What are the emerging jus ad bellum issues of the international law applicable to cyber warfare, considering the diverging interpretations of the law by the western and non-western states?

Is a constitutionalist or pluralist regulation of cyber possible, and would it have the potential to account for all properties of cyber?

University of Southern Denmark
Full Name: Martynas Jankus
Date of Birth: 21.03.1996
Character count:189.482

Abstract

The jus ad bellum international law faces the most transformative period in recent history due to the rise of cyber warfare. This thesis will, therefore, analyse the emerging issues of international law applicable to cyber warfare. Firstly, it will outline the properties of cyber, particularly the differing conceptualization of cyber, by states, and the transformative extent of cyber capacities of anonymity, instantaneousness, collateral damage, and non-kinetic effects. The legal analysis will then explore the international law regulating use of force and self-defence in cyberspace. The legal interpretation of jus ad bellum applicability by western and the interpretation of non-applicability by some non-western states will be presented. These interpretations will then be analysed according to legal interpretative principles, considering the object, purpose, subsequent practise and preparatory work, of the jus ad bellum law codified in the UN Charter. The use of force international law analysis will primarily be concerned with the prohibition of the use of force in the art.2(4) of the UN Charter. The following issues of use of force pertaining to cyber will be demonstrated: divided practise of interpretation, the narrow scope and inapplicability of art.2(4) to certain non-kinetic attacks. It will be argued that the opposing interpretations claiming that jus ad bellum law is applicable, or not applicable to cyber, have significant support and legal basis. The self-defence international law analysis will assess the art.51 of the UN Charter, customary international law and jurisprudence, to determine if cyber operations can constitute an armed attack warranting self-defence. Legal principles of damage threshold, attribution, necessity and proportionality will be examined in relation to cyber warfare. It will be argued that these principles are difficult to apply to cyber due to its properties. The thesis will then utilize the theories of legal constitutionalism and pluralism to analyse the factors from which issues of jus ad bellum international law emerged and the potential effects that those may have in the future of international legal order. The thesis will argue that a constitutionalist approach, while limited due to its need for consensus, is the preferable approach for universalising international law applicability to cyber, to ensure peace and stability.

Abbreviations

Art./arts.	Article/s (of a treaty/declaration/memorandum)
NATO	North Atlantic Treaty Organization
NSA	Non-state actor
LOAC	Laws of armed conflict
EU	European Union
GGE	Group of Governmental Experts
ICJ	International Court of Justice
ICT	Information and communications technology
ILC	International Law Commission
NAM	Non-Aligned Movement
Para./paras.	Paragraphs of a treaty
PIL	Public International Law
Res.	Resolution
SIGINT	Signals intelligence
UK	United Kingdom
UN	United Nations
UNASUR	Union of South American Nations
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
US	United States of America
USSR	Union of Soviet Socialist Republics
VCLT	Vienna Convention on the Law of Treaties

Table of Contents

1. Introduction

War is the most gruesome curse brought upon humanity that has dragged people into the abyss of sorrow, despair and misery for centuries. These times, now only but a haze of history and stories for some, served as a catalyst for humanity to become repulsed of what our fellow men and women can do. This repulsion can be seen forming within our states throughout history. A custom has emerged for states to settle disputes peacefully, diplomatically, and to prohibit the unjust use of force for the self-interest of states. International law has been and continuous to be the foundational medium of establishing what states, and through it, the polity, believe to be a just way to coexist in the world. Despite technological revolutions in warfare with the development of machine guns, tanks, and weapons of mass destruction, that presented unforeseen force, our compatriots, tamed these beasts, through fierce deliberations.[1] They managed to create the United Nations and codify the aforementioned customs into rules that to this day regulate the *jus ad bellum:* the circumstances under which it is just to partake in warfare. States are prohibited from needlessly using force, to destroy and kill peoples of other states. Force, with consideration of necessity and proportionality, is only allowed in self-defence where a hostile state has violated the prohibition.

The 21st century thrusts us into a new age of technology and revolution in warfare once again—the age of cyber and cyber warfare. You, the reader, and I, are tasked to be at least a fractional part of this generation's global deliberations. Today's state, its defences, and its people are highly interconnected and dependent on the perks of technology. Any device, no matter how secure, even if not connected to a network, can be rendered inoperable, destroyed or manipulated. Cyberspace allows hostile actors to use code and disable the stock markets, electricity grids, meltdown nuclear power plants, manipulate and destroy military systems. We have now seen most of these in action, with NotPetya viruses destroying computers worth of billions, Stuxnet successfully used to sabotage nuclear facilities, cyber-attacks disabling weapon systems and shutting down electricity grids.[2] The current international law regulating

[1] Clausewitz C. von, *On War* (1989), Princeton University Press, at Book 1; Münkler H. 'Old and New Wars', in M. D. Cavelty and V. Mauer (eds.), *The Routledge Handbook of Security Studies* (2010).

[2] BBC, *US 'Launched Cyber-Attack on Iran Weapons Systems'*, 2019 (available at https://www.bbc.com/news/world-us-canada-48735097); Farwell J.P. and Rohozinski R., 'Stuxnet and the Future of Cyber War', 53*Global Politics and Strategy* (2011), at 23–29; Hemsley K. and Fisher R., 'A History of Cyber Incidents and Threats Involving Industrial Control Systems', 542*IFIP Advances in Information and Communication Technology* (2018), at 227–230; Lorenzo Carrazana, 'The Economics of Cybersecurity and Cyberwarfare: A Case Study' (2018) (available at ECON Colloquium), at 3–7; Osawa J., 'The Escalation of State

jus ad bellum, is made explicitly with conventional weaponry in mind, simply because cyber technology did not exist in the time when these customs were forming and laws were being codified. Therefore, international law has not, ever, dealt with technology like cyber, attacks of which are exceptionally scientifically sophisticated, instantaneous, anonymous, entirely virtual, often having no explicit kinetic effects, very cheap, and so interconnected with our most basic infrastructure. It is also easily replicable and empowers non-state actors, like terrorists with the means of effective covert warfare.[3] The broad inquiry of today's legal experts and states remains to determine how the most fundamental laws that regulate warfare, ensure peace and stability, can be applicable to cyber warfare. The first research question of this thesis will, therefore, be as follows:

What are the emerging jus ad bellum issues of the international law applicable to cyber warfare, considering the diverging interpretations of the law by the western and non-western states?

Cyber warfare is an entirely new phenomenon, the perception of which depends on one's legal, political, geopolitical and technological perspectives. Considering the potential of cyber to transform warfare and international relations of today, there is a multitude of legal stances that have emerged globally, regarding the precise applicability of certain international laws to cyber warfare. This thesis will dedicate its primary efforts to determine these different legal stances, and the issues that are emerging or may emerge when applying the jus ad bellum international laws. It will analyse whether the current jus ad bellum law can truly be applied to cyber, and if so what are the emerging issues in determining: the level of damage of cyber required to constitute a use of force, whether a cyber-attack can constitute an armed attack that warrants self-defence, and the difficulties of applying the concepts of proportionality and necessity to cyber. Furthermore, as there is significant division over the applicability of said laws and legal principles, the thesis must also consider the means and ends of regulating cyber. Particularly the extent to which the regulation of cyber should be constitutionalised or pluralised. Therefore, the secondary research question is as follows:

Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', 24*Asia-Pacific Review* (2017), at 113–118.

[3] Kello L., *The Virtual Weapon and International Order*, The Virtual Weapon and International Order (1st ed., 2017), at 1–7.

Is a constitutionalist or pluralist regulation of cyber possible, and would it have the potential to account for all properties of cyber warfare?

Through the theoretical lens the legal reasoning behind certain regulatory approaches of states, towards jus ad bellum and cyber warfare will be explored. The possibility of fragmentation of international law, an ongoing contemporary issue, will be examined, as well as its effect on the ability of the international community to regulate cyber effectively.

