatically becomes internationalised on the basis of its transborder aspect. In the cyber context, there would be the place of launching an attack (*locus actus*), the place of committing an attack (*locus criminis*), and the place of routing an attack. Most cyber attacks take a detour through numerous states or computer networks for the purpose of causing difficulties in tracing and attribution. Hence, the questions remain as to which *locus* should be considered as the place of actual cyber hostilities and to what extent the *loci*

[48] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* (Jurisdiction) ICTY (2 October 1995) para 70.

relevant to a cyber armed conflict should be regarded as the places where the LOAC is applicable.

Contemporary armed conflicts which are challenging in terms of geography of LOAC would be TAC (or extraterritorial armed conflict) and cyber armed conflict in that both types of armed conflicts feature deterritorialised characteristics not being fully covered by the existing rules of LOAC relating to geography. Deterritorialisation herein refers to 'without any regard to territorial boundaries' that may be global or regional in scope.

TAC refers to the situation in which a state directly uses force against non-state actors, such as terrorists or terrorist groups, located in other states' territory. According to the development of military technologies, such as drones, a state has found a way to selectively target terrorists, who need to be eliminated for its military and strategic purpose, outside its territory. In other words, extraterritorial military operations against non-state actors has become plausible and feasible on the basis of military necessity due to the development of military technologies. Differentiated from the traditional form of NIAC that is originated within one country's territory and later crosses borders (spill-over NIAC), this type of armed conflict between a state and an organised armed group has caused controversy about whether a new category of armed conflict is required for classifying this. Since the positive rules for this use of forces are not fully adaptive, it could be contested whether this kind of armed conflict falls within the application of IHL, domestic laws of territorial states, or other laws. In the light of relevant state practice to date, some extraterritorial use of forces was claimed that they had acquired the consent of territorial states and conformed to the

rules of IHL in those military operations.[49] However, there have been some cases that no consent was forthcoming, unclear, or disputed as seen the anti-ISIS coalition in Syria.[50]

Cyber armed conflict has been a concern of states because there are no consents among states about the rules to regulate cyber armed conflict situations and neither the existing LOAC nor territorial boundaries are neatly suited to manage cyber armed conflict situations. Even more concerning, actual situations of cyber armed conflict have not yet occurred, though they are likely to occur in the near future. So in order to apply the rules of IHL, which have been territorially conceptualised, to these deterritorialised armed conflicts, it is little wonder that confusion abounds. In this regard, the classification of cyber armed conflicts can be said to closely relate to the issue of how to conceptualise 'space' in terms of IHL.

---

[49] For instance, the US could legitimately be part of the armed conflict against AQAP (considered being part of Al-Qaeda) in Yemen, after being asked to fight on behalf of the Yemeni government. (Sasha Radin, 'Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflict' 89 International Law Studies 696 733-734) Drone strikes by the US air force against Al-Qaeda in Pakistan in 2004-2005 were at least known as approved by Pakistani government. (Mirza Shahzad Akbar, 'Can Musharraf Save US from Liability for Drone Attacks?' *CNN* (10 May 2013) <https://edition.cnn.com/2013/05/10/opinion/pakistan-musharraf-drones/index.html> accessed 5 August 2018; Jon Boone and Peter Beaumont, 'Pervez Musharraf admits permitting 'a few' US drone strikes in Pakistan' *The Guardian* (12 April 2013) <https://www.theguardian.com/world/2013/apr/12/musharraf-admits-permitting-drone-strikes> accessed 5 August 2018); Precisely speaking, whether or not the territorial state consents to the use of force against non-state actors in its territory is subject to the legality or legitimacy of use of force, that is, *jus ad bellum*, not an issue of *jus in bello*.

'Consent may be granted for carrying out self-defence operations, conducting operations in association with a non-international armed conflict, or assisting the territorial state in its own non-international armed conflict. Since the legal basis of the state's presence is consent, the activities of its forces are limited to the scope of that consent.'(Michael N. Schmitt, 'Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law' 52 Columbia Journal of Transnational Law 77 82-83); Terry D. Gill, 'Military Intervention at the Invitation of a Government' in Terry D. Gill and Dieter Fleck (eds), *The Handbook of the International Law of Military Operations* (OUP 2010) 229-232.

[50] Terry D. Gill, 'Classifying the Conflict in Syria' 92 International Law Studies 353 371.

It should be simultaneously noted that reconsideration for new phenomena of armed conflict does not necessarily equate with destructing of the existing LOAC.[51] Rather, limitation of territorialised reasoning in confirming the scope of armed conflict in the existing LOAC could be the result of the lack of positive rules and insufficient state practice in actual incidents. Since the discourse about TAC has been more developed in both state practice and literatures compared to cyber armed conflict, it is helpful to first examine the discussion around TAC in the kinetic context. As mentioned in the introduction, there is no reason to differentiate the categories of an armed conflict between kinetic and cyber space. Thus, for TAC to be recognised as a new category, the argument also needs to be applicable to cyber armed conflicts.

III. Transnational Armed Conflict: A New Type of Armed Conflict?

There is an opinion in relation to classification that believes TAC, which has these days prominently taken place, should be added as a new third type of armed conflict.[52] All the issues of TAC are not necessarily required to be addressed in this section. The TAC argument concerning geography (or territoriality) in relation to the classification of kinetic armed conflicts would be selectively examined for the purpose of examining whether this argument could be analogically applied to cyber armed conflicts.

[51] Arimatsu, 'Spatial Conceptions of the Law of Armed Conflict'; Louise Arimatsu, 'Classifying Cyber Warfare' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

[52] Schöndorf, 'Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?' 3.

1. Applicable Laws

There are positive rules relating geography in NIAC such as article 3 common to the Geneva Conventions and the AP II. Under the common article 3, the Geneva Conventions apply to the cases of 'armed conflict not of an international character occurring in the territory of one of the High Contracting Parties'.[53] Common article 3 was designed to cover the classic civil wars occurring within one state's territory between its government and dissident armed group(s); however, this approach would not be sustained.[54] As supported by the commentaries of International Committee of the Red Cross (ICRC), 'the article should be applied as widely as possible.'[55] So the question then arises as to whether this phrase means that a NIAC taking place in two or more state territories fall outside the scope of common article 3. One opinion is that the phrase of 'in the territory of one of the High Contracting Parties' takes a role of confinement to those conflicts that take place within the territorial boundaries of a single state.[56] According to this view, an armed conflict that crosses a border would in general qualify as an IAC, irrespective of the actors concerned. Alternatively, it could be interpreted as a simple reminder that recalls the concerned conflict generally occurs within the territorial jurisdiction of a member state. That is to say, a reference to the territory of any of the contracting parties is sufficient to apply common article 3.

[53] Geneva Conventions I-IV, art 3

[54] Dietrich Schindler, 'The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols' 163 RCADI 125 145.

[55] Jean S. Pictet (ed) *Commentary I the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Aremd Forces in the Field* (ICRC 1952) 50.

[56] Lindsay Moir, 'The Concept of Non-International Armed Conflict' in Andrew Clapham, Paola Gaeta and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015) 400-403; Sandesh Sivakumaran, 'The Addressees of Commom Article 3' in Andrew Clapham, Paola Gaeta and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015); Michael N. Schmitt, 'Charting the Legal Geography of Non-International Armed Conflict' 52 Military Law and the Law of War Review 93.

The phrase imposes no territorial limitation in so far as at least one concerned state is a party to the Geneva Conventions.

If the latter position is taken, it is understood that the phrase was included within the provision in order to make it clear that common article 3 is only applicable in connection with the territory of states that have ratified the Geneva Conventions. The latter view has acquired broader support rather than the former view.[57] Even if taking the former view, the result would not be that different in reality, since the Geneva Conventions have achieved global recognition with 196 state parties[58] (virtually any territory would be that of a high contracting party).[59] Under the current conditions, the common article 3 has clearly been accepted as customary international law, the application of the provision is not even limited to the high contracting parties. Therefore, with regards to NIACs pertaining to the common article 3, the territorial issue has little of contention. So, 'if cyber attacks are undertaken during a NIAC from outside the territory of the state, that fact alone will not cause the conflict to be international in character.'[60]

---

[57] Moir, 'The Concept of Non-International Armed Conflict' 400-403; Schmitt, 'Charting the Legal Geography of Non-International Armed Conflict'.

[58] ICRC, Treaties, States Parties and Commentaries, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949 <https://www.icrc.org/applic/ihl/ihl.nsf/INTRO/365?OpenDocument> accessed 2 May 2018; ICRC, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949 <https://www.icrc.org/applic/ihl/ihl.nsf/INTRO/375?OpenDocument> accessed 2 May 2018; ICRC, Treaties, States Parties and Commentaries, Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949 <https://www.icrc.org/applic/ihl/ihl.nsf/INTRO/380> accessed 2 May 2018.

[59] Noam Lubell, 'The War (?) against Al-Qaeda' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 435.

[60] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 386. (In addition, 'it must also be borne in mind that the transit of data through cyber infrastructure located outside a state in which a non-international armed conflict is occurring does not render the conflict international.')

AP II applies to NIACs 'which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organised armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol'.[61] The additional territorial criterion only stipulated in the AP II could be interpreted in two ways. First, it may be broadly perceived that even temporary control of geographically limited area would suffice to justify the application of the AP II. In that case, despite the foregoing different scope of application to NIACs between the common article 3 and the AP II, the latter NIAC comes close to the former one. On the other hand, if article 1(1) of the AP II is strictly interpreted, the concerned NIACs are restricted to armed conflicts in which organised armed groups exercise almost identical control to that of a state, and the nature of the concerned conflicts could thus be nearly identical to that of IACs.[62]

About this territorial control, the ICRC takes the following position in the commentary on the APs:

> In many conflicts there is considerable movement on the theatre of hostilities; it often happens that territorial control changes hands rapidly. Sometimes domination of a territory will be relative, for example, when urban centres remain in government hands while rural area escape their authority. In practical terms, if the insurgent armed groups are organised in accordance with the requirements of the Protocol, the extent of

[61] Additional Protocol II, art 1(1)

[62] Lindsay Moir, *The law of internal armed conflict* (CUP 2002) 106.

territory they can claim to control will be that which escapes the control of the government armed forces.[63]

This would also suggest that 'some degree of stability' is a critical aspect for them to be capable of effectively applying the rules of the Protocol.[64]

The *Akayesu* Trial Judgement in the International Criminal Tribunal for Rwanda (ICTR) held that the armed forces opposing government 'must be able to dominate a sufficient part of the territory so as to maintain sustained and concerted military operations and to apply AP II. In essence, the operations must be continuous and planned. The territory in their control is usually that which has eluded the control of the government forces'.[65] Considering the object and purpose of AP II to expand the application of IHL to NIACs, the territorial control requirement hence does not need to be strictly interpreted.[66]

About the normative relationship between the common article 3 and the AP II, it should be borne in mind that this instrument expands and supplements the common article 3, but that it does not change its conditions of application.[67] Due to the additional territorial control requirement of the AP, a conflict may fall within the material field of application of the common article 3 without fulfilling the conditions

[63] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC / Martinus Nijhoff 1987) para 4467.

[64] Ibid.

[65] *The Prosecutor v. Jean-Paul Akayesu* (Judgement) ICTR-96-4-T, T Ch I (2 September 1998) para 626.

[66] Yoram Dinstein, *Non-International Armed Conflicts in International Law* (CUP 2014) 137. ('AP II looks like a condensed version of the substance of AP I jointly formulated in 1977.')

[67] Additional Protocol II, art 1(1)

determined by the AP II.[68] Alternatively, all the conflicts governed by the AP II simultaneously correspond to the conflicts stipulated by the common article 3. The territorial requirement added in article 1(1) therefore only relates to the field of application of the Protocol and do not extend to the entire law of NIAC. In this way, the AP II, separate from common article 3, was not intended to bring modifications to the scope of article 3 itself, and common article 3 retains an independent existence.[69]

The above-mentioned provisions of international instruments to NIAC are not textually applicable to a spill-over NIAC and extraterritorial military operations against non-state actors outside of a specific territory.[70] The spill-over NIAC that an internal armed conflict in a state's territory spreads or transfers into other states' territory is not internationalised only based on the fact that it crossed the border,[71] whereas there is another opinion that the concerned armed conflict becomes internationalised.[72] Common article 3 seems applicable whereas the application of AP II would depend on respective details of the concerned internal armed conflict. This situation of extraterritorial armed conflict is neither an IAC enshrined in article 2 common to the Geneva Conventions because an organised armed group is not a state party, nor a NIAC enshrined in article 1(1) of the AP II because it exceeds the

[68] Dieter Fleck, 'The Law of Non-International Armed Conflicts' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (OUP 2008) 620-626; Sandesh Sivakumaran, *The Law of Non-International Armed Conflict* (OUP 2012) 185-187; Dinstein, *Non-International Armed Conflicts in International Law* 136.

[69] Sandoz, Swinarski and Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* para 4454.

[70] Jelena Pejic, 'The Protective Scope of Common Article 3: More than Meets the Eye' 93 IRRC 189 194-198.

[71] Ibid 195; Milanovic, 'The Applicability of the Conventions to 'Transnational' and 'Mixed' Conflicts' 40-41; Hoffmann, 'Squaring The Circle? International Humanitarian Law And Transnational Armed Conflicts' 240-241.

[72] *The Public Committee against Torture in Israel v. The Government of Israel* High Court of Justice, HCJ 769/02 (13 December 2006) (*Targeted Killings* case); More details will be examined at the following section.

territory of one state. Put in the context of non-international cyber armed conflict, the question arises as to whether the territorial control requirement is still meaningful for the AP II to be applied or if the common article 3 only is applicable. Otherwise, a new type of TAC is also arguable to encompass both extraterritorial use of force against an organised armed group and non-international cyber armed conflicts.

2. Extraterritorial Military Operations and Its Implications

After 11 September, the so-called 'war on terror' operations ignited controversies surrounding extraterritorial armed conflict.[73] Hostilities between a state and an organised armed group located in the territory of another state – such as the airstrikes by the US and allies against Islamic States (IS) in Iraq and Syria – have been continuously occurring and challenging to the existing framework of classification of an armed conflict. When a state takes military operations against non-state armed groups, such as terrorist, rebellious, or dissident groups located in other states' territory (even non-neighbouring), but the territorial state where those non-state actors exist does not involve itself in the concerned conflict, how to classify the concerned armed conflict becomes more problematic.

The ICJ has dealt with this question in *Nicaragua*[74] and *Armed Activities in the Congo*,[75] not to mention so much state practice in relation to the extraterritorial use of

[73] Dinstein uses the concept of 'extraterritorial law enforcement' refers to 'the phenomenon of recourse in self-defence to non-consensual cross-border counter-force against hostile organised armed groups within a foreign state'. (Yoram Dinstein, *War, Aggression and Self-Defence* (6th edn, CUP 2017) 293-294) Dinstein argues that such action is legitimate if it is in response to an armed attack unleashed by a non-state actor from the other state's territory and if that state is unwilling or unable to prevent repetition of that armed attack. (ibid 288-299)

[74] *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14.

force against non-state actors. Recent examples include the use of force by Israel in Lebanon in 2006,[76] Uganda, Rwanda and Democratic Republic of the Congo case,[77] Columbia attacks on the FARC in Ecuador in 2008,[78] and US targeting of persons connected with Al–Qaeda in Yemen,[79] Somalia,[80] and Pakistan[81]. In similar situations, it is also possible that despite the use of force by a state against non-state armed groups, the degree of violence does not reach the threshold of an armed conflict.[82] Once it reaches the level of an armed conflict, it is problematic how the distinction of between IAC and NIAC would apply to these transnational conflicts at the very first

---

[75] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Judgement) [2005] ICJ Rep 168.

[76] Human Rights Council, *Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1* (UNGA 23 November 2006); Iain Scobbie, 'Lebanon 2006' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 387-420.

[77] United Nations Human Rights Office of the High Commissioner, *Report of the Mapping Exercise documenting the most serious violations of human rights and international humanitarian law committed within the territory of the Democratic Republic of the Congo between March 1993 and June 2003* (August 2010); Louise Arimatsu, 'The Democratic Republic of the Congo 1993-2010' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 146-202; The ICJ, in the *Armed Activities in DRC* case, states that 'the obligations arising under the principles of non-use of force and non-intervention were violated by Uganda even if the objectives of Uganda were not to overthrow President Kabila, and were directed to securing towns and airports for reason of its perceived security needs, and in support of the parallel activity of those engaged in civil war.' (*Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*) para 163) In conclusion, the Court applied the law of international armed conflicts to the activities of Uganda in the DRC and even to acts of Uganda outside the province of *Ituri*, which was held to have been under Ugandan occupation.

[78] Felicity Szesnat and Annie R. Bird, 'Colombia' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 203-241; Dapo Akande, 'Classification of Armed Conflicts: Relevant Legal Concepts' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 74.

[79] Scott Shane, Mark Mazzetti and Robert F. Worth, 'Secret Assault on Terrorism Widen on Two Continents' *The New York Times* (14 August 2010) <http://www.nytimes.com/2010/08/15/world/15shadowwar.html?pagewanted=all&_r=0> accessed 5 August 2014; Lubell, 'The War (?) against Al-Qaeda' 423-424.

[80] Karen De Young, 'U.S. Strike in Somalia Targets Al-Qaeda Figure' *The Washington Post* (9 January 2007) <http://www.nytimes.com/2010/08/15/world/15shadowwar.html?pagewanted=all&_r=0> accessed 5 August 2014; Lubell, 'The War (?) against Al-Qaeda'421-454.

[81] David Ignatius, 'A Quiet Deal with Pakistan' *The Washington Post* (4 November 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2008/11/03/AR2008110302638.html> accessed 10 November 2014; Lubell, 'The War (?) against Al-Qaeda'.

[82] *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*; Human Rights Council, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston - Study on targeted killings* (A/HRC/14/24/Add.6 28 May 2010) para 52-53.

stage:[83] 'classification of hostilities which occur over multiple territories not even sharing a border raises the difficulty of whether they can be said to be part of a single conflict.'[84] States have to characterise extraterritorial armed conflict so that the authorities of war can apply the IHL rules to the concerned armed conflict.[85] The fact that we are faced with new style of hostilities, which did not exist when the basic instruments of IHL were created, gives us reason to reconsider the existing framework of characterisation.[86] In addition, military operations are no longer limited to the kinetic theatre of war. In cyberspace, cross-border and extraterritorial armed conflict situations ordinarily occur by its borderless nature.

There are two schools of thought about whether a new category of TAC is required. The more traditional approach asserts that the basic structure of international and non-international armed conflict is still valid. Therefore, extraterritorial armed conflicts between a state and non-state armed groups should fall within the existing

[83] In taking an analogical approach from the extraterritorial military operation against non-state actors, it should be noted that the main extraterritorial operations carried out are targeting (direct killing) and detaining. This seems to partly originate from the factual limit that it is in effect impossible to execute overall counter-terrorist operations (similar with the concept of total war) in the territories of other sovereign states without their consent. However, by dragging out for the purpose of national security and from the strategically considered needs, selective targeting having an effect of minimising collateral damages could be regarded as a realistically optimal choice. To satisfy the military and security necessity, on the other hand, the operational authority has to prepare the legal basis of targeting not to violate the LOAC. Some commentators express this sort of so-called 'war everywhere' (resulting from targeted killing) as an extrajudicial killing. Herein, the term 'extrajudicial' seems to imply that this kind of targeted killing in and of itself is not yet legal.

[84] Lubell, 'The War (?) against Al-Qaeda' 451; With respect to the phrase of 'part of a single conflict' in here, for example, 'where the conflict between the foreign state and the non-state group is inextricably bound up with another conflict (notably a conflict between two states) such that acts under the two conflicts (to the extent the conflicts can be distinguished) cannot be separated, the participants will, in reality, be bound to observe the law of international armed conflicts.' (Akande, 'Classification of Armed Conflicts: Relevant Legal Concepts' 72-73)

[85] Geoffrey Corn and Eric Talbot Jensen, 'Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations' 42 Israel Law Review 46 58; Human Rights Council, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston - Study on targeted killings* para 46-48.

[86] Schöndorf, 'Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?' 10; Human Rights Council, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston - Study on targeted killings* para 52-56.

classification frame. A majority of those taking this stance seems to take the position that these conflicts would be NIACs. The other position is that the existing binary armed conflict framework is underinclusive, failing to address the situations of armed hostilities falling outside of its scope,[87] stressing that more incidents which do not suit the existing classification structure appear as time and technology progress. There have also been suggestions of new methods of classification to better suit current conflicts. Thus, these new phenomena have been termed TAC, 'to represent the extraterritorial application of military combat power by the regular armed forces of a state against a transnational non-state armed enemy.'[88] This argument contends that IHL ought to admit that as a new type of armed conflict positing that 'an extraterritorial non-inter-state combat operation launched by a state using regular armed forces could qualify as an armed conflict triggering law of war regulation. Such an operation would fail to satisfy the requisite 'dispute between states' necessary to qualify as an IAC within the meaning of common article 2. However, based on the traditional understanding of NIAC – the definition shared by virtually all scholars and practitioners prior to 11 September – the possibility that an armed conflict falling somewhere between an internal armed conflict and an inter-state, state-armed conflict should theoretically be subject to the regulatory effect of the laws of war was necessarily excluded. Accordingly, these TACs fell into a regulatory gap that necessitated the application of regulation by policy mandate.'[89]

---

[87] Geoffrey S. Corn, 'Geography of Armed Conflict: Why it is a Mistake to Fish for the Red Herring' 89 International Law Studies 77 78.

[88] Geoffrey S. Corn, 'Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict' 40 Vanderbilt Journal of Transnational Law 295 299-300.

[89] Ibid 309; Schöndorf, 'Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?' 7 ('Instead of forcing extra-state armed conflicts into a normative framework that was not designed to fit their unique characteristics, this article proposes the conceptualisation of extra-state armed conflicts as a separate category of armed conflicts.')

This approach has not gained much support from the scholars who want to sustain more traditional shape of IHL as it currently exists.[90] There are several reasons to reject this argument. First, it calls into question whether we are confronted with fully new situations:[91] 'states acting extraterritorially against non-state actors is not a new phenomenon and has occurred in the context of spill-over conflicts, or in assistance of other governments.'[92] Second, it is uncertain why the current framework does not suit an extraterritorial armed conflict in the legal sense.[93] There are several phased steps for the existing law to respond to new cases or phenomena before creating a new law. Even if any positive provisions are not entirely applicable to new incidents, this itself does not directly lead to the necessity of creating a new law. Instead, several steps could precede this, such as the resort to whether or not customary laws exist, the interpretational approach to positive rules and other soft laws, and the analogical approach based on the existing ruling system. By contrast, the argument of newly labelling 'TAC' seems to jump to the last stage without sufficient justification in its reasoning. The logic used by Corn could be said to excessively lean towards policy-making, strategic, and even teleological approach.[94] From a pessimistic outlook, this could be seen as intentionally constructing logic in favour of the military strategy and foreign policy of the US, which is the most powerful and advanced country in military capabilities, to free it from the existing legal restraints and gain more discretion by means of arguing legal *lacuna* where none exist.

---

[90] Corn and Jensen, 'Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations' 50; Kreß, 'Some Reflections on the International Legal Framework Governing Transnational Armed Conflcits'.

[91] Lubell, 'The War (?) against Al-Qaeda' 439.

[92] Ibid; *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*

[93] Lubell, 'The War (?) against Al-Qaeda' 439-440.

[94] Corn, 'Geography of Armed Conflict: Why it is a Mistake to Fish for the Red Herring' 77-107.