The thesis will demonstrate that jus ad bellum international law non-applicability to cyber has support and some legal basis. Overall it will argue that jus ad bellum applicability to cyber warfare currently has relatively sturdier basis. However, cyber still presents numerous serious difficulties in applying the law. The analysis to answer the two outlined research questions will be presented throughout specific sections of the thesis, that deal with the *properties of cyber warfare*, the *law regulating the use of force*, the *law regulating self-defence*, legal *constitutionalist and pluralist approaches towards international legal order*. These essential concepts and international laws will be analysed throughout the thesis as follows:

Section 2 will serve as the methodological foundation for the thesis. It will present the precise scope and methods needed to answer the specific research questions. It will also outline legal sources and documents that will be analysed throughout the thesis, as well as the interpretative methods that shall be used when considering the law. It will also present the theoretical framework that will be utilized to examine the legal order that may regulate cyber.

Section 3 will analyse the nuanced conceptualizations of cyber by legally significant states, and how this forms the bedrock of the legal stances that the states take. Furthermore, the section will also analyse the potential capacity of cyber to cause damage in order to outline the scope of the properties that international law will have to address.

Section 4 will analyse the relevant international law regulating the use of force and present the legal analysis regarding interpretation, practise, preparatory work, case law and the issues that stem from these, primarily: the persistent demand not to apply use of force laws to cyber, divided state subsequent practise and limits outlined in case law jurisprudence.

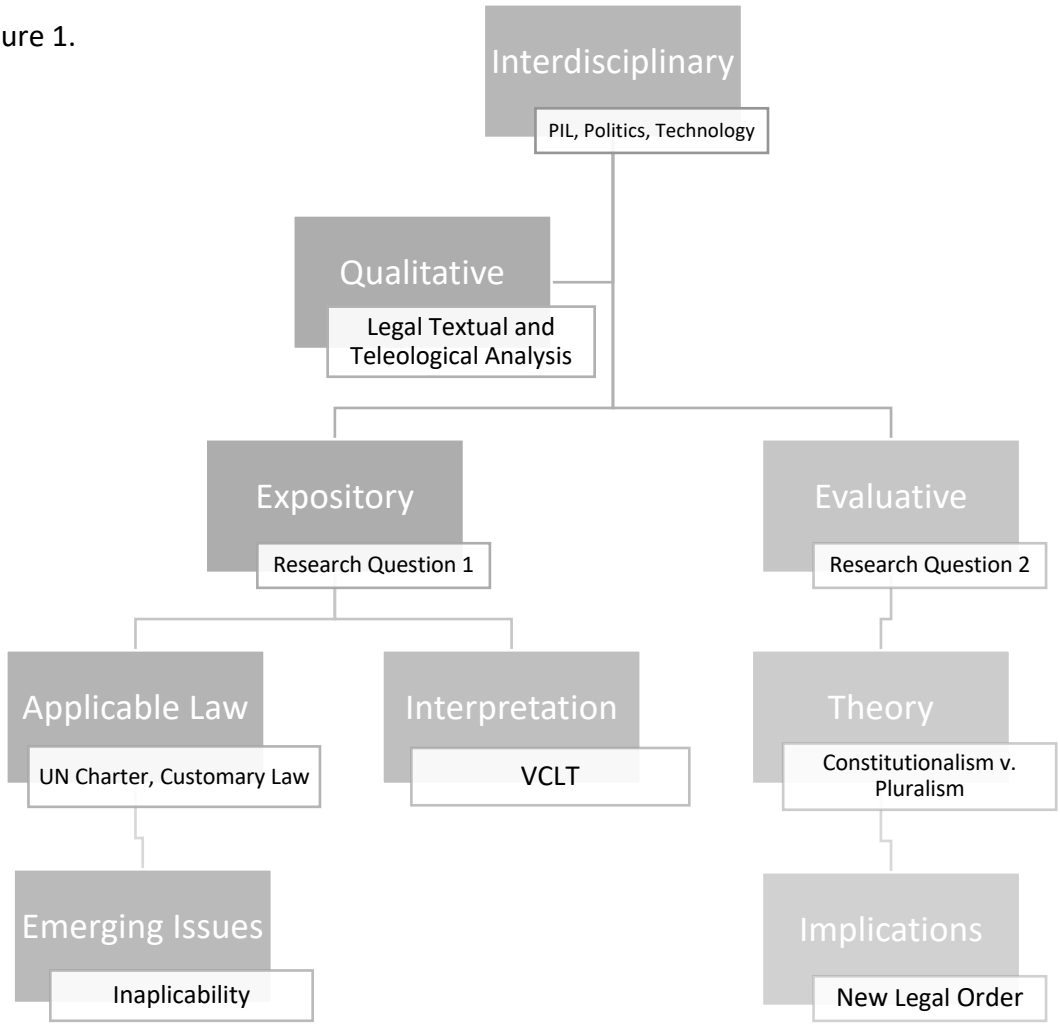
Section 5 will analyse the international law regulating self-defence and present the legal analysis of case law, state practise, and customary law, which will showcase the following difficulties of: applying the legal damage threshold to cyber, legally attributing cyber-attacks, and ensuring the application of necessity and proportionality in cyber.

Section 6 will analyse legal constitutionalist and pluralist approaches towards employing international law to regulate cyber and will showcase the limitations of international law in addressing cyber warfare. Primarily it will showcase the inability of constitutionalism to reconcile different interpretations of the law, while pluralism fails to ensure peace and stability if applied to jus ad bellum.

2. Methodology and Theoretical Framework

Methodology forms the foundation that is essential for sound legal research. As the rigidity of methods has long been under scrutiny in international legal research, this thesis will attempt to present a clear framework of the study.[4] The methodological approach is often pre-determined by the nature of the research questions. However, a methodology often consists of several layers that vary in specificity. When studying law, a choice has to be made on the interdisciplinarity of the study, qualitative and quantitative research, as well as other more specific methods of inquiry. Figure 1. attempts to showcase an outline of a methodological structure, particularly tailored for the study of international law and cyber warfare.

Figure 1.



[4] Fisher E. et al., 'Maturity and Methodology: Starting a Debate about Environmental Law Scholarship', 21*Journal of Environmental Law* (2009), at 224–230.

2.1 Interdisciplinarity

Understanding cyber, and cyber warfare requires the consideration of several disciplines. As cyber can be used for warfare, public international law (PIL) is of primary concern. The perceived purpose and resort to cyber is often dictated by politics, while the actual capacity of cyber, its potential for destruction and disturbance is dictated by technological nuances. Therefore, while the main focus of the thesis remains to be international law, the approach will to an extent be interdisciplinary and provide the necessary political and technological considerations. *Section 3* will provide an analysis of the technological, strategic and political nuances that influence the conceptualization, perception and legal interpretation of cyber by states.

2.2 Qualitative methodology

Due to the nature of the legal research questions of this thesis, an overall qualitative approach will be utilized. The qualitative approach will encompass a legal textual, teleological and political approaches, that rely on the interpretation of primary and secondary sources in accordance with Vienna convention of the law of treaties (VCLT) and other interpretative tools, where appropriate. The specific utilization of the VCLT and legal interpretative tools will be further delved into the relevant part of the methodology.

2.3 Expository approach

The two research questions require further, separate methodological consideration. The methods for the primary research question "*What are the emerging jus ad bellum issues of the international law applicable to cyber warfare, considering the diverging interpretations of the law by the western and non-western states?"* will be considered as follows:

Determining the jus ad bellum international law (law stipulating legal conditions to resort to use of force or war) applicable to cyber warfare, its subsequent interpretations and emerging issues requires an *expository* study, a descriptive and analytical approach that aims to demonstrate how the law in this specific area, is considered to work.[5] As western and some

[5] Cryer R. et al., *Research Methodologies in EU and International Law* (2011), at 9–10.

non-western states disagree on how the law is considered to work, such an approach will also highlight the emerging issues of jus ad bellum, particularly in the conflicting or ineffective application of the laws, diverging interpretations, as well as the difficulties in regulating cyber in itself. The expository study will form the most extensive part of the thesis. The reasoning behind the *western* and *non-western* dichotomous terminology is for the sake of simplicity, as the disagreement on the law is primarily between states situated in the west, and those that are not. This does not mean that all non-western states have the same exact oppositional interpretation of the law. International law is a product of treaties, judicial decisions, and various other sources. It is also a product of custom, formed via deliberations and actions, primarily by states. In legal literature these concepts are referred to as opinio juris and state practice, respectively. Those can take the form of statements, political, military documents, memorandums of understanding and more. Therefore, the expository part in *sections 4 and 5,* will involve the analysis of the texts, documents and treaties that form part of the jus ad bellum laws or the ongoing legal deliberations.[6] The sources of law, relevant treaties and the methods used to interpret them, will be discussed in the next section of the methodology.