There is another distinct position that the determination of law applicable to transnational conflicts between a state and non-state armed groups would depend on whether the territorial state on which the non-state armed groups are based has given consent to the foreign state using force against those groups.[95] Of course, regardless of the existence of a territorial state's consent, in case that the non-state group belongs to or acts on behalf of a state (other than the intervening state), a conflict between that non-state group and the intervening state could become an IAC, since the actions of the non-state group are attributable to the state and so hostilities between the states follows. According to this opinion, if the Lebanese authorities had consented to Israel's military operations against Hezbollah on its territory, the conflict would have regarded as a NIAC. However, it is doubtful that the consent of territorial state could be a critical aspect in determining the legal character of the concerned armed conflict. Rather, it is the issue of *jus ad bellum*, referring to the legality and legitimacy of extraterritorial use of force not the classification itself of *jus in bello*.[96]

There is an argument that the cross-border component of armed conflicts between state armed forces and transnational armed groups operating in the territory of another state without the latter's consent could be treated as an IAC.[97] The argument that an IAC exists where a state uses force against a non-state armed group on the territory of another state without the consent of the latter state was confirmed by the UN

[95] Akande, 'Classification of Armed Conflicts: Relevant Legal Concepts' 73; Dieter Fleck (ed) *The Handbook of International Humanitarian Law* (3rd edn, OUP 2013) 584-585.

[96] About the relationship of the consent of territorial state and classification, Gill, 'Classifying the Conflict in Syria' 366-373.

[97] Paulus and Vashakmadze, 'Asymmetrical War and the Nothing of Armed Conflict - A Tentative Conceptualization' 112.

Commission of Inquiry into the conflict in Lebanon in 2006.[98] The Commission pointed out that 'hostilities were, in fact, only between the Israel Defence Forces (IDF) and Hezbollah. However, the fact that the Lebanese Armed Forces did not take an active part in them neither denies the character of the conflict as a legally cognisable IAC, nor does it negate that Israel, Lebanon, and Hezbollah were parties to it.'[99] Both Israel and Lebanon had the view that the conflict was international despite the fact that Israel first targeted Hezbollah and Lebanese armed forces were not involved in that conflict.[100] In the *Targeted Killing* case, the Israel Supreme Court also took the similar position that 'this law applies in any case of an armed conflict of international character – in other words, one that crosses the borders of the state – whether or not the place in which the armed conflict occurs is subject to belligerent occupation.'[101]

Despite the cross-border aspect, it is more convincing to identify the conflict between Israel and Hezbollah as a NIAC unless a certain level of connection (or attribution) between Hezbollah and Lebanese armed forces would be proven.[102] Even if there had been some clashes between Israel and Lebanese armed forces, it should have been considered separately from the conflict between Israel and Hezbollah. It also seems to be the result of misunderstanding as to whether the territorial state expressed its consent to military operations of the intervening state against non-state armed groups should be taken into account when characterising the concerned armed conflict. The existence of consent of a territorial state would be the matter of legality of

[98] Human Rights Council, *Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1* (A/HRC/3/2 23 November 2006) para 50-62.

[99] Ibid para 55.

[100] Ibid para 56-62.

[101] *The Public Committee against Torture in Israel v. The Government of Israel* para 18.

[102] Scobbie, 'Lebanon 2006' 409; Hoffmann, 'Squaring The Circle? International Humanitarian Law And Transnational Armed Conflicts' 240-241.

extraterritorial use of force by the intervening state (*jus ad bellum*), not the matter of classification in *jus in bello*.[103] Classification of the concerned conflict in order to determine applicable rules of the LOAC must be a part of *jus in bello*. Even though the Israeli military operations against Hezbollah located on the territory of Lebanon without Lebanon's consent could result in large-scale destruction or collateral injury and death of Lebanese people, this is linked to the legality and legitimacy (including the proportionality and the principle of distinction) for the use of force conducted by Israeli armed forces rather than the legal character of conflict itself.

Put another way, the geographical aspect should not be considered when we assess the concerned armed conflict as international or non-international. According to Bassiouni, the 'fact that, historically, such conflicts were confined to the territory of a given state does not alter the legal status of the participants in that conflict and the IHL applicable to them. The LOAC are not geographically bound.'[104] In sum, the order of, first, examining whether the violence between a state and non-state groups is an armed conflict, and second, deciding whether that armed conflict is international or non-international, is still valid in characterising extraterritorial armed conflicts. Thus, it may be a NIAC as long as a state uses its armed forces solely against non-state armed groups, and not against the territorial state in which those transnational armed groups located.[105] In the *Hamdan* judgment, the US Supreme Court concluded that the nature and applicable laws of armed conflict between a state and non-state actors that go beyond the territory of the state is not of an international character, which is

[103] Whether a state is eligible to directly target non-state actors outside territory should depend on *jus ad bellum* theories such as the 'unwilling or unable' test.

[104] M. Cherif Bassiouni, 'Legal Control of International Terrorism: A policy-Oriented Assessment' 43 Harvard International Law Journal 83 99.

[105] The issues surrounding the principle of non-intervention and the prohibition of use of force are different dimension from classification itself.

governed by common article 3 of the Geneva Conventions.[106] That is to say, the critical aspect for determining the applicability of LOAC obligations was whether the US was engaged in an armed conflict against Al–Qaeda, and not the geographic scope of the conflict.[107]

It is uncertain whether there is customary international law covering extraterritorial use of force against non-state entities. Otherwise, one might argue that TAC is on the way to customary international law but in order for TAC to be recognised as a new law, it must follow certain stages. As a *lex ferenda*, there must be state practice to be recognised as a deemed-to-be law. It should be ascertained where TAC is situated on the process of law development, whether it is on the stage of accumulating state practice or of gaining *opinion juris*. To date, there seems neither consistent state practice nor *opinio juris* to confirm the customary rule regulating it.[108]

In addition, if TAC, as argued, is required as a new third category of armed conflicts in IHL, it would be necessary afterwards to identify which set of IHL rules are

[106] *Hamdan v. Rumsfeld, Secretary of Defense et al.* US Supreme Court 548 U.S. 557, 126 S.Ct. 2749 (29 June 2006)

[107] (Nonetheless, 'the Court left unresolved whether the conflict with Al-Qaeda is part of an inter-state armed conflict, an intra-state armed conflict, or perhaps a third novel category of armed conflicts. The legal regime applicable to the conflict with Al-Qaeda also remains partially open. The Court concluded only that common article 3 applies, *as a minimum*, to this conflict.') Eran Shamir-Borer, 'Revisiting Hamdan v. Rumsfeld's Analysis of the Laws of Armed Conflict' 21 Emory International Law Review 601 618; Geoffrey S. Corn and Eric Talbot Jensen, 'Untying the Gordian Knot: A Proposal for Determining Applicability of the Laws of War to the War on Terror' 81 Temple Law Review 787; Corn, 'Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict'.

[108] Paulus and Vashakmadze, 'Asymmetrical War and the Nothing of Armed Conflict - A Tentative Conceptualization' 112.

applicable to TAC. The question may also arise as to what the practical difference and benefit is in distinguishing TAC from NIAC and IAC.[109]

In conclusion, the author suggests that extraterritorial kinetic armed conflicts should be characterised as NIAC because geographical aspect is merely subsidiary, not essential, in classification. It is not necessary to admit the distinctive concept of TAC in order to apply IHL to a situation in which a state extraterritorially uses force against non-state transnational armed groups crossing borders of more than two countries. Furthermore, the non-geographical approach seems to have considerable implication for the characterisation of cyber armed conflicts having a borderless character, even if it can be, at best, said that the formation of customary norms governing extraterritorial armed conflicts is under way and not yet completed.[110]

3. Classification of Internal Cyber Armed Conflict

The question as to whether TAC is necessary as a new category of classification could be more conclusively answered after considering its suitability to cyber armed conflicts. Cyberspace is fundamentally not a real dimension but a virtual one, except for cyber infrastructure physically located on states' territories. For the purpose of regulating cyber space in the legal sense, the detailed characteristics of cyberspace need to be considered. As a new category of armed conflict, TAC requires far less for a cyber armed conflict since geographical scope or proximity of cyber attacks have little impact on characterising a cyber armed conflict.

---

[109] Human Rights Council, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston - Study on targeted killings* para 48-49.

[110] Schöndorf, 'Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?' 76.

International courts have asserted that the application of LOAC is not limited to the actual scope of internal armed conflict.[111] The international group of experts for the *Tallinn Manual 2.0*, moreover, agreed that 'the LOAC applies to activities conducted in the context of the conflict that occur outside the state in question.'[112] This is particularly important in that cyber activities, in furtherance of a NIAC, may well be launched remotely, far from conventional hostilities, to avoid the physical trace of accusation of the authorities in the concerned territory.[113] It is more enticing for the non-state attackers to leave the territory in question and to route cyber attacks in a complicated manner, since there are various differences amongst states in their capacity to assert power over cyberspace. Some states have more developed cyber network and well-structured regulations for it whereas others only have a basic level of cyber infrastructure, less technological capability, and ill-structured regulations, which results in a sort of breeding ground for base camps of non-state cyber attackers to conduct more freely and actively. Even in this situation, states with comparatively advanced cyber environments cannot assure an effective defence and corresponding law enforcement against those cyber attacks: 'the information obstacle thus affects the ability to reach a definitive analysis of classification.'[114]

This lack of information within the cyber context is further intensified in both time and manner (means and methods). For the proper counter cyber operation to be taken, the tracing and identification of the original cyber attack should be completed first. If

[111] *Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* para 70.

[112] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 386.

[113] Ibid 386-387.

[114] Lubell, 'The War (?) against Al-Qaeda' 451.

missing a decent window of opportunity for a counterattack, the whole counter operation might be contrary to the principles of IHL such as military necessity, proportionality, and humanitarian consideration. On the other hand, when it comes to ways to gather sufficient information, technical proof issues (not legal reasoning) matter most.

Considering all the specific characteristics of cyber conflicts, and if we accept the concept of TAC as self-standing, a majority of non-international cyber armed conflicts will be classified as TAC. We would then face more chaotic situations in applying IHL to those cyber conflicts in that there has no sufficient consensus about the nature and details of TAC in IHL. In addition, such a method cannot be understood from the perspective of international law development, in that the argument of TAC is driven more by policy-and-strategy orientation, not by a sequential chain of legal reasoning.

Nonetheless, it still remains open as to whether or not the geographical relevance in a non-international cyber armed conflict can be completely ignored. Regarding this issue, the international group of experts for the *Tallinn Manual* 2.0 acknowledged 'the existence of a narrower approach that accepts the possibility of a NIAC which crosses borders, but that imposes a requirement of geographical proximity to the state involved in the conflict.'[115] However, the Manual does not go further beyond the level of introduction of divided opinions. With respect to the geographical issues of cyber armed conflicts, the *Tallinn Manual* 2.0 seems to take passive stance to provide new

[115] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 387.

legal interpretations or to suggest new political solutions.[116] The manual repeats most of the existent rules regarding geography of armed conflicts but does not provide any answers about extraterritorial operations against non-state actors.

In regard to the focus of classification, the cyber conflict between a state and non-state armed groups may be identified and interpreted within the frame of a NIAC, regardless of extraterritoriality or transnationality. Under the LOAC, the division of IAC and NIAC is first based on the criteria of 'actor' and 'intensity'. Geography as an additional factor is only partly found in treaty law as afore-mentioned. Only if a concrete connection to a state which successfully establishes 'attributability' is proven, those cyber confrontation would be internationalised. Under the significantly changed cyber circumstances, it seems more necessary to focus on the criteria of actors rather than geography in cyber conflicts. Considering the characteristics of modern technology in war, the limitation of spatial and geographical scope has little meaning. Giving excessive weight to territoriality factors could bring about the result that most of cyber conflicts would be qualified as either an international cyber armed conflict or a transnational cyber armed conflict. It currently seems better to choose a NIAC framework to respond to the likely occurring cyber clashes between a state and non-state armed groups, located in and outside of the concerned state's territory. Rather, it is more important to clarify the fundamental criteria of 'actor' and 'intensity' in order to confirm the existence of a non-international cyber armed conflict. But this stance does not strictly deny any possibility of overall change in the LOAC system in the future.

[116] Ibid 378-380 and 386-387.