2.4 Determining applicable jus ad bellum law – Legal sources for the expository approach

The sources of international law are determined in the ICJ statute, article 38 paragraph 1.[7] A shortened rendition of the sources could be presented as: *treaties, custom, general principles of law, judicial decisions and teachings of most highly qualified publicists*. The methods will consider the changing primacy of these sources, primarily the importance of judicial decisions in identifying the law, and the decreasing significance of teachings.[8] Fortunately, the jus ad bellum laws are foundational to the public international legal system, and are some of the most established laws in treaties, customary international law and exemplified in judicial decisions.

2.4.1 Treaties

The Charter of the United Nations is the foundational regulating treaty, with 193 signatories. As a source it has acquired a supreme position in the international law system that does not

[6] *Ibid.*, at 5.
[7] Statute of the International Court of Justice, 1945, p. art.38, para.1.
[8] Roberts A. and Sivakumaran S. 'The Theory and Reality of the Sources of Law', in M. D. Evans (ed.), *International Law* 5th (2018) , at 99.

have an extensive hierarchical arrangement. The UN charter stipulates, under art. 103, that obligations under the charter will prevail over other international agreements, in the event of conflicting norms.[9] As the U.N. was created as a result of the devastation of the second world war, its primary purpose, has been and continues to be, the maintenance of international peace and security.[10] Therefore, its regulation of warfare is the primary source that needs to be investigated in relation to cyber warfare to determine emerging jus ad bellum issues. The following sections of the U.N. charter, regulating warfare or otherwise contributing to the laws of war will be considered:

1. Chapter I: Purposes and principles.[11]

Primarily art. 1 that outlines the purposes of the charter, that form the context for all subsequent articles of the charter, and to an extent their interpretation. Art. 2(4) is the core law that prohibits the use of force, albeit with exceptions that will be considered later, and forms the foundation of the jus ad bellum.

2. Chapter VII: Action with respect to threats to the peace, breaches of the peace, and acts of aggression.[12]

Primarily art. 51, which stipulates one of the exceptions to the prohibition of force, in the event of self-defence. Furthermore, chapter VII, outlines the second exception to the prohibition of force, the authority of the Security Council to authorise actions to maintain peace.

These laws will be foundational in the analysis in *section 4 and 5*, however other treaties, such as the Covenant of the League of Nations, the Kellog-Briand pact and similar, will be referred to throughout the thesis.[13] Furthermore, there are other aspects that the UN charter and jus ad bellum laws regulate, such as countermeasures, reprisals, but these will not be covered in an

[9] United Nations, Charter of the United Nations, Art. 103, 1945.
[10] United Nations, Charter of the United Nations, Art. 1, 1945.
[11] United Nations, Charter of the United Nations, Chapter I: Purposes and Principles, 1945.
[12] United Nations, Charter of the United Nations, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, 1945.
[13] F. B. Kellogg and A. Briand, General Treaty for Renunciation of War as an Instrument of National Policy, 1928; The Covenant of the League of Nations, 1919.

in-depth manner, as other areas of jus ad bellum pose more issues in relation to cyber.

2.4.2 Customary international law

Customary international law is a source of law that may not be codified but is nonetheless identifiable, and binding to states. It forms from state practice and opinio juris. State practice consists of the actions that states take in a particular matter. This must be accompanied by opinio juris (opinion as to what law is), statements which showcase that states believe the practice to be law. The opinio juris can be made by any governmental body, but just as state practice, it should remain consistent and without contradictions.[14]

Customary law will be considered in areas where certain norms are not directly codified in the U.N. charter or other treaties. Customary law also serves to show the concreteness of the law, as some custom can acquire the status of jus cogens. Jus cogens, otherwise known as a peremptory norm, refers to custom that has become so widespread and established that no derogation from it could be lawful. This thesis will consider the customary law foundations guiding the use of force, particularly the prohibition of the use of force. Customary law becomes particularly relevant when analysing the applicability of self-defence, and principles such as proportionality and necessity.[15]

2.4.3 General principles

General principles of law guide matters where no formal norm or customary law regulates an area of international relations. [16] Legal concepts such as pacta sund servanda, meaning that a treaty must be upheld in good faith, may become relevant to new developing interpretation. Historically some states and legal subjects have attempted to propose interpretations that are not in good faith compared to alternative interpretations. This may be of significance considering very diverging interpretative disagreements and serve as a set of principles for reasonable application of the law. However, as jus ad bellum laws are well established, the resort to general principles may not be frequent.

[14] Roberts and Sivakumaran, *supra* note 8.
[15] Shelton D. 'International Law and 'Relative Normativity'', in M. D. Evans (ed.), *International Law* 4th (2014).
[16] Roberts and Sivakumaran, *supra* note 8.

2.4.4 Judicial decisions and the teachings of highly qualified publicists

The Judicial decisions, otherwise known as case law, serve an important task of reaffirming that laws regulating specific matters, in this case jus ad bellum, derive from the aforementioned legitimate sources. The International Court of Justice (ICJ) will be of most relevance to jus ad bellum. Judicial decisions identify and demonstrate interpretation of certain law, and specific applicability of said law.[17] Judicial decisions have arguably been increasing in significance. In such a case, judicial decisions can further the legal application and interpretation of law.[18] The following judicial decisions will be used to clarify the applicability of the international law regulating jus ad bellum, in relation to cyber:

1. ICJ Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)
2. ICJ Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)
3. ICJ Case Concerning oil platforms (Islamic Republic of Iran v. United States of America)
4. ICJ Corfu Channel Case (Albania v. United Kingdom)

These will provide useful argumentation regarding the legal basis to view or not to view cyber as use of force, armed attack, or as requiring attribution, certain damage threshold and effective control over non-state actors. Furthermore, other jurisprudence will also be considered, such as the *ICJ Legality of the Threat or Use of Nuclear Weapons* case, which is not a judicial decision, but rather an advisory opinion, that is not law, but serves to advise and clarify the interpretation of the law.[19] The aforementioned cases will be of primary concern, however, the list of judicial decision and advisory opinions is not exhaustive.

2.4.5 Interpretation

The interpretation of international law, particularly that based on treaties is guided by the Vienna convention of the law of treaties. It encompasses the principles of appropriate legal interpretation and will, therefore, guide this work. The interpretation of jus ad bellum laws will adhere to the hierarchy of interpretative principles outlined in the VCLT. First and

[17] *Ibid.*, at 98–99.
[18] *Ibid.*, at 106.
[19] The International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996.

foremost, as per VCLT art. 31 paras. 1 and 2, the interpretation of documents and treaty-based law must adhere to the principle of good faith. It must also consider the document with the ordinary meaning of terms, consistent with their context, object and purpose.[20] Secondly, this must also be taken into account, as per VCLT art. 31 para. 3, with the context of any subsequent agreement between parties on interpretation or application, as well as any subsequent practice of application of said treaty, that may establish an agreement of interpretation. Thirdly, Other international law that may be applicable must also be considered.[21] Lastly, the VCLT art.32 allows for supplementary methods of interpretation, in events of difficulty in determining the meaning of terms, that causes terms to be ambiguous, obscure or leads to outcomes that are absurd or unreasonable. For such cases, other means, such as travaux préparatoires, the preparatory work of the treaty, can be reviewed to eliminate obscurities.[22] While there is subjectivity to the interpretation of the law, in fact, there is a subjective school of interpretation that primarily focuses on the perceived intent of the parties, it is evident that the VCLT maintains an approach more focused on the text and objectives set out in the treaty. This could be identified as a combination of an objective and the teleological approaches, that consider the textual side of the law, as well as its intended purpose. The methodology of interpretation will adopt this view as well.[23]

2.5 Evaluative approach

The secondary legal research question *"Is a constitutionalist or pluralist regulation of cyber possible, and would it have the potential to account for all properties of cyber warfare?"* will employ a differing approach.