4. Geography in Non-International Cyber Armed Conflict

The LOAC applies to all hostilities conducted in the course of the armed conflict, and all associated effects, wherever they occur in or outside of the territory of the state involved in a non-international cyber armed conflict.[117]

There is the concept of 'zone of hostilities' (or 'zone of combat') to expand the geographical scope of armed conflicts. This begins with military necessity of a state to eliminate non-state fighters, who have undertaken hostilities in other states' territories, against that state in terms of targeting. This concept means that the factual geography of an armed conflict equates to its legal geography for which the LOAC applies.[118] The concept of zone of hostilities in and of itself is neutral that can cover both international and non-international armed conflicts.

The political rhetoric of 'war on terror' has a problem that terrorist groups and individual operatives are dispersed and can carry out their tasks, such as training members, setting substructures, raising funding, and conducting concrete attacks. The demand to respond extraterritorially against these non-state actors comes to the foreground in terms of policy. The US and other Western authorities insist on *political* geography of an armed conflict since the actors located in other states' territories actually execute attacks or indispensable works to carry out hostilities. They argue that the 'battlefield' should be expanded up to those territories on which

[117] Ibid 386.

[118] Three distinguishable dimensions of 'geography' in an armed conflict was addressed earlier in this chapter.

the enemies are based.[119] This need, from the perspective of policy-making, leads to the attempt to expand the *legal* geography of the armed conflict in question. Some have started to argue that the geographical scope of an extraterritorial armed conflict can reach the territory of host states in which organised armed groups or their members stay in order to justify expanding the scope of targeting to the extent where important enemy figures are located.[120]

The major purpose in considering geography of an extraterritorial armed conflict is to provide humanitarian protection with non-state actors and other civilians established in LOAC, not to serve state interests.[121] In this regard, it can be said that IHL applies to wherever actual hostilities exist. However, the purpose of zone of hostilities logically reverses this implication of geography of an armed conflict. Before actual hostilities take place in the territory of host state in question, it is assumed that the concerned armed conflict already exists in that area in order to take military operational advantages of targeting. It cannot be accepted as the legal base of targeting because it is an inverted legal logic which relies on a teleological approach. In the case of an extraterritorial use of force against non-state actors, *legal* geography of an armed conflict can be drawn based on the *factual* geography of the concerned armed conflict, which is formed after actual hostilities between the parties occurred.

---

[119] Jennifer C. Daskal, 'The Geography of the Battlefield: A Framework for Detention and Targeting outside the "Hot" Conflict Zone' 161 University of Pennsylvania Law Review 1165; Laurie R. Blank, 'Defining the Battlefield in Contemporary Conflict and Counterterrorism: Understanding the Parameters of the Zone of Combat' 39 Georgia Journal of International and Comparative Law 1 20-26; Rosa Ehrenreich Brooks, 'War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror' 153 University of Pennsylvania Law Review 675; As a contrary view, Mary Ellen O'Connell, 'Combatants and the Combat Zone' 43 University of Richimond Law Review 845.

[120] Brooks, 'War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror'.

[121] Jean S. Pictet (ed) *Commentary III the Geneva Convention Relative to the Treatment of Prisoner of War* (ICRC 1960) 23. ('It must not be forgotten that the Conventions have been drawn up first and foremost to protect individuals, and not to serve state interests.')

When put in the cyber context, it becomes more obvious. If the theory of zone of hostilities is analogically applied to non-international cyber armed conflicts, it will bring about substantive effect that *legal* geography of cyber armed conflicts could expand all over the world in the end, even before actual hostilities break out. Even if there would be other legal techniques, such as tests of proportionality or imminence, to bar the implementation of attacks, it is not appropriate and logical to set a zone of hostilities in the legal sense. Targeting non-state actors located in other states' territory should depend on *jus ad bellum* such as the consent of those host states, a Security Council mandate under Chapter VII of the UN Charter,[122] the lawful exercise of the right of self-defence such as 'unwilling or unable' test.[123]

Cyber armed conflict between a state and an organised hacker group should be conclusively classified as non-international cyber armed conflict on the basis of the two fundamental criteria of 'actors' and 'intensity'. Then, the room for the geographical approach to involve in characterisation of armed conflict should be reduced in both kinetic and cyber contexts. In addition, targeting issues of

[122] Gill, 'Military Intervention at the Invitation of a Government' 230-232; Noam Lubell, *Extraterritorial Use of Force against Non-State Actors* (OUP 2010) 29-36; Schmitt, 'Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law' 79-81.

[123] The doctrine of 'unwilling or unable' refers to a state may act in self-defence against non-state actors within another state's territory if the territorial state is either unwilling or unable to take the necessary action against the non-state actors. About the conditions to refer to 'unwilling or unable' test, Deeks suggests '(i) prioritize consent or cooperation with the territorial state over unilateral use of force, (ii) ask the territorial state to address the threat and provide adequate time for the latter to respond, (iii) reasonably assess the territorial state's control and capacity in the relevant region, (iv) reasonably assess the territorial state's proposed means to supress the threat, and (v) evaluate its prior interaction with the territorial state'. (Asheley S. Deeks, '"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense' 52 Virginia Journal of International Law 483); Dawood I. Ahmed, 'Defending Weak States against the "Unwilling or Unable" Doctrine of Self-Defence' 9 Journal of International Law and International Relations 1; Jens David Ohlin, 'The Unwilling or Unable Doctrine Comes to Life' Opino Juris <http://opiniojuris.org/2014/09/23/unwilling-unable-doctrine-comes-life/> accessed 2 November 2018.

extraterritorial use of force must be strictly distinguished from classification, so the theory of 'zone of hostilities' has little relevance with the theme of this thesis.

IV. Conclusions

The key questions examined in this chapter revolve around how international law should develop in order to accommodate those hostilities which possess transboundary characteristics. On this point, it is concluded that the existing bifurcated structure of IAC and NIAC does not need to add the third category of TAC. At the first glance, cyberspace seems to be completely different and novel in applying IHL as it is established on the premise of kinetic space. However, as analysed though this chapter, cyberspace is also the space in which governance of state sovereignty would exist. Then, only the details of its implementation would be different or in question due to the inherent characteristics of cyberspace itself.

Cyber operations may be conducted from, or with effects to, the entire territories of the parties to the conflict, international waters or airspace, and, subject to certain limitations, outer space.[124] Cyber operations that violate the LOAC are prohibited elsewhere. Restrictions based on geographical limitations are particularly difficult to implement in the context of cyber conflict. For example, in the case of a cloud-computing system, data (including malware, programme, or code, etc.) used for the attack from one state can be replicated across a number of servers over other states but is only observably reflected on the systems where the attack is initiated and

[124] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 378.

completed.[125] There is, in principle, no general prohibition on the mere transit of data through areas where the conduct of cyber operations is otherwise prohibited during an armed conflict.[126] That international cyber armed conflict would not be relevant to geographical issues relating to classification regardless of its borderless character. Cyber attacks detouring into third states in an IAC is then related to neutrality not classification. Cyber operations that transit to a third, neutral territory and may have unintended effects should be dealt with in the context of the law of neutrality.

When it comes to classification of non-international cyber armed conflicts, the meaning of geography has to be unavoidably reduced, considering the unique characteristics of cyberspace. Hence, we should concentrate on the original criteria of 'actors' and 'intensity' in characterising cyber armed conflicts. Extraterritorial cyber armed conflict between a state and an organised cyber armed group located in other states' territory must be classified as NIAC, not a special category of TAC.

[125] Ibid 378-379.

[126] Ibid 33-34.

Chapter 6 – Conclusion

I. Introduction

For the last decade, cyber conflicts have occurred widely and frequently all over the world. Accordingly, the ensuing concerns about cyber armed conflicts are also natural and reasonable. Among many problems arising from cyber incidents, the question as to whether stand-alone cyber armed conflicts have the genuine characteristics of warfare is controversial. Even though a cyber armed conflict in terms of international humanitarian law (IHL) has not yet occurred, it does not mean that the preparation for cyber armed conflicts is unnecessary. In this regard, this thesis has aimed to reconsider the existing framework of classification (or characterisation) of IHL for kinetic armed conflicts, and to examine whether these rules are still applicable to cyber armed conflict situations in order to be regulated by IHL.

II. Contributions

1. Cyber Armed Conflicts Will Take Place

There is a debate about whether a stand-alone type of cyber armed conflict will take place in the future. The debate often features interdisciplinary and cross-over theories among international relations and strategy and law. There has not yet been a cyber armed conflict which has escalated to a threshold in which the law of armed conflict (LOAC) would apply. The author anticipates its occurrence and insists on being

prepared for the future cyber armed conflicts in terms of IHL. The thesis is written to contribute to the classification of cyber armed conflicts as the preliminary step to apply the rules of LOAC to cyber armed conflicts.

Thomas Rid suggested that there will not be a cyber war in the future, given that to date no cyber attack on record satisfies all the requirements of an 'act of war' – violent (at least potentially lethal), instrumental, and politically attributed (according to Clausewitz's definiton)[1] – and that far more sophisticated acts of network-enabled sabotage, espionage, and subversion will increase instead of breaking out into a cyber war in the future.[2] He thus predicts cyber attacks will remain auxiliary to an act of war but will not constitute such an act in and of themselves. Similarly, Larry May makes three points in arguing why cyberwar would not take place. First, 'cyber attacks do not cross borders in the way that foreign troops do', as computer network attacks do not bring with them the same concerns associated with armed border crossing. Second, 'because in the launching of a cyber attack there is no intention directly to kill enemy soldiers there is another reason not to extend to cyber attacks the label of war with its corresponding rules allowing for killing but seeking only to render the killing more humane.' Lastly, 'the kind of disruption of services that cyber attacks can achieve is insufficient to count as an act of war.'[3] May instead thinks that a cyber attack is closer to the concept of embargoes.

---

[1] Clausewitz established the three main elements of war: violence, instrumentality, and political intention. A 'war' has a violent character which is always potentially or actually lethal for some participants on at least one side. And an act of war has to take a means to fulfil its political intention. (Carl von Clausewitz, *Vom Kriege* (Ullstein 1832) translated by Michael Howard & Beatrice Heuser, *On War* (OUP 2007)) Rid takes the same viewpoint of Clausewitz about an act of war in his article. (Thomas Rid, 'Cyber War Will Not Take Place!' 35 Journal of Strategic Studies 5)

[2] Thomas Rid, *Cyber War Will Not Take Place* (Hurst 2013)

[3] Larry May, 'The Nature of War and the Idea of "Cyberwar"' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (OUP 2015) 8-9.

However, John Stone convincingly refutes this argument. Stone disagrees with Rid's opinion that a cyber attack cannot be a real act of war due to their lack of violence or potential lethality. War demands no necessary causal connection between the aforementioned three aspects of Clausewitz's definition of war. Therefore, force does not necessarily imply violence, particularly lethality.[4] In addition, Stone points out that 'Clausewitz's definition of war as an act of force does not require that the act be claimed or attributable.'[5] He concludes that the argument of Rid is not realistic in that it requires too much violence to be acceptable in determining what amounts to an act of war.[6] In this analysis, only a few keystrokes could amount to an act of war in some cases.

This debate depends on the nature and character of war itself. Both opinions are worth listening to as strategists' views. While admitting the potential to call for special laws for cyber war, the sceptics have hesitated to accept the concept of cyber attack in terms of IHL and have stuck to the traditional concept of 'just war'.[7] But this sceptical argument seems to take an excessively passive attitude in preparation for potential future cyber conflict development and misunderstands the implication of 'attack'. Stone's view corresponds more closely to the perspective of law: in characterising war (or armed conflict), it is more convincing and effective to regard an act of war as a consequence-based concept. If we consider an act of war as one of lethally violent

[4] John Stone, 'Cyber War Will Take Place!' 36 Journal of Strategic Studies 101 103.

[5] Ibid 105.

[6] Ibid 106.

[7] 'Though cyber attacks do not have to be clandestine, until they are public acts, it is once again hard to see them as instances of war properly. It is hard to imagine a computer virus or worm being successfully used against a foreign computer system if it is acknowledged in advance. Therefore, the prohibition on clandestine warfare that runs throughout the Just War tradition seems not to sit well with the idea of cyberwar.' (May, 'The Nature of War and the Idea of "Cyberwar"' 5)

force using instruments (such as arms) with political intention (or attribution), the scope of an act of war comes to be much too limited and then the application of IHL is also confined. In other words, neither the intention nor the means used to harm objects of a cyber attack are main concerns in determining the existence of a cyber attack from the angle of IHL. Of course, in assessing the consequence of a cyber attack, a causal relationship is considered. However, this does not mean that all the indirect injuries or damages should be excluded from the consequences of cyber attack. Despite Rid's strategic efforts to push cyber attacks beyond the scope of an act of war, it seems inconsistent with the reality of cyber attacks that can bring about substantive violent effects.

Despite this strategy-oriented argument, there is an obvious possibility of cyber armed conflicts and the need for legal preparation to cope with that potential. Law usually follows the development of actual practice. Although we cannot accurately predict the direction in which future cyber conflicts will unfold, it is impossible to deny the fact that cyber conflicts do occur which suggests severe future threats and challenges against national and international security. This also brings about practical fears and tensions between states and non-state actors as well as between states. Routinely utilised cyber attacks (including attacks which are not even meaningful in terms of LOAC but are generally referred to as an attack) can sometimes be characterised as espionage or exploitations but may also sometimes qualify as an 'attack' in terms of IHL.

2. Research Conclusions

In order to analyse the classification of cyber armed conflicts, the thesis takes the same definition of 'armed conflict' suggested by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the *Tadić* case and broadly accepted afterwards.[8] According to the definition, 'actors' and 'intensity' are the main criteria to identify the existence of armed conflict. Coping with increasing-ever cyber incidents to date, how to view the traditional geographical demarcation in IHL in cyberspace is problematic. As already questioned in kinetic armed conflicts, extraterritorial armed conflict situations (for example, drone attack, anti-terrorism operations crossing over the borders) have raised similar issues in classifying whether it should be regarded as an international armed conflict (IAC) or a non-international armed conflict (NIAC), or even the new third type of armed conflict. From the perspective of focusing more on the trans-border character, there is one opinion to regard it as an IAC, whereas from the perspective of focusing on the involved actors, it could be seen as a NIAC. Hence, cyber armed conflicts having a genuine character of borderlessness impose a similar issue on classification. In this regard, geographical issues were separately addressed in Chapter 5.

In order to identify the legal character of cyber confrontation, the indication of actors first needs to be considered. The bifurcated structure of the existing LOAC as IAC and NIAC is still relevant despite the trend of convergence between the two within

[8] 'An armed conflict exists whenever there is a resort to armed force between states or protracted armed violence between governmental authorities and organised armed groups or between such groups within a state.' (*Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction* (Jurisdiction) ICTY (2 October 1995) para 70)

the rules of IHL.[9] Therefore, the criterion of actors is critical in differentiating an IAC from a NIAC at the initial stage of classification of the concerned situation.[10] Chapter 3 of this thesis looks into the changed features and characteristics of actors in cyber conflicts. An IAC can be characterised through identifying at least two states involved as parties to the concerned conflict. In this regard, chapter 3 focuses on how to identify state armed forces and state-affiliated or sponsored actors whose conducts are attributed to the state in cyberspace. There are continuous trends of establishing specialised cyber units in national military service of states and outsourcing some of state's cyber function and resources. States also tend to approach cyber security issues with overall and comprehensive national strategies. In cyberspace, intertwined military and civilian computer network systems or the connection among states' online networks make the tracing and proof required to prove attribution far more difficult. Chapter 3 mainly analyses these actors-centred issues. It is next necessary to examine the issue of whether the 'intensity' criterion matters in classifying an IAC. On the basis of accumulated debates in the context of international kinetic armed conflicts, if two states are engaged in cyber attacks amounting to armed hostilities in or through cyberspace, an international cyber armed conflict would exist regardless of short time or limitation in its scope.

Chapter 4 analyses non-international cyber armed conflicts. In order to identity the existence of a non-international cyber armed conflict, the concrete requirements for being an organised armed group in cyberspace should be established. This is because

[9] Bruce "Ossie" Oswald, 'The Harmonization Project: Improving Compliance with the Law of War in Non-International Armed Conflicts' 53 Columbia Journal of Transnational Law 105; Christine Byron, 'Armed Conflicts: International or Non-International?' 6 Journal of Conflict & Security Law 63 63-66.

[10] In identifying involved actors, the principle of distinction, which must be sustained in the cyber context, aims to protect civilians by distinguishing from combatants or members of organised armed groups.

cyber operations conducted by individuals or by an unorganised group of hackers do not satisfy the prerequisite for the existence of a NIAC, no matter how intense the concerned situation is. In this regard, the status of virtually organised armed groups in cyberspace is important. The formation of a group organised entirely online has to be examined on the basis of objective standards regardless of its intention or purpose to conduct cyber hostilities. Chapter 4 next analyses the intensity assessment of cyber armed conflicts. The intensity criterion, which consists of 'gravity' and 'duration', is more crucial in identifying the existence of NIAC than IAC. The definition of cyber attack as the standard of assessment is examined in chapter 1 as one of the main terms of the thesis, prior to chapter 4 in which intensity measuring of cyber operations is fully considered. It would be illogical to say that the use of cyber means and methods of warfare brings about either a lower or higher intensity bar than currently applied bar to kinetic war operations. As long as one takes consequence-based approach in defining 'attack' and 'cyber attack', there is no reason to apply a different standard in assessing intensity level.[11] In order to distinguish non-international cyber armed conflict from internal cyber disturbances and tensions, the case-by-case approach taken by international courts and tribunals in assessing intensity in kinetic cases seems sustainable. When it comes to cyber attacks, in order for the aggrieved party to determine the timing of countermeasures or counter-attack, they need to determine the temporal scope of the concerned cyber conflict. Depending on the starting point of a cyber attack triggering a cyber armed conflict, the possible reaction of the counterparty could be legally decided. At this point, the unique characteristics of cyber operation such as time-setting malware programme would be considered.

[11] Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' 25 Stanford Law & Policy Review 269 293.

Finally, chapter 5 analyses the geographical issues surrounding cyber armed conflicts and concludes that a de-geographical approach is required for cyber armed conflicts. Chapter 5 distinguishes the contextual meanings of geography (*factual*, *legal*, and *political*) used in press and policy regarding armed conflicts. As extraterritorial armed conflicts have increasingly occurred, there has been an argument that a new third category of 'transnational armed conflict' (TAC) should be supplemented to classification. The argument of TAC in kinetic space also need to be inclusive of cyber armed conflicts in order to be admitted. However, considering borderless character of cyberspace, TAC is hardly acceptable to apply to both kinetic and cyber armed conflicts. Rather, the author argues that classification should focus on the originally fundamental criteria of 'actors' and 'intensity'. It also points out that the factual concept of 'zone of hostilities' in terms of *jus in bello* should be completely separate from the issues of targeting in terms of *jus ad bellum*. The theory of zone of hostilities to justify targeting non-state actors who located in other states' territory is not only illogical but also meaningless in the cyber context because geographical demarcation in cyberspace is highly unlikely. The chapter concludes that geography (or territoriality) has little implication in terms of the classification of cyber armed conflicts.

The rules of classification kinetic armed conflicts have been established by law, judicial reviews, and literature. However, some loopholes have been uncovered that need to be filled by interpretation. The fundamental consistency of classification (using the criteria of 'actors' and 'intensity') in both kinetic and cyber armed conflicts can be sustained within the current IHL frame. This basic concept of classification in both kinetic and cyber space removes the need for a new category of armed conflict

(TAC) which has been argued as a method to adapt to the increasingly extraterritorial military operations against non-state actors. The process of classification of cyber armed conflicts should be simplified with the basic criteria of 'actors' and 'intensity' that require to be elaborately analysed to adapt to cyberspace.

III. Limitation and Future of Cyber Armed Conflicts

The limitation of this research points to the fact that there has not been any actual cyber armed conflict in practice. This lack of state practice can make the research more abstract and hypothetical. This limitation is simultaneously linked to the value of the research in order to prepare for the possible outbreak of cyber armed conflicts in the near future.

To date, international norms, principles, and rules of law regulating cyberspace have not been agreed to in the international community. Since 2004, United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has discussed the international cyber regulation at the global level.[12] After the UN GGE repost of 2015, it was faced with a deadlock when the UN GGE tried to take the process a step further and discuss the application of international law to cyber conflicts in 2017.[13] Some countries, including Russia and China, opposed the mention of international humanitarian law, the law of self-defence, and the right of states to

[12] For the overall progress in UN GGE, see, < https://www.un.org/disarmament/topics/informationsecurity/> accessed 5 October 2018.

[13] Michael Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' *Just Security* 30 June 2017 <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> accessed 31 October 2018.

take countermeasures. They claimed this would lead to the militarisation of cyberspace. As mentioned in chapter 1, Russia and China, along with other countries, have pushed for more regulations to clarify how international law applies to cyberspace with the aim of exercising more sovereignty – and state control – over the internet. However, this attempt has continuously faced opposition from the US, the UK, and other likeminded states on the ground that it would be used by states to justify their domestically repressive policies against the open and free use of internet. From the perspective of Western states, no additional regulations are required.[14] They want to focus on the application of existing rules of international law as the basis for maintaining security and for conflict prevention.[15] 'Cyberspace is not lawless, and international law applies to peace and cyber conflicts.'[16]

The recent revelations of Russian cyber attacks may bring about a more intense impasse in developing common set of international law for cyberspace.[17] Given that Russia has been calling for rules in cyberspace based on UN Charter principles, such as respect for national sovereignty and non-interference in internal affairs, exposing

[14] Attorney General Jeremy Wright QC MP, *Cyber and International Law in the 21st Century* (UK Government 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 5 October 2018.

[15] Joyce Hakmeh, 'Cyberattack Revelations Appear to Undercut Russia's UN Efforts' Chatham House Expert Comment <https://www.chathamhouse.org/expert/comment/cyberattack-revelations-appear-undercut-russia-un?utm_source=Chatham%20House&utm_medium=email&utm_campaign=9929905_CH%20Newsletter%20-%2012.10.2018&utm_content=Russia-CTA&dm_i=1S3M,5WTYP,NUT6YG,N4U8O,1> accessed 10 October 2018.

[16] Ibid; A new version of the *Tallinn Manual* added the rules for cyber operations in peace time. (Michael N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017))

[17] The cyber attacks were carried out against the Organisation for the Prohibition of Chemical Weapons (OPCW), the International Olympic Committee (IOC) and the Canadian Centre for Ethics in Sport, as well as Brazil relating to anti-doping test during the Olympics (Pippa Crerar, Jon Henley and Patrick Wintour, 'Russia Accused of Cyber-Attack on Chemical Weapons Watchdog' The Guardian (4 October 2018) <https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body> accessed 5 October 2018.

its numerous attacks which go against these same principles undermines Russian stance.[18] Other states whose covert hostile cyber operations have not yet been revealed also have to be attentive to this point.

The future of cyber armed conflicts cannot be firmly asserted but can be carefully predicted on the basis of the preceding cyber incidents. As humankind has experienced technological developments, such as submarines and nuclear weapons, in the military arena through history, no one can deny the advent of lethal cyber weapons and the future possibility of cyber armed conflicts. In this regard, keeping an eye on the progress of state practice in the field, the discourse surrounding cyber armed conflicts, especially classification issues, needs to be developed.