Demonstrating whether international law is taking or should take a more constitutionalist or pluralistic form in the regulation of cyber, and whether this would be able to account for all of the properties of cyber requires an *evaluative* study. That is an assessment of how the law works, identifying the limitations, shortfalls and potential improvements that can result from a more centralized or dispersed approach.[24] This part of the thesis will employ a more

[20] United Nations, Vienna Convention on the Law of Treaties, Art. 31, 1969.
[21] *Ibid.*
[22] United Nations, Vienna Convention on the Law of Treaties, Art. 32, 1969.
[23] Fitzmaurice M. 'The Practical Working of the Law of Treaties', in M. D. Evans (ed.), *International Law* 5th (2018), at 152–153.
[24] Cryer et al., *supra* note 5, at 9–10.

theoretical approach. The theories of constitutionalism and pluralism inform how the changes in international law can be conceptualized in a study and will aid in identifying the issues in the jus ad bellum law in relation to cyber, that could have the most significant impact.[25] *Section 6* will primarily deal with the evaluative theoretical approach.

2.6 Determining the preferable approach to regulate cyber – Legal theory and the evaluative approach

2.6.1 The theoretical framework of Constitutionalism and Pluralism

A theory provides a lens that is supposed to enhance the properties of the issue at hand, therefore careful selection could yield more insight. The secondary research question sets a difficult task that requires more than an analysis of the law. It requires the determination of how the changes in international law may affect cyber warfare. The most appropriate theoretical framework appears to be that of legal constitutionalism v. legal pluralism, because as it will be showcased in the analysis, the substantial disagreement on the application of jus ad bellum to cyber, threatens to fragment the law. Legal constitutionalism is a theory that views international law as a centralized matter, or one that ought to be centralized, around a constitutional framework. It views law as a universalistic, ethical approach that regulates global endeavours. It also supposes that progress in international law, the efficiency, the order of the system rests on maintaining or advancing further towards a more constitutionalized and centralized international legal regime. In such a view, international law should be a set of universal minimum rules that regulate the international order that states accept, and as a result, can operate in predictability and security.[26] Legal pluralism, on the other hand, views the voluntary nature of international law as an inevitable cause of fragmentation. It asserts that fragmentation is not necessarily the breakdown of the international system, but rather evidence for its efficiency. In such a way, a more pluralistic international legal system, allows for more freedom, diversity and increases adherence to the rules that states accept.[27] These theories are particularly relevant to the regulation of cyber warfare, because they can help assess whether

[25] *Ibid.*, at 5.
[26] Bianchi A. 'Constitutionalism and Global Governance', in *International Law Theories: An Inquiry into Different Ways of Thinking* (2016).
[27] Hoffmann F. 'International Legalism and International Politics', in A. Orford and F. Hoffmann (eds.), *The Oxford Handbook of the Theory of International Law* 1st (2016).

the disagreement over how to regulate cyber should be resolved with a pluralistic approach, or whether there must be consensus on universal norms.

Fragmentation has been occurring for decades and has affected international law broadly. International criminal law has experienced fragmentation with the increasing proliferation of courts and tribunals that use hybrid approaches involving international and national law and methods. Similar fragmentation is seen in international environmental law, international trade law where WTO appellate body has stopped functioning due to disagreements and has refrained from applying certain legal principles.[28] Therefore, constitutionalism and pluralism theories encompass the very essence of the current change in international law. Moreover, while fragmentation has been occurring in a multitude of legal areas, the jus ad bellum laws have been less affected. As the core mission of international law is to maintain peace, and regulate warfare, it is to no surprise that there hasn't been an interpretative collapse and fragmentation of jus ad bellum, but instead less system shocking interpretative disagreements of custom regarding self-defence, attribution or funding of militias. However, the disagreement over the entire applicability of jus ad bellum laws to cyber, has the potential to result in a first serious fragmentation over the interpretation of the jus ad bellum. These dichotomous theories will, therefore, provide a framework to assess whether the challenges that jus ad bellum laws face, will result in fragmentation. And if so, the theoretical approach will also allow for an assessment of the potential of jus ad bellum fragmentation happening, and the impact this could have on the legal order.

[28] Bianchi A. 'Legal Pluralism', in *International Law Theories: An Inquiry into Different Ways of Thinking* (2017) , at 231; Dunoff J. l. and Trachtman J.P. 'A Functional Approach to International Constitutionalization', in *Ruling the World? Constitutionalism, International Law, and Global Governance* (2009), at 31.

3. The properties of cyber warfare

Cyber warfare is not only a new phenomenon that is difficult to situate in international law, it is also a slippery concept to fully define. Hence, prior to reviewing the legal endeavours sparked by these technological changes, it is paramount to establish an understanding and conceptual basis of cyber warfare, for the purposes of this thesis. This is also crucial in order to understand the basis of the legal position's states will take. The following sections will aim to expand on the defining properties of cyber, and furthermore, the very impact said technology might have on warfare and international relations.

3.1 Cyber and warfare: Conceptualization and its importance to international law

Cyberspace and cyber warfare are terms that have been assigned differing meanings by the west and the non-western states. Common conceptualization is vital, in order to have effective deliberations in law-making. International law has seen excruciating negotiations of definitions and parameters, which in some occasions, can set parties at dead ends.[29] Western states have been rapidly developing cyber policy and military doctrines to appropriately conceptualize cyber within their state structures. While non-western states and other sympathizing states have primarily focused on domestic legislation regarding cyber.[30] Moreover, the respective counterparts in the cyber debate appear to be using different terms and have assigned differing properties and concepts to cyber. Therefore, establishing a universal definition of cyber warfare, may not be as useful, as analysing how the particular key players see cyber. Western states', and NATO allies' doctrinal approaches are similar, and convergencies can be seen comparing any western or liberal state. To exemplify, the Danish and American joint doctrines for military cyber operations can be utilized. The Danish doctrine defines cyberspace as "*the global volume of entities processing, storing and transmitting digital information and code, regardless of whether they are connected or not".*[31] The US doctrine provides a more expansive and technical definition of *"A global domain within the information environment consisting of the interdependent networks of information*

[29] See, for an exemplification of difficult international negotiations, Barriga S. and Grover L., 'A Historic Breakthrough on the Crime of Aggression', 105*The American Journal of International Law* (2011), at 517–531.
[30] Boas T.C. 'Weaving the Authoritarian Web: The Control of Internet Use in Nondemocratic Regimes', in J. Zysman and A. Newman (eds.), *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology* (2006) , at 4–20; Tselikov A., 'The Tightening Web of Russian Internet Regulation', *SSRN Electronic Journal* (2014), at 1–7.
[31] RDDC, Joint Doctrine for Military Cyberspace Operations, September, 2019, at 8.

technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[32] The Danish, US and French doctrines adopt a layered view of cyber, consisting of physical, logical and cyber-persona levels. These layers outline exactly how cyber is interconnected with hardware, equipment and virtual identities.[33] Furthermore, they have gone to great lengths to conceptualize offensive and defensive cyber operations, and how precisely they are to be used and operationalized against conventional targets.[34] Western states have developed a very in-depth framework of understanding regarding cyber, have declared it an environment in itself, on par with land, air and sea.[35] The public western conceptualizations outstrip any available non-western cyber doctrines by a large margin, perhaps because these countries are the most interconnected. Russian definitions are more difficult to determine as their cyber strategy is often not as coherent or publicly available. Determining Russian perception of cyberspace, warfare and the properties assigned to cyber, depends on the publications of Russian information strategy, military strategy, FSB statements and academic publications. Despite the dispersed information, one should not immediately assume that Russia does not have an extensive understanding and conceptualization of cyberspace, and offensive practices within it. However, it is definite that Russia, unlike western states, conceptualizes the emerging technological changes as the 'information space' and 'information warfare' rather than cyber, or cyber warfare.[36]

Perhaps appearing as a minor analytical divergence at first, it will serve to be a part of a broader perception difference, regarding the framing of computer technology as a weapon or part of warfare in the international legal arena. A more concrete perspective can be found in Russia's presented proposal of a convention on international information security, where in art.2, information space is termed 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*".[37]

[32] US Joint Staff, *Cyberspace Operations* (2018), Joint Publication, at GL-4.
[33] Ministère des Armées, *Éléments Publics De Doctrine Militaire De Lutte Informatique Offensive* (2019), at 5–6; RDDC, *supra* note 31, at 8; US Joint Staff, *supra* note 32, at VIII.
[34] US Joint Staff, *supra* note 32, at II-1 to II – 9.
[35] RDDC, *supra* note 31, at 9.
[36] Baumard P., *Cybersecurity in France* (2017), Springer, at 71.
[37] The Ministry of Foreign Affairs of the Russian Federation, *Convention on International Information Security*, 2016.