[18] 'Coordinated revelations about Russia's behaviour could be part of a negotiation strategy that the UK and its allies are implementing with the aim of challenging Russia's negotiating position, as it tries to lobby other countries to endorse its resolutions. By strategically timing the announcement – it has been almost six months since GRU operators were caught in an attempted hack and signals interception of the Organisation for the Prohibition of Chemical Weapons – the UK, the US and their allies hope to weaken Russia's position in the UN deliberations.' (Hakmeh, 'Cyberattack Revelations Appear to Undercut Russia's UN Efforts')

Bibliography

Article

Akande D, 'Classification of Armed Conflicts: Relevant Legal Concepts' in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)

Arimatsu L, 'The Democratic Republic of the Congo 1993-2010' in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)

——, 'Spatial Conceptions of the Law of Armed Conflict' in Robert P. Barnidge J (ed), *The Liberal Way of War* (Ashgate 2013)

——, 'Classifying Cyber Warfare' in Tsagourias N and Buchan R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015)

Asada M, 'The Concept of "Armed Conflict" in International Armed Conflict' in O'Connell ME (ed), *What Is War?: An Investigation in the Wake of 9/11* (Martinus Nijhoff 2012)

Blank LR, 'Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace' in Ohlin JD, Govern K and Finkelstein C (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015)

Boothby WH, 'The Legal Challenges of New Technologies: An Overview' in Nasu H and McLaughlin R (eds), *New Technologies and the Law of Armed Conflict* (Springer 2014)

Chimni BS, 'Legitimating the International Rule of Law' in Crawford J and Koskenniemi M (eds), *The Cambridge Companion to International Law* (CUP 2012)

Clapham A, 'The Concept of International Armed Conflict' in Clapham A, Gaeta P and Sassòli M (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015)

——, 'Focusing on Armed Non-State Actors' in Clapham A and Gaeta P (eds), *The Oxford Handbook of International Law in Armed Conflict* (OUP 2014)

Crawford J, 'Sovereignty as a Legal Value' in Crawford J and Koskenniemi M (eds), *The Cambridge Companion to International Law* (CUP 2012)

David E, 'Internal (Non-International) Armed Conflict' in Clapham A and Gaeta P (eds), *The Oxford Handbook of International Law In Armed Conflict* (OUP 2014)

Fleck D, 'The Law of Non-International Armed Conflicts' in Fleck D (ed), *The Handbook of International Humanitarian Law* (OUP 2008)

Frowein JA, 'Self-Determination as a Limit to Obligations under International Law' in Tomuschat C (ed), *Modern Law of Self-Determination* (Martinus Nijhoff Publishers 1993)

Gat A, 'The Changing Character of War' in Strachan H and Scheipers S (eds), *The Changing Character of War* (OUP 2011)

Gill TD, 'Military Intervention at the Invitation of a Government' in Gill TD and Fleck D (eds), *The Handbook of the International Law of Military Operations* (OUP 2010)

Hagen A, ‘The Russo-Georgian War 2008’ in Healey J (ed), *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (A CCSA Publication 2013)
Haines S, ‘The Nature of War and the Character of Contemporary Armed Conflict’ in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)
——, ‘The Developing Law of Weapons’ in Clapham A and Gaeta P (eds), *The Oxford Handbook of International Law in Armed Conflict* (OUP 2014)
Hoffmann T, ‘Squaring The Circle? International Humanitarian Law And Transnational Armed Conflicts’ in Académie de Driot International de La Haye (ed), *Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts (Law Books of Academy)* (Brill 2010)
Hollis DB, ‘Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?’ in Ohlin JD, Govern K and Finkelstein C (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (OUP 2015)
Hughes R, ‘Towards a Global Regime for Cyber Warfare’ in Geers CCaK (ed), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009)
Kleffner JK, ‘Scope of Application of International Humanitarian Law’ in Fleck D (ed), *The Handbook of Humanitarian International Law* (3rd edn, OUP 2013)
Lubell N, ‘The War (?) against Al-Qaeda’ in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)
May L, ‘The Nature of War and the Idea of "Cyberwar"’ in Ohlin JD, Govern K and Finkelstein C (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (OUP 2015)
Milanovic M, ‘The Applicability of the Conventions to 'Transnational' and 'Mixed' Conflicts’ in Clapham A, Gaeta P and Sassòli M (eds), *The 1949 Geneva Convnentions: A Commentary* (OUP 2015)
Moir L, ‘The Concept of Non-International Armed Conflict’ in Clapham A, Gaeta P and Sassòli M (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015)
Pejić J, ‘Status of armed conflicts’ in Breau EWS (ed), *Perspectives on the ICRC Study on Customary International Humanitarian Law* (CUP 2007)
Rowe NC, ‘The Attribution of Cyber Warfare’ in Green JA (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015)
Schmitt MN, ‘Classification in Future Conflict’ in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)
Scobbie I, ‘Lebanon 2006’ in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)
Sheldon R and MacReynolds J, ‘Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias’ in Lindsay JR, Cheung TM and Reveron DS (eds), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (OUP 2015)
Sivakumaran S, ‘The Addressees of Commom Article 3’ in Clapham A, Gaeta P and Sassòli M (eds), *The 1949 Geneva Conventions: A Commentary* (OUP 2015)
Szesnat F and Bird AR, ‘Colombia’ in Wilmshurst E (ed), *International Law and the Classification of Conflicts* (OUP 2012)
Tomuschat C, ‘Self-Determination in a Post-Colonial World’ in Tomuschat C (ed), *Modern Law of Self-Determination* (Martinus Nijhoff Publishers 1993)
Vardi G-I, ‘The Change from Within’ in Strachan H and Scheipers S (eds), *The Changing Character of War* (OUP 2011)

Weller M, ‘Introduction: International Law and the Problem of War’ in Weller M (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015)

Ahmed DI, ‘Defending Weak States against the "Unwilling or Unable" Doctrine of Self-Defence’ 9 Journal of International Law and International Relations 1
Arimatsu L, ‘Territory, Boundaries and the Law of Armed Conflict’ 12 YBIHL 157
Bassiouni MC, ‘Legal Control of International Terrorism: A policy-Oriented Assessment’ 43 Harvard International Law Journal 83
Bertram SK, ‘Authority and Hierarchy within Anonymous Internet Relay Chat Networks’ 6 Journal of Terrorism Research 15
Blank LR, ‘Defining the Battlefield in Contemporary Conflict and Counterterrorism: Understanding the Parameters of the Zone of Combat’ 39 Georgia Journal of International and Comparative Law 1
Boothby WH, ‘Differences in the Law of Weaponry When Applied to Non-International Armed Conflict’ 88 International Law Studies 197
Brooks RE, ‘War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror’ 153 University of Pennsylvania Law Review 675
Buchan R, ‘Cyber Warfare and the Status of Anonymous under International Humanitarian Law’ 15 Chinese Journal of International Law 741
——, ‘Cyber Attack: Lawful Uses of Force or Prohibited Interventions? ’ 17 Journal of Conflict & Security Law 211
Byron C, ‘Armed Conflicts: International or Non-International?’ 6 Journal of Conflict & Security Law 63
Carnahan BM, ‘Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity’ 92 AJIL 213
Carron D, ‘Transnational Armed Conflicts’ 7 Journal of International Humanitarian Legal Studies 5
Cassese A, ‘The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgement on Genocide in Bosnia’ 18 EJIL 649
Corn G and Jensen ET, ‘Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations’ 42 Israel Law Review 46
Corn GP and Taylor R, ‘Sovereignty in the Age of Cyber’ 111 AJIL Unbound 207
Corn GS, ‘Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict’ 40 Vanderbilt Journal of Transnational Law 295
——, ‘Geography of Armed Conflict: Why it is a Mistake to Fish for the Red Herring’ 89 International Law Studies 77
Corn GS and Jensen ET, ‘Untying the Gordian Knot: A Proposal for Determining Applicability of the Laws of War to the War on Terror’ 81 Temple Law Review 787
Daskal JC, ‘The Geography of the Battlefield: A Framework for Detention and Targeting outside the "Hot" Conflict Zone’ 161 University of Pennsylvania Law Review 1165
Debuf E, ‘Tools to Do the Job: The ICRC’s Legal Status, Privileges and Immunities’ 97 IRRC 319

Deeks AS, '"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense' 52 Virginia Journal of International Law 483
Demarest GB, 'Espionage in International Law' 24 Denver Journal of International Law and Policy 321
Dinstein Y, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' 89 International Law Studies 276
Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' 112 AJIL 583
Ferraro T, 'The ICRC's Legal Position on the Notion of Armed Conflict Involving Foreign Intervention and on Determining the IHL Applicable to This Type of Conflict' 97 IRRC 1227
Franzese PW, 'Sovereignty in Cyberspace: Can It Exist?' 64 The Air Force Law Review 1
Geiß R, 'Armed Violence in Fragile States: Low-intensity conflicts, spillover conflicts, and sporadic law enforcement operations by third parties' 91 IRRC 127
Geiss R, 'Cyber Warfare: Implications for Non-International Armed Conflicts' 89 International Law Studies 627
Giladi RM, 'Reflections on Proportionality, Military Necessity and the Clausewitzian War' 45 Israel Law Review 323
Gill TD, 'Classifying the Conflict in Syria' 92 International Law Studies 353
Ginsburg T, 'Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0' 111 AJIL Unbound 205
Goldsmith J, 'How Cyber changes the Laws of War' 24 EJIL 129
Greenwood C, 'International Humanitarian Law and the *Tadić* Case' 7 EJIL 265
Hathaway OA and others, 'The Law of Cyber-Attack' 100 California Law Review 817
Hayashi N, 'Military Necessity as Normative Indifference' 44 Georgetown Journal of International Law 675
Heinegg WHv, 'Territorial Sovereignty and Neutrality in Cyberspace' 89 International Law Studies 123
Heyns C and others, 'The International Law Framework Regulating the Use of Armed Drones' 65 ICLQ 791
Higgins AP, 'Submarine Warfare' 1 BYBIL 149
Hlavkova M, 'Reconstructing the Civilian/Combatant Divide: A Fresh Look at Targeting in Non-International Armed Conflict' Journal of Conflict & Security Law 1
Hughes R, 'A Treaty for Cyberspace' 86 International Affairs 523
Hutchinson T and Duncan N, 'Defining and Describing What We Do: Doctrinal Legal Research' 17 Deakin Law Review 83
Im J-I and others, 'North Korea's Cyber War Capability and South Korea's National Counterstrategy' 29 The Quarterly Journal of Defense Policy Studies 9
Jackson RB, 'Perfidy in Non-International Armed Conflicts' 88 International Law Studies 237
Johnson DR and Post D, 'Law and Borders - The Rise of Law in Cyberspace' 48 Stanford Law Review 1367
Jorritsma R, 'Where General International Law meets International Humanitarian Law: Attribution of Conduct and the Classification of Armed Conflicts' 23 Journal of Conflict & Security 405

Kelsey JTG, ‘Hacking into International Humanitarian Law: the Principles of Distinction and Neutrality in the Age of Cyber Warfare’ 106 Michigan Journal of International Law 1427
Kilovaty I, ‘World Wide Web of Exploitations — The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach’ 18 Columbia Science & Technology Law Review 42
Kreß C, ‘Some Reflections on the International Legal Framework Governing Transnational Armed Conflcits’ 15 Journal of Conflict & Security Law 245
Langbroek P and others, ‘Methodology of Legal Research: Challenges and Opportunities’ 13 Utrecht Law Review 1
Lanovoy V, ‘The Use of Force by Non-State Actors and the Limits of Attribution of Conduct’ 28 EJIL 563
Lin H, ‘Cyber Conflict and International Humanitarian Law’ 94 IRRC 515
Lin HS, ‘Offensive Cyber Operations and the Use of Force’ 4 Journal of National Security Law and Policy 63
Lind WS, ‘Understanding Fourth Generation of War’ 84 Military Review 12
Mar KD, ‘The Requirement of ‘Belonging’ under International Humanitarian Law’ 21 EJIL 105
Margulies P, ‘Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"’ 89 International Law Studies 54
——, ‘Sovereignty and Cyber Attacks: Technology’s Challenge to the Law of State Responsibility’ 14 Melbourn Journal of International Law 496
Margulies P and Sinnot M, ‘Crossing Borders to Target Al-Qaeda and Its Affiliates: Defining Networks as Organised Armed Goups in Non-International Armed Conflicts’ 16 YBIHL 319
Meron T, ‘The Martens Clause, Principles of Humanity, and Dictates of Public Conscience’ 94 AJIL 78
Moore S, ‘Cyber Attacks and the Beginnings of an International Cyber Treaty’ 39 North Carolina Journal of International Law & Commercial Regulation 223
O'Connell ME, ‘Combatants and the Combat Zone’ 43 University of Richimond Law Review 845
——, ‘Defining Armed Conflict’ 13 Journal of Conflict & Security Law 393
Ohlin JD, ‘The Combatant’s Privilege in Asymmetric and Covert Conflicts’ 40 Yale Journal of International Law 337
Okimoto K, ‘The Relationship between a State and an Organised Armed Group and Its Impact on the Classification of Armed Conflict’ 5 Amsterdam Law Forum 33
Oswald BO, ‘The Harmonization Project: Improving Compliance with the Law of War in Non-International Armed Conflicts’ 53 Columbia Journal of Transnational Law 105
Padmanabhan VM, ‘Cyber Worriors and the *Jus in Bello*’ 89 International Law Studies 288
Parker G, ‘The "Military Revolution," 1560-1660 - a Myth?’ 48 The Journal of Modern History 195
Paulus A and Vashakmadze M, ‘Asymmetrical War and the Nothing of Armed Conflict - A Tentative Conceptualization’ 91 IRRC 95
Pejić J, ‘Extraterritorial Targeting by Means of Armed Drones: Some Legal Implications’ 96 IRRC 67
——, ‘The Protective Scope of Common Article 3: More than Meets the Eye’ 93 IRRC 189

Ponemon Institute, ‘The Rise of Nation State Attacks’ 4 Journal of Law & Cyberwarfare 1
Pratt RL, ‘The International Legal Prohibition on Perfidy and Its Scope in Non-International Armed Conflicts’ 56 Virginia Journal of International Law 1
Radin S, ‘Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflict’ 89 International Law Studies 696
Ranganathan S, ‘Global Commons’ 27 EJIL 693
Rid T, ‘Cyber War Will Not Take Place!’ 35 Journal of Strategic Studies 5
Rid T and McBurney P, ‘Cyber-Weapons’ 157 The RUSI Journal 6
Roach A, ‘Legal Aspects of Modern Submarine Warfare’ 6 Max Plank Yearbook of United Nations Law 367
Ruys T, ‘The Syrian Civil War and the Achilles' Heel of the Law of Non-International Armed Conflict’ 50 Stanford Journal of International Law 247
Ryngaert C and Meulebroucke AVd, ‘Enhancing and Enforcing Compliance with International Humanitarian Law by Non-State Armed Groups: an Inquiry into some Mechanisms’ 16 Journal of Conflict & Security Law 443
Schindler D, ‘The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols’ 163 RCADI 125
Schmitt MN, ‘Cyberspace and International Law: The Penumbral Mist of Uncertainty’ 126 Havard Law Review Forum 176
——, ‘Rewired Warfare: Rethinking the Law of Cyber Attack’ 96 IRRC 189
——, ‘Military Necessity and Humanity in Internaitonal Law: Preserving the Delicate Balance’ 50 Virginia Journal of International Law 795
——, ‘Drone Attacks under the Jus ad Bellum and Jus in Bello: Clearing the 'Fog of Law'’ 13 YBIHL 311
——, ‘Classification of Cyber Conflict’ 17 Journal of Conflict & Security Law 245
——, ‘Drone Law: A Reply to UN Special Rapporteur Emmerson’ 55 Virginia Journal of International Law 14
——, ‘Charting the Legal Geography of Non-International Armed Conflict’ 52 Military Law and the Law of War Review 93
——, ‘Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law’ 52 Columbia Journal of Transnational Law 77
——, ‘The Law of Cyber Warfare: Quo Vadis?’ 25 Stanford Law & Policy Review 269
Schmitt MN and Vihul L, ‘Respect for Sovereignty in Cyberspace’ 95 Texas Law Review 1639
——, ‘Sovereignty in Cyberspace: *Lex Lata Vel Non*?’ 111 AJIL Unbound 213
Schöndorf RS, ‘Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?’ 37 New York University Journal of International Law and Politics 1
Shamir-Borer E, ‘Revisiting Hamdan v. Rumsfeld's Analysis of the Laws of Armed Conflict’ 21 Emory International Law Review 601
Shulman MR, ‘Discrimination in the Laws of Information Warfare’ 37 Columbia Journal of Transnational Law 939
Siers R, ‘North Korea: The Cyber Wild Card 2.0’ 6 Journal of Law & Cyberwarfare 155
Spector P, ‘In Defense of Sovereignty, In the Wake of Tallinn 2.0’ 111 AJIL Unbound 219
Stewart JG, ‘Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict’ 85 IRRC

Stone J, ‘Cyber War Will Take Place!’ 36 Journal of Strategic Studies 101
Tabansky L, ‘Basic Concepts in Cyber Warfare’ 3 Military and Strategic Affairs 75
Walker PA, ‘Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine’ 1 National Secuirty Law Brief 33
Wallace D and Reeves SR, ‘The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare ’ 89 International Law Studies 646
Wenger A and Mason SJA, ‘The Civilianization of Armed Conflict: Trends and Implications’ 90 IRRC 835

Book

Andress J and Winterfeld S, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Syngress 2011)
Barela SJ, *Legitimacy and Drones: Investigating the Legality, Morality and Efficacy of UCAVs* (Routledge 2016)
Bothe M, Partsch KJ and Solf WA, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (2nd edn, Martinus Nijhoff Publishers 2013)
Buchan R, *Cyber Espionage and International Law* (HART Publishing 2019)
Carr J, *Inside Cyber Warfare* (O’Reilly Media 2010)
Clarke RA and Knake KK, *Cyber War* (HarperCollins Publishers 2010)
Clausewitz Cv, *On War (Translated by Michael Howard and Peter Paret)* (Oxford World's Classics 2007)
Clough J, *Principles of Cybercrime* (CUP 2010)
Crawford E, *The Treatment of Combatants and Insurgents under the Law of Armed Conflict* (OUP 2010)
Crawford JR, *The Creation of States in International Law* (OUP 2007)
Crowe J and Weston-Scheuber K, *Principles of International Humanitarian Law* (Edward Elgar 2013)
Cullen A, *The Concept of Non-international Armed Conflict in International Humanitarian Law* (CUP 2010)
Dinniss HH, *Cyber Warfare and the Laws of War* (CUP 2012)
Dinstein Y, *War, Aggression and Self-Defence* (6th edn, CUP 2017)
——, *War, Aggression, and Self-defence* (5 edn, CUP 2011)
——, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn, CUP 2016)
——, *Non-International Armed Conflicts in International Law* (CUP 2014)
Fleck D (ed) *The Handbook of International Humanitarian Law* (3rd edn, OUP 2013)
——, *The Handbook of International Humanitarian Law* (2 edn, OUP 2008)
Fresard J-J, *The Roots of Behaviour in War - A Survey of the Literature* (2004)
Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2008)
Grotius H, *De jure belli ac pacis libri tre* (1625)
Henckaerts J-M and Doswald-Beck L (eds), *Customary International Humanitarian Law Volume I: Rules* (ICRC, CUP 2005)
Krutzsch W, Myjer E and Trapp R (eds), *The Chemical Weapons Convention: A Commentary* (OUP 2014)

Lubell N, *Extraterritorial Use of Force against Non-State Actors* (OUP 2010)
Moir L, *The law of internal armed conflict* (CUP 2002)
Newton M and May L, *Proportionality in International Law* (OUP 2014)
Okimoto K, *The Distinction and Relationship between Jus ad Bellum and Jus in Bello* (Hart Publishing 2011)
Oppenheim L, *International Law II War and Neutrality* (2 edn, Longmans, Green and Co. 1912)
Owens WA, Dam KW and Lin HS (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press 2009)
Pictet JS (ed) *The ICRC Commentary I on the Geneva Convention of 12 August 1949* (ICRC 1952)
Pictet JS (ed) *The ICRC Commentary III on the Geneva Convention of 12 August 1949* (ICRC 1960)
Rid T, *Cyber War Will Not Take Place* (Hurst 2013)
Rodenhäuser T, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law* (OUP 2018)
Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP 2014
Sandoz Y, Swinarski C and Zimmermann B (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC / Martinus Nijhoff 1987)
Schmitt MN (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017)
—— (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013)
Schmitt MN, Garraway CHB and Dinstein Y, *The Manual on the Law of Non-International Armed Conflict with Commentary* (IIHL 2006)
Schneider BR and Grinter LE (eds), *Battlefield of the Future 21st Century Warfare* (Air University Press 1998)
Singer PW and Friedman AA, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (OUP 2014)
Sivakumaran S, *The Law of Non-International Armed Conflict* (OUP 2012)
Stiennon R, *Surviving Cyberwar* (Government Institutes 2010)
Tikk E, Kaska K and Vihul L (eds), *International Cyber Incidents: Legal Considerations* (CCDCOE 2010)
Tonkin H, *State Control over Private Military and Security Companies in Armed Conflict* (CUP 2011)
Warren P and Streeter M, *Cyber Crime & Warfare: All that Matters* (Hodder & Stoughton 2013)
Wilson HA, *International Law and the Use of Force by National Liberation Movement* (OUP 1988)
Woltag J-C, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014)
Zamir N, *Classification of Conflicts in International Humanitarian Law: The Legal Impact of Foreign Intervention in Civil Wars* (Edward Elgar 2017)

Case

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) ((Judgement) [2007] ICJ Rep 43)
Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) ((Judgement) [2005] ICJ Rep 168)
Corfu Channel case ((Merit) [1949] ICJ Rep 4)
Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America) ((Merits) [1986] ICJ Rep 14)
Legality of the Threat or Use of Nuclear Weapons ((Advisory Opinion) [1996] ICJ Rep 226)
Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory ((Advisory Opinion) [2004] ICJ Rep 136)
Oil Platforms (Islamic Republic of Iran v. United States of America) ((Merits) [2003] ICJ Rep 161)

Prosecutor v. Dusko Tadić Decision on the Defence motion for Interlocutory Appeal on Jurisdiction ((Jurisdiction) ICTY (2 October 1995))
Prosecutor v. Dusko Tadić ((Judgement) ICTY IT-94-1-T (7 May 1997))
Prosecutor v. Dusko Tadić ((Judgement) ICTY IT-94-1-A (15 July 1999))
Procesutor v. Enver Hadžihasanović, Amir Kubura ((Judgement) ICTY IT-01-47-T (15 March 2006))
Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu ((Judgement) ICTY IT-03-66-T (30 November 2005))
Prosecutor v. Ljube Boškoski, Johan Tarčulovski ((Judgement) ICTY IT-04-82-T (10 July 2008))
Prosecutor v. Ljube Boškoski, Johan Tarčulovski ((Judgement) ICTY IT-04-82-A (9 May 2010))
Prosecutor v. Mile Mrkšić, Miroslav Radić, Veselin Šljivančanin ((Judgement) ICTY IT-95-13/1-T (27 Septemeber 2007))
Prosecutor v. Rajic, Review of the Indictment Pursuant to Rule 61 (ICTY IT-95-12-R61(1996))
Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj ((Judgement) ICTY IT-04-84-T (3 April 2008))
Prosecutor v. Slobodan Milošević Decision on Motion for Judgement of Acquittal (ICTY IT-02-54-T (16 June 2004))
Prosecutor v. Zejnil Delalić, Zdravko Mucić, Hazim Delić, and Esad Landžo ((Judgement) ICTY IT-96-21-T (16 November 1998))

The Prosecutor v. Jean-Paul Akayesu ((Judgement) ICTR-96-4-T, T Ch I (2 September 1998))
The Prosecutor v. Thomas Lubanga Dyilo ((Decision on the Confirmation of Charges) ICC-01/04-01/06, Pre-T Ch I (29 January 2007))

The Case of the S.S. Lotus (France v. Turkey) (1927 P.C.I.J. (ser. A) No. 10 (Sept. 7))

Island of Palmas (or Miagnas) (The Netherland v. The United States America) (PCA Case No. 1925-01)

Eritrea-Ethiopia Claims Commission Partial Award: Jus Ad Bellum (International Arbitral Awards 2005)

Juan Carlos Abella v. Argentina (Inter-American Commission on Human Rights Case 11.137 (18 November 1997))

Hamdan v. Rumsfeld, Seceretary of Defense et al. (US Supreme Court 548 U.S. 557, 126 S.Ct. 2749 (29 June 2006))

The Public Committee against Torture in Israel v. The Government of Israel (High Court of Justice, HCJ 769/02 (13 December 2006))

Electronic article

Anderson K, 'Targeted Killing and Drone Warfare ' A Future Challenges Essay <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Anderson.pdf>