Evidently, the main difference is the inclusion of the individual and societal "consciousness" which refers to social norms and opinions that form peoples' perception of reality. It relates to the broader Russian strategy of influence, and further solidifies the widely discussed Russian focus on the importance of controlling information.[38] On the other hand, China, does not have a thorough publicly available view of cyber, and in the past has denied amassing cyber experts and setting up cyber forces, a fact which was conclusively determined by US SIGINT intelligence collection and through leaks.[39] It still remains undisputed that China adopts similar views of cyber, as primarily an information domain, where information dominance is essential to maintain stability.[40] In its military strategy, China dedicates a modest space to emphasize that it will now develop cyber military forces and cyber defence capabilities. In it, China also proclaims that cyberspace "*has become a new pillar of economic and social development*", to an extent also emphasizing the societal paradigm of cyber warfare.[41] Evidently, there are different views on cyber and its role in international relations. Western states view it more as a technological tool and a weapon of the military, defining it rigidly, in technical terms. While Russia and China, conceptualize it as a society impacting domain. This presents a difficult starting point for international law deliberations because for these states, cyber has different purposes. Overall, it could be said that these nations concur that cyber is a very interconnected domain, therefore capable of impacting information, technology and physical objects. Therefore, the urgency to deliberate persists.

The significantly differing conceptualization of cyber, and cyber warfare by these legal subjects of major influence, form rather different approaches to the law. Consider the states that strongly believe cyber is primarily a tool of social impact, used to control societal perceptions and information availability. Their dilemma rests on regulating cyber, to prevent any effects on their society. While states that are interconnected and strongly believe cyber is a tool of warfare capable of causing serious damage, will be preoccupied with applying the law in order to regulate the use of cyber force. The impact of these conceptualizations will become more apparent in, section 4, the expository analysis of the jus ad bellum laws applicable to cyber. Particularly when dealing with the interpretation of terms, the scope of

[38] Herpen M.H. Van, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (2016), at 19–30, 81–90.
[39] Baumard, *supra* note 36, at 12.
[40] Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (2019), at 45.
[41] The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (2019), at 13.

the prohibition of the use of force and its exceptions. Furthermore, the diverging conceptualization, as in other areas of law, also serves as the driving force for a potential pluralist fragmentation of the largely constitutionalist, universal and centralized, jus ad bellum international law. This will become more apparent in, section 6, the evaluative theoretical analysis of the factors driving the voluntary fragmentation of law applicable to cyber.

3.2 Is cyber a revolution in warfare?

States have made it clear, cyber is a crucial new domain, based on their conceptualization of how particularly it affects international relations or societies. However, one must not only rely on the views of states. It remains to be determined, for the sake of international legal regulation, whether cyber is just another security dilemma, or whether it is set to revolutionize warfare. Warfare has gone through numerous technological revolutions in history, that have spurred new generations of warfare. History is forever marked by 3rd generation warfare, based on a Clausewitzian trinity of the state, citizenry, and the army.[42] The onset of the nuclear revolution, and later terrorism and non-state actors have propelled warfare into 4th and potentially 5th generations, a distinction still fiercely debated in academia.[43] Cyber and the interconnectedness it has brought about, has the potential to constitute yet another revolutionary push towards new generations of war. With every generation of warfare, international law encounters new difficulties of regulation. Due to the nature of custom, cases and deliberation, international law regarding revolutionary technology, often develops the most following great travesties. An onset of revolutionary changes, as it had in the past, would present extensive difficulties for international law. Two camps have emerged in academia, those that believe cyber to be a revolution in warfare, and those that believe cyber will induce 'restraint' in actors. These camps set the basis for a different allocation of properties to cyber and allows to understand why states perceive it in certain ways. Apart from differing conceptualization, states also appear to be in a dispute regarding the true properties of cyber. The two camps also outline the potential properties international law may have to encompass when regulating. While this section will refer to some legal concepts relevant to cyber properties, the thorough legal analysis with consideration of the properties of cyber will be conducted in section 4 and 5.

[42] Clausewitz, *supra* note 1, at Book 1; Münkler, *supra* note 1.
[43] See, for a debate on the development of warfare, Hammes T., 'Fourth Generation Warfare Evolves, Fifth Emerges', 87*Military Review* (2007); Kaldor M., 'In Defence of New Wars', *International Journal of Security and Development* (2013).

The potentially revolutionary properties of cyber could be grouped into two layers: uncertainty and capacity. The uncertainty is brought about due to limited cases of cyber that can be thoroughly studied. Furthermore, the scientific complexity of cyber itself presents unknown factors. This will be difficult for states and international law to address. The cases of cyber usage for the purposes of warfare are a small subset. Information is often confidential, denied by the victims or accused perpetrators, tainted with politicised perceptions, or they are simply on a very low scale. International judiciary cases on cyber are essentially non-existent. Broad conclusion in the academic or political field has been criticised for this very limitation. The limitation prevents specialised theorists, cyber experts, and cyber statesmen from emerging. In academia, cyber is primarily, absorbed into long-established theoretical mechanisms in current literature.[44] Arguably, for this reason, scholars have not conclusively established the effects of cyber on international legal order and how it should be regulated. The difficulty of employing data bout cyber raises a methodological issue, while some traditional experts also disregard cyber, because it is not a kinetic, observable force.[45] However, perhaps, the fact that there are limited cases of large-scale cyber incidents, that are concerning enough for states to publicly attribute and dissect, shows that states are not inclined to use cyber as a new revolutionary method, opting for a 'restraint' position.

The scientific complexity and advancement of cyber may also be at play here. The technicalities of cyber often become too complex even for computer scientists as it involves sophisticated code and methods. Due to this cyber can't be modelled the same way other technology, such as nuclear fission, can be, reducing the predictability of attacks. Also, cyber capabilities and technology that could be used for warfare, unlike the technologies of the past, change so rapidly that it outstrips not only the understanding of experts but state strategy itself.[46] Even those that argue that cyber is not a revolutionary force, concede that the predicament of its capacity could change in the future.[47] Overall, it is evident that determining whether cyber is revolutionary, is a strenuous task, at least for now. Furthermore, there are indications that cyber can in some ways be a transformative tool. The lack of cases, and its scientific complexity presents a very difficult domain for international law, courts and states

[44] Kello, *supra* note 3, at 2–4.
[45] Kello L., 'The Meaning of the Cyber Revolution Perils to Theory and Statecraft', 38*International Security* (2013), at 9–15; Kello, *supra* note 3, at 11; Solis G.D., 'Cyber Warfare', *Military Law Review* (2014), at 1–5.
[46] Kello, *supra* note 3, at 6–7; Shackelford S.J., 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27*Berkeley Journal of International Law* (2009), at 216–219.
[47] B. Valeriano and R. Maness, Cyber War Versus Cyber Realities, 2015, pp. XI, 51.

when attempting to apply longstanding customary law, and judge damage, attribution, proportionality and other legal concepts.

There are additional qualities of cyber that complicate regulation further. Cyber-attacks are extremely fast and hard to control. Furthermore, it is non-kinetic, difficult to attribute, empowers NSAs, increases the uncertainty of expectations and collateral damage. Some of these factors already pose issues in international law, but cyber adds unique caveats. Cyber-attacks are often instantaneous and completed in milliseconds, challenging long-established international law norms of self-defence, because one cannot defend after the fact of an attack. The spread of cyber-attacks often cannot be controlled. Technology is now connected to the most basic infrastructure, therefore the unintended and domino effects known as *orders of effect*, can truly make cyber-attacks into self-sustaining force multipliers, which constitute a new kind of force. [48] It is difficult to view unintentional virtual damage through the lens of jus ad bellum. One can see the likes of NotPetya malware, which unintentionally spread globally and cost billions in damages.[49] Such events could be cited to settle that cyber is a tremendous force. However, this arguably, also makes cyber less appealing, because it becomes difficult to use cyber on specific targets. States also have an interest in preserving their economies and positive image in the eyes of their citizens. The risk of using cyber-attacks that could spread, and damage your own economy, your allies', or that of your enemies' (that remain your trading partners) and you may lose voters, allies, and reputation.[50] Perhaps this factors does not matter to non-western states in question, as they are already under sanctions.

Furthermore, cyber-attacks are non-physical, and often do not have physical effects. International law and particularly jus ad bellum, has never dealt with matters of force that can be entirely virtual. This also makes it hard to attribute, and in addition to the superb availability of cyber weapons, it is a favourable tool for non-state actors that have ambitious political goals, but poor defences, making covertness essential. Concepts of deterrence may also be at risk, because of the anonymity of cyber. Therefore, as many have argued, unlike, previous revolutionary weapons of warfare, like the atom bomb, which drove international actors further away from war, cyber provides the means for less capable actors, states, and perhaps

[48] Kello, *supra* note 3, at 6.
[49] E. Kovacs, *Maersk Reinstalled 50,000 Computers After NotPetya Attack*, 2018, Security Week (available at https://www.securityweek.com/maersk-reinstalled-50000-computers-after-notpetya-attack).
[50] Nye J., 'Normative Restraints on Cyber Conflict.', 1*Cyber Security Project* (2018), at 11–14.

incentivises them to use cyber warfare for their goals.[51] However, other perspectives are emerging. Theorists have become critical of how truly anonymous cyber is. Rightfully so, as cyber is often utilized by aggressive states, already involved in regional, or other clear-cut political struggles. Even without technical analysis, it possible to suspect the potential perpetrator of cyber-attacks against Ukraine during the ongoing struggles in Crimea and Donbass, or the cyber-attacks sabotaging Iran's nuclear facilities.[52] Evidence is also emerging that cyber may not be as cheap as expected. The accumulative costs of resources, expertise and time can reach high enough, that only states can afford to conduct such attacks. For the purposes of NSAs, bombings, and conventional attacks may remain a more effective tool.[53] Overall, cyber is a complex domain to map. While it certainly has the potential to cause widespread damage, there are also indications that actors may remain a bit restrained for that very reason. While the cost and secrecy seem to proliferate more capacity for malicious actors, there are serious considerations that come with cyber.

Determining whether cyber is a double-edged sword, a revolutionary tool, or even, 'restraint' inducing, may not yet be, entirely possible. It is however clear, that it has been and continues to be used, perhaps more rarely than expected, to cause serious damage to actors in the international arena. While the potential to cause more damage in the future is also present. Therefore, it is essential for cyber to be addressed by international law, in order to provide conditions of expectation, to a domain, that is clearly very difficult to navigate. Law is a tool that can provide some certainty, even to matters, that are by their nature uncertain. The impact of the capacity of cyber will become more apparent in, section 4, when analysing the scope of jus ad bellum laws, as the sources of international law are primarily states, their conceptualization and perceived capacity of cyber will significantly impact the interpretation and formation of international law. As the conceptualization of states, and the potential properties of cyber warfare, have been showcased it now remains to be determined: the legal stances states have taken regarding the application of jus ad bellum and the issues that are emerging. This will be explored in the following section.

[51] Kello, *supra* note 3, at 2–4.
[52] Valeriano and Maness, *supra* note 47, at 46–48.
[53] *Ibid.*, at 51.

4 International law regulating the use of force in cyber warfare

4.1 Jus ad Bellum Issue: Divided interpretation of jus ad bellum applicability

The cyber technological changes in warfare have been at the forefront of the legal debate between states for several decades, at the United Nations. As per VCLT art.31(3)(a) and (b) states' subsequent agreement on interpretation and subsequent practise of application of the law, is crucial to determine in order to show how the jus ad bellum functions in cyber warfare.[54] In 2001, The UN General Assembly (UNGA) initiated the group of governmental experts (GGE) to study the *"Developments in the Field of Information and Telecommunications in the Context of International Security"*, which essentially is a task to determine, via consensus, the exact interpretation and application of international law, and jus ad bellum to cyber.[55] It initially consisted of 15 members, as per para.4 of the resolution, constituting "*equitable geographical distribution"*. The members voiced a preference to determine interpretation themselves, rather than referring the issue to the international law commission, which is tasked to codify the law. The members were notably Russia, China, US, Brazil, and many other western and non-western states.[56] While being criticised for being slow, and not considering key issues, it has held five sessions and produced three consensus reports.[57] The second, a substantive consensus report in 2013, confirmed that international law and specific principles of the UN charter can be applied to cyber.[58] The thirds consensus report in 2015 built further on establishing confidence measures, and accepted certain state responsibility applicability, like preventing the targeting of critical infrastructure, urging to offer assistance in addressing non-state actors and their potential to use cyber to destabilize peace.[59] Analysing the discussion transcripts leading up to the 2013, and 2015 reports, there is almost no mention of concrete jus ad bellum applicability, neither by U.S., U.K., Russia or

[54] United Nations, *supra* note 20.
[55] UN General Assembly Resolution 56/19, UN Doc.A/RES/56/19, January, 2002; UN General Assembly Resolution 58/32, UN Doc. A/RES/58/32, 2003.
[56] Henriksen A., 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace', 5*Journal of Cybersecurity* (2019), at 2–3; United Nations Office for DIssarmament Affairs, *Group of Governmental Experts*, 2020 (available at https://www.un.org/disarmament/group-of-governmental-experts/).
[57] CCDCOE, *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly*, 2017, Nato Ccdcoe (available at https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html).
[58] UN General Assembly Resolution 68/98, UN Doc. A/Res/68/98, 2013.
[59] CCDCOE, *supra* note 57; General Assembly, UN General Assembly Resolution 70/174, UN Doc. A/Res/70/174, 2015; Henriksen, *supra* note 56, at 3.

China. [60] Interestingly, only Egypt, on behalf of the whole Arab league, continuously stressed for the need to apply art.2 (4) to cyberspace.[61] Evidently, the GGE refrained from considering the applicability of jus ad bellum laws to cyber, until the fifth, 2016-2017 session. This session failed to reach consensus on the applicability of the foundational art.2(4) of the UN charter that regulates warfare, by prohibiting the use of force, with specific exceptions in art.51 self-defence and Security council authorization.