Arimatsu L and Choudhury M, *The Legal Classification of the Armed Conflicts in Syria, Yemen and Libya* (Chatham House International Law PP 2014/01, 2014) <https://www.chathamhouse.org/sites/default/files/home/chatham/public_html/sites/default/files/20140300ClassificationConflictsArimatsuChoudhury1.pdf>

Biller LCJ and Schmitt M, 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences' EJIL:Talk! <https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/>

Dörmann K, 'Applicability of the Additional Protocols to Computer Network Attacks' (International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law

Goldsmith J, 'Cybersecurity Treaties - A Skeptical View' *Future Challenges in National Security and Law,* edited by Peter Berkowitz <http://www.futurechallengesessays.com>

Hakmeh J, 'Cyberattack Revelations Appear to Undercut Russia's UN Efforts' Chatham House Expert Comment <https://www.chathamhouse.org/expert/comment/cyberattack-revelations-appear-undercut-russia-un?utm_source=Chatham%20House&utm_medium=email&utm_campaign=9929905_CH%20Newsletter%20-%2012.10.2018&utm_content=Russia-CTA&dm_i=1S3M,5WTYP,NUT6YG,N4U8O,1>

Lin H, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' Aegis Paper Series <https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0>

Mueller B, *The Laws of War and Cyberspace: On the Need for a Treaty Concerning Cyber Conflict* (LSE IDEAS Strategic Update 2014)

< http://www.lse.ac.uk/ideas/research/updates/cyber>
Ohlin JD, 'The Unwilling or Unable Doctrine Comes to Life' Opino Juris <http://opiniojuris.org/2014/09/23/unwilling-unable-doctrine-comes-life/>
Rodenhäuser T and Cuénoud J, 'Speaking law to business: 10-year anniversary of the Montreux Document on PMSCs' Humanitarian Law & Policy Blog <http://blogs.icrc.org/law-and-policy/2018/09/17/speaking-law-business-10-year-anniversary-montreux-document-pmscs/?utm_source=ICRC+Law+%26+Policy+Forum+Contacts&utm_campaign=c1e18b2fd7-EMAIL_CAMPAIGN_2018_09_13_08_22_COPY_01&utm_medium=email&utm_term=0_8eeeebc66b-c1e18b2fd7-105936333&mc_cid=c1e18b2fd7&mc_eid=3e837c1a9e>
Schmitt M and Biller LCJ, 'The NotPetya Cyber Operation as a Case Study of International Law' EJIL: Talk! <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/>
Schmitt M and Vihul L, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' *Just Security* 30 June 2017 <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>
Sullivan JP and Elkus A, 'Plazas for Profit: Mexico's Criminal Insurgency' Small Wars Journal (26 April 2009) <http://smallwarsjournal.com/jrnl/art/plazas-for-profit-mexicos-criminal-insurgency>
_____, 'Israel Adds Cyber-Attack to IDF' <http://www.defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/>

Press

Akbar MS, 'Can Musharraf Save US from Liability for Drone Attacks?' *CNN* (10 May 2013) <https://edition.cnn.com/2013/05/10/opinion/pakistan-musharraf-drones/index.html>
Almosawa S and Nordland R, 'Drone Strike in Yemen Said to Kill Senior Qaeda Figure' *The New York Times* (5 Feb 2015) Middle East <http://www.nytimes.com/2015/02/06/world/middleeast/senior-qaeda-figure-in-yemen-killed-in-drone-strike.html?emc=edit_tnt_20150205&nlid=53442825&tntemail0=y&_r=0>
Boone J and Beaumont P, 'Pervez Musharraf admits permitting 'a few' US drone strikes in Pakistan' *The Guardian* <https://www.theguardian.com/world/2013/apr/12/musharraf-admits-permitting-drone-strikes>
Burgess M, 'DHL's Delivery Drone Can Make Drops Quicker Than A Car' *WIRED* (10 May 2016) <https://www.wired.co.uk/article/dhl-drone-delivery-germany>
Crerar P, Henley J and Wintour P, 'Russia Accused of Cyber-Attack on Chemical Weapons Watchdog' *The Guardian* (4 October 2018) <https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body>

Goldsmith J, ‘Cybersecurity Treaties - A Skeptical View’ *Future Challenges in National Security and Law,* edited by Peter Berkowitz <http://www.futurechallengesessays.com>
Gordon MR, Cooper H and Shear MD, ‘Dozens of U.S. Missiles Hit Air Base in Syria’ *New York Times* (6 April 2017) <https://www.nytimes.com/2017/04/06/world/middleeast/us-said-to-weigh-military-responses-to-syrian-chemical-attack.html>
Greenberg A, ‘How an Entire Nation Became Russia’s Test Lab for Cyberwar’ WIRED <https://www.wired.com/story/russian-hackers-attack-ukraine/>
——, ‘The Untold Story of Notpetya, The Most Devastating Cyberattack in History’ WIRED <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
Guernsey L, ‘Welcome to the World Wide Web. Passport, Please? ’ *The New York Times* (15 March 2001) Technology <http://www.nytimes.com/2001/03/15/technology/15BORD.html>
Hern A, ‘DHL launches first commercial drone 'parcelcopter' delivery service’ *The Guardian* (25 September 2014) <http://www.theguardian.com/technology/2014/sep/25/german-dhl-launches-first-commercial-drone-delivery-service>
Ignatius D, ‘A Quiet Deal with Pakistan’ *The Washington Post* (4 November 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2008/11/03/AR2008110302638.html>
Krebs B, ‘Report: Russian Hacker Forums Fueled Georgia Cyber Attacks’ *The Washington Post* (16 October 2008) Security Fix <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>
Lee J, ‘Record of Cyber Terror from North Korea’ *Yonhap News* (10 Apr 2013) <http://www.yonhapnews.co.kr/bulletin/2013/04/10/0200000000AKR20130410097700014.HTML?input=1179m>
Lyall N, ‘China's Cyber Militias: China’s cyber power is in the grip of dual trends: pluralism and centralization’ *The Diplomat* (1 March 2018) <https://thediplomat.com/2018/03/chinas-cyber-militias/>
Markoff J and Kramer AE, ‘U.S. and Russia Differ on a Treaty for Cyberspace’ *The New York Times* (27 June 2009) <http://www.nytimes.com/2009/06/28/world/28cyber.html>
Mazzetti M, ‘New Terror Strategy Shifts C.I.A. Focus Back to Spying’ *The New York Times* (23 May 2013) <http://www.nytimes.com/2013/05/24/us/politics/plan-would-orient-cia-back-toward-spying.html?emc=tnt&tntemail0=y&_r=0>
Murphy K, ‘Things to Consider Before Buying That Drone’ *The New York Times* (6 December 2014) <http://www.nytimes.com/2014/12/07/sunday-review/things-to-consider-before-buying-that-drone.html?emc=edit_tnt_20141206&nlid=53442825&tntemail0=y>
Palmer D, ‘NotPetya Malware Attack: Chaos But Not Cyber Warfare’ *ZDNet* (16 August 2018) <https://www.zdnet.com/article/notpetya-malware-attack-chaos-but-not-cyber-warfare/>
Rogin J, ‘NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'’ *Foreign Policy* <http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>
Sanger DE, ‘Obama Order Sped Up Wave of Cyberattacks Against Iran’ *The New York Times* (1 June 2012)

<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0>
Shane S, Mazzetti M and Worth RF, 'Secret Assault on Terrorism Widen on Two Continents' *The New York Times* (14 August 2010) <http://www.nytimes.com/2010/08/15/world/15shadowwar.html?pagewanted=all&_r=0>
Wingfield N, 'Now, Anyone Can Buy a Drone. Heaven Help Us.' *The New York Times* (26 November 2014) Technology <http://www.nytimes.com/2014/11/27/technology/personaltech/as-drones-swoop-above-skies-thrill-seeking-stunts-elicit-safety-concerns.html?emc=edit_tnt_20141126&nlid=53442825&tntemail0=y>
Young KD, 'U.S. Strike in Somalia Targets Al-Qaeda Figure' *The Washington Post* (9 January 2007) <http://www.nytimes.com/2010/08/15/world/15shadowwar.html?pagewanted=all&_r=0>
_____, 'Syria in Civil War, Red Cross Says' *BBC NEWS* (15 July 2012) <http://www.bbc.co.uk/news/world-middle-east-18849362>
_____, 'South Korea to develop Stuxnet-like cyberweapons' *BBC News* (21 February 2014) Technology <http://www.bbc.co.uk/news/technology-26287527>
_____, 'Syria War Stirs New U.S. Debate on Cyberattacks' *The New York Times* (24 February 2018) <http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?nl=todaysheadlines&emc=edit_th_20140225&_r=0>

Others

UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* (A/RES/25/2625 24 October 1970)
——, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/66/359 14 September 2011)
——, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/69/723 13 January 2015)
——, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/65/201 16 July 2010)
——, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98 24 June 2013)
——, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174 22 July 2015)

HRC, *Investigation by the Office of the United Nations High Commissioner for Human Rights on Libya: detailed findings* (A/HRC/31/CRP.3 23 February 2016)
——, *Report of the Independent International Commission of Inquiry on the Syrian Arab Republic* (A/HRC/28/69 5 February 2015)
——, *Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1* (A/HRC/3/2 23 November 2006)
——, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston - Study on targeted killings* (A/HRC/14/24/Add.6 28 May 2010)

ILC, *Articles on the Responsibility of States for Internationally Wrongful Acts* (A/56/83 3 August 2001)
——, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law* (A/CN.4/L.682 13 April 2006)

ILA, *Final Report on the Meaning of Armed Conflict in International Law* (Use of Force Committee 2010)

ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (31st International Conference of the Red Cross and Red Crescent, 2011)
——, *Syria: Parties to the Fighting Must Distinguish between Civilians and Fighters* (News Release 27 May 2012)
——, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (31st International Conference of the Red Cross and Red Crescent, 2011)
——, *Holdings Armed Groups to International Standards: An ICRC Contribution to the Research Project of the ICHRP* (1999)
——, *The Montreux Document - On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict* (2008)

UN Human Rights Office of the High Commissioner, *Report of the Mapping Exercise documenting the most serious violations of human rights and international humanitarian law committed within the territory of the Democratic Republic of the Congo between March 1993 and June 2003* (UN August 2010)

Osula A-M, *National Cyber Security Organisation: United Kingdom* (CCDCOE, 2015)
Raud M, *China and Cyber: Attitudes, Strategies, Organisation* (CCDCOE, 2016)

Office of General Counsel, *Department of Defense Law of War Manual* (US Department of Defense 2015 (Updated December 2016))
US Departmet of Defense, *Department of Defense Cyberspace Policy Reoport* (Novemeber 2011)
US Deputy Secretary of Defence Memorandum, *The Definition of Cyberspace* (12 May 2008)

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

UK Ministry of Defence, *Supplementary Written Evidence from the Ministry of Defence* (2012)
——, *Cyber Primer* (2nd edn, Development, Concepts and Doctrine Centre July 2016)
HM Government, *UK National Cyber Security Strategy 2016 to 2021* (1 November 2016)
——, *A Strong Britain in an Age of Uncertainty* (HM Government 8 October 2010)
Cabinet Ofiice, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (25 November 2011)
House of Commons Defence Committee, *Defence and Cyber-Security Written Evidence* (2012)
Attorney General Jeremy Wright QC MP, *Cyber and International Law in the 21st Centrury* (UK Government 23 May 2018)

The Ministry of Foreign Affairs of the Russian Federation, *The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law* (2016)
The Ministry of Foreign Affairs of the Russian Federation, *Draft United Nations Convention on Cooperation in Combating Information Crimes* (2018)

Conflict Studies Research Centre & Institute of Information Security Issues, *Russia's "Draft Convention on International Information Security" A Commentary* (2012)

Ibrügger L, *The Revolution in Military Affairs - Special Report* (1998)
International Council on Human Rights Policy, *Ends & Means: Human Rights Approaches to Armed Groups* (2000)
MARSH, 'NotPetya Was Not Cyber "War"' (August 2018) <https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/NotPetya-Was-Not-Cyber-War-08-2018.pdf>
Melzer N, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009)