The deliberations failed regarding, what the deliberating part termed as paragraph 34 of the consensus document. The draft consensus report is not available to the public, but according to the parties, para.34 aimed to clarify the application of the use of force and self-defence to cyberspace. The disagreement appears to be quite firmly between western and some specific authoritarian non-western countries.[62] Cuba provided an extensive position to the GGE, outlining the fear of militarization of cyberspace, while Russia provided a separate statement via their ministry of foreign affairs. Cuba referred to cyber as Information and communications technology (ICT) and claimed it should be used for betterment of life rather than war. Therefore, they argued that acceptance of the applicability of jus ad bellum to ICT (read: cyber) would convert it into a military arena, drawing in unnecessary military confrontations to ICT incidents. It rejected that ICT can constitute use of force or an armed attack.[63] Russia echoed the same strong sentiments, arguing that there was a *"fundamental political disagreements among the participants concerning their visions of the future of the global information space",* further claiming that they want peace and prevention of an arms race in the information space, urging the UN to remain the primary negotiation arena for separate, new non-use and non-interference principles. This would be based on adopting rules of responsible behaviour of states , based on the shanghai cooperation organisation's cyber code of conduct developed outside of the UN.[64] Russia argues that adopting jus ad bellum

[60] UN General Assembly, UN GAOR, 65th Sess., 1st Comm. 15th Mtg. UN Doc. A/C.1/65/PV.15, 2010; *UN GAOR, 68th Sess., 1st Comm. 20th Mtg. UN Doc. A/C.1/68/PV.20* (2013); United Nations, 'UN GAOR, 69th Sess., 1st Comm. 19th Mtg., UN Doc. A/C.1/69/PV.19', (2014).
[61] UN General Assembly, *supra* note 60, at 27; United Nations, *supra* note 60, at 2.
[62] Delerue F., 'Reinterpretation or Contestation of International Law in Cyberspace?', *Israel Law Review* (2019), at 305.
[63] *Ibid.*, at 307; Representaciones Diplomáticas de Cuba en El Exterior, *Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.*, 2017 (available at http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information).
[64] The Ministry of Foreign Affairs of the Russian Federation, *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere*, 2017 (available at

rules to "information space" (read: cyberspace) is a way of perpetuating conflict and imposing rules tailored for western technological and conventional capacity. Russia here is perhaps referring to the fear of a conventional response, to their cyber operations. It also disapproves of forceful measures, falling below the use of force threshold, such as countermeasures (immediate unlawful non-violent actions in response to unlawful actions), as these would further remove the need for attribution.[65] Russia regards attribution as a major issue of cyber. It claims that there are no means of technical and therefore legal attribution of cyber-attacks, due to the difficulty of technical proof when identifying the perpetrator. Hence Russia believes it may be impossible to apply jus ad bellum laws, as lawfully responding in self-defence requires the identification of the perpetrator.[66] This arguably stems from their conceptualization of cyber as a societal control tool rather than primarily a tool of warfare. They also seem to accept that cyber has the potential to revolutionize warfare due to the inability to attribute attacks.

Russia asserts that there are many states that support their view of the interpretation of international law, and the numerical support behind Russia will be explored later. One of said states is China. China has expressed the wishes of non-militarization of cyberspace early on in 2012, according to the discussion transcripts of the GGE.[67] China hasn't published any official extensive statements on why they disagreed with the consensus document, but reportedly they did reject para.34, regarding the applicability of self-defence, use of force within jus ad bellum.[68] This is expected considering their non-militarization of cyber stance, taken in all of the GGE deliberations leading up to 2017. For the most part, China's *public* cyber strategy is categorized as ultra-pacifist, wanting not much more than total sovereignty within their cyberspace.[69] This arguably stems from their conceptualization of cyber as a pillar of development, while it also seems to believe that the rapid proliferation is a revolutionary

https://coe.mid.ru/en_GB/sotrudnicestvo-v-sfere-pravoporadka/-/asset_publisher/jYpWpmrO5Zpk/content/otvet-specpredstavitela-prezidenta-rossijskoj-federacii-po-voprosam-mezdunarodnogo-sotrudnicestva-v-oblasti-informacionnoj-bezopasnosti-a-v-krutskih-n?inhe); 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 Recent. A/69/723, 2015.

[65] Delerue, *supra* note 62, at 307–308; The Ministry of Foreign Affairs of the Russian Federation, *supra* note 64.

[66] CCDCOE, *supra* note 57.

[67] UN General Assembly, UN GAOR, 67th Sess., 1st Comm. 17th Mtg. UN Doc. A/C.1/67/PV.17, 2012, at 11–12.

[68] Delerue, *supra* note 62, at 309.

[69] CCDCOE, *supra* note 57.

property of cyber. China fears an arms race and militarization of cyber space. They have been critical of the Tallinn manual, considering it a NATO centred legal interpretation meant to ensure dominance of the west in "information space".[70] Overall China tends to avoid voicing strict interpretation of the law, opting to wait out to see the trajectory of cyber development, and perhaps using the legal uncertainties to their advantage.[71] Evidently, Russia, China and other states have taken a very limited interpretation of jus ad bellum laws, and claim they do not apply to cyberspace. This stems from their conceptualization of cyber, first and foremost as a domain of information control and societal transformation. These conceptualizations stem from political considerations. The rejection of jus ad bellum serves to prevent western superior conventional responses to any potential Russian, Chinese cyber operations. While the emphasis on cyber sovereignty, non-militarization, and non-interference in society, serves to maintain stability in their states. Furthermore, if the non-western states did accept the applicability of jus ad bellum, this would indirectly mean that cyber operations outside of jus ad bellum, such as interference, would certainly not constitute force. This is not preferable for Russia, because it is susceptible to interference. With the current predicament, they can lawfully respond to interference with cyber. Maintaining the non-western position would be a two-fold advantage to the emerging global powers: Maintenance of control over their population, while the west cannot respond lawfully to their cyber operations.[72]

Western states, particularly the US have been vocal supporters of GGE consensus para.34 and the applicability of jus ad bellum to cyber. The US department of state statement on the GGE para.34 is the best representation of the western interpretation of the law, it encompasses many of the views of other western states and conveys them in an in-depth manner. The US claims that the consensus report should not have proceeded as is, because it would have produced an unclear legal interpretation of the law, and not fulfil the mandate of the GGE.[73] The US claims that without clear applicability of use of force, self-defence and countermeasures *"States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions. That is a dangerous and unsupportable view."*[74] US representatives made it

[70] Henriksen, *supra* note 56, at 4–5.
[71] *Ibid.*
[72] A. M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, 2017 (available at https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well).
[73] Delerue, *supra* note 62, at 306.
[74] M. G. Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of*

clear that the non-western states' claim that: applying jus ad bellum laws to cyber, in their opinion, goes against the GGE goal of achieving peaceful dispute settlement and conflict prevention in cyberspace, is false. The US, rejects such argumentation, asserting that the UN charter jus ad bellum law can be applied and should be applied in order to provide lawful ways to use self-defence against cyber use of force, with the purpose of constraining, deterring and preventing actors from resorting to conflict.[75] The US therefore continues to maintain that use of force, self-defence, and countermeasure laws apply.[76] This notion is supported by several other, primarily western, more liberal states that participated in the GGE; UK, Germany, Netherlands, Australia, and many other EU nations represented by the EU observer at the deliberations.[77] Though while many of these states argue for the application of jus ad bellum laws, they often apply said laws differently, maintaining some interpretative divide within western countries. This divide is however not particularly major.[78] Evidently, western states adopt a contrary view on the interpretation of the law and its applicability. This stems from western military and security culture, that has now, for decades conceptualised and operationalised cyber as a tool for warfare. Furthermore, the view is political, as western states are some of the most interconnected states in cyber terms.[79]

The two different interpretations of jus ad bellum rely on different conceptions of cyber and cyber warfare. Russia, China and other supportive states have a cyber revolution-based perception, where attribution of cyber-attacks is very difficult, it has the capacity to militarize "information space" and result in far reaching conflict. This can be seen in their state practise, as Russia has denied any attribution of cyber-attacks to states, and does not resort to citing jus

International Security, 2017, United States Department of State (available at https://www.state.gov/explanation-of-position-at-the-conclusion-of-t…rmation-and-telecommunications-in-the-context-of-international-sec/).

[75] *Ibid.*

[76] Delerue, *supra* note 62, at 306.

[77] UN General Assembly, UN GAOR, 72nd Sess., 1st Comm. 19th Mtg. UN Doc. A/C.1/72/PV.19, 2017, at 16,23; UN GAOR, 72nd Sess., 1st Comm. 20th Mtg. UN Doc. A/CA/C.1/72/PV.20, 2017, at 16,20.

[78] For example, divergencies can be seen as France suggests that pre-emptive self-defense may be possible in cyber, while the US is indicating some support for collective countermeasures. Measures that are traditionally unlawful and do not yet have support. For an extensive review, see, A. Väljataga, *Joint Air & Space Power Conference*, 2019, CCDCOE (available at https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf).

[79] Waxman M.C., 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', *Yale Journal of International Law* (2011), at 50–52.

ad bellum laws when justifying or condemning cyber-attacks.[80] Furthermore their conceptualization of cyber as information space primarily linked to societal perceptions, and their strategic interests also bestow them with a different lens when interpreting the law. "Information space" is seen simply as that, information, it can be portrayed as not part of jus ad bellum. On the other hand, the west has a more cyber 'restrained' view, believing that cyber can be regulated, that attribution is to some extent possible, and that international law, particularly jus ad bellum, can serve as an efficient tool in ensuring predictability, and the deterrence against resorting to conflict. This can also be seen in their state practise, multiple states such as the UK, Germany, France and the US have continuously attributed and referred to international law regarding cyber-attacks.[81]

In the light of this major divide, it becomes very difficult to universalise the law, and apply it relatively consistently, when these major legal subjects see cyber as two different matters. This essentially results in a lockdown of international law interpretation and application, leaving states in ambiguity on the appropriate expectations of cyber warfare in international relations. The GGE statements provide opinio juris on what the law is, such statements are necessary for the formation or change in customary law. There are emerging stances that for custom to form or change, opinio juris may suffice, and perhaps it does not need to be widespread and geographically diverse.[82] However, these views are controversial, and this change is unlikely, as the two opposing blocks are equally significant. Furthermore, jus ad bellum laws, particularly the prohibition of the use of force, are peremptory *jus cogens* norms, that cannot be deviated from. They can only be changed by a diverging peremptory norm that has the same universal acceptance, which is not the case in this scenario.[83] It could be argued that Russia and China are deviating from the peremptory norm, which is unlawful. However,

[80] Kello, *supra* note 3, at 3–15; P. Roguski, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, 2020, Just Security (available at https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/).
[81] H. Von Der Burchard, *Merkel Blames Russia for 'Outrageous' Cyberattack on German Parliament*, 2020 (available at https://www.politico.eu/article/merkel-blames-russia-for-outrageous-cyber-attack-on-german-parliament/); National Cyber Security Centre, *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, 2018 (available at https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed); M. R. Pompeo, *The United States Condemns Russian Cyber Attack Against the Country of Georgia*, 2020 (available at https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/); Valeriano and Maness, *supra* note 47, at 45–51; Väljataga, *supra* note 78.
[82] Baker R.R.B., 'Customary International Law in the 21st Century: Old Challenges and New Debates', 21*European Journal of International Law* (2010), at 176–182; Roberts and Sivakumaran, *supra* note 8, at 104.
[83] Shelton, *supra* note 15, at 142.

the positions of western and non-western states also involve interpretative considerations of the relevant law, which can shape legal application more rapidly, because customs take a long time to form and to affirm. Therefore, depending on the validity of the legal basis for the interpretations asserted by these primary makers of international law, more states may eventually voice interpretative agreement with one of the interpretations as per VCLT art.31(3)(a).[84] One interpretation may become dominant and determine how cyber warfare will be conducted, justified and regulated legally, in the future. However, it is crucial to determine whether the interpretations taken by these states do not violate the intended interpretation, scope of the customary laws of jus ad bellum codified in the UN charter. It is also important to establish whether the subsequent practise, as per VCLT art.31(3)(b) of UN charter jus ad bellum laws showcases the applicability to cyber. States, as codified in the VCLT have a jus cogens obligation of *pacta sund servanda*, a customary rule to uphold agreements made in treaties, like the UN Charter. Russia, China and the west technically have a duty to adhere to the established agreement even when new norms emerge. However, there is the obvious difficulty of determining which interpretation is lawful based on the purpose, context, intent and subsequent practise.[85] The following sections will explore the legal basis for both of the interpretations.

4.2 The applicability of article.2 (4) to cyber

The foundation of jus ad bellum is the UN charter, art.2(4) which codifies the customary law of the prohibition of the use of force, in international relations. It is first and foremost essential to deduce whether the prohibition of the use of force applies to cyberspace. In the case that it would not, cyber would be viewed as a domain or a tool that cannot result in grave enough damage to be considered force in international relations. In the same way that the prohibition of the use of force does not apply to international trade law, where tariffs or sanctions, while perhaps seriously damaging, would not constitute use of force. Art. 2(4) is as follows:

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[86]

[84] United Nations, *supra* note 20.
[85] Crootof R., 'Change Without Consent: How Customary International Law Modifies Treaties Rebecca', 41*Yale Journal of International Law* (2016), at 279–284.
[86] United Nations, Charter of the United Nations, Art.2(4), 1945.

The article provides several terms relevant to its potential applicability to cyber. The meaning of term of primary concern is "use of force". It is crucial to determine whether the legal term 'force' could be applicable to cyber. The terms of "territorial integrity or political independence" is also relevant as cyber, unlike conventional weaponry, cyber can circumvent the territorial boundaries as understood in traditional manner. Furthermore, the 'threat' of use of force, is not yet, of significant matter, as no cyber threats have been recorded and may even be impossible due to the covert nature of cyber.[87] Consideration of the applicability of the terms with consistency regarding the purposes of the UN, is also crucial, not only because VCLT art.31(1) deems it so, but because art.2(4) also specifically refers to this.

4.3 Textual meaning of force, and its incorporation of cyber

Applying an objective textual interpretative approach and viewing the term 'force' in its textual meaning does not provide a definitive interpretation. Black's law dictionary has definitions of force, in its basic form, and in legal form. Force in a basic form is defined as "power, violence, or pressure directed against a person or thing".[88] Other legal dictionaries use the same definition supplementing it by adding "*consisting in a physical act"*.[89] Such definition implies that force is physical, therefore not applicable to cyber. In an entirely legal, contemporary national context it is defined as *"Power dynamically considered, that is, in motion or in action; constraining power, compulsion; strength directed to an end. Usually the word occurs in such connections as to show that unlawful or wrongful action is meant".*[90] Evidently, the textual interpretation leads towards an understanding of force as actions, perhaps violent and physical, that compels an actor unlawfully. This however does not reveal the entire meaning of force in the context of the charter, making it very difficult to see whether cyber could fall within its scope. International law dictionaries usually state that force is too difficult to define in strict terms.[91] Therefore the term must be viewed in a teleological manner, with consideration of its context, purposes and subsequent practise. The term's meaning may

[87] Fraser A., 'From the Kalashnikov to the Keyboard: International Law's Failure to Define a 'Cyber Use of Force' Is Dangerous and May Lead to a Military Response to a 'Cyber Use of Force'', 15*Hibernian Law Journal* (2016).
[88] Roscini M. 'Cyber Operations and the Jus Ad Bellum', in *Cyber Operations and the Use of Force in International Law* (2014) , at 45.
[89] Duhaime's Law Dictionary, *Physical Force Definition*, 2020 (available at http://www.duhaime.org/LegalDictionary/P/PhysicalForce.aspx).
[90] Black's Law Dictionary, *What Is Force?* (available at https://thelawdictionary.org/force/).
[91] Grant J.P., Barker J.C. and Parry C., *Parry and Grant Encyclopaedic Dictionary of International Law* (2009), at 222.

also need to be ascribed relying on the definitions stemming from the *travaux préparatoires*.

4.4 Art.2(4) and the context of the UN Charter Chapter VII and preamble

As per VCLT art.31(1) considering the art.2(4) in the context of the whole UN charter also provides additional clarification on the meaning of 'force'. The unqualified term 'force' is mentioned only twice in the charter. It, however, is qualified in art.41 and 44, as armed force, meaning conventional, not cyber, weaponry. It refers to it in the UN Charter chapter VII context, that provides exceptions to the prohibition of force. Art.41 deals with measures not involving *armed force*. Firstly, it specifically refers to force as armed, and essentially lays out exactly what is not armed 'force', such as severance of diplomatic or economic relations. Cyber is of course not mentioned. If said measures fail, Art.42 lays out the instances of 'force' that can be used. Those would primarily take shape in armed operations, by land, air and sea. Art.44 specifies that if the Security Council sanctions *force* as outlined in art.42, states are can carry out such force, with their armed forces. This suggests that 'force' should be seen as armed force.[92] Arguably, these qualified references to 'force', could be construed as meaning 'armed force' only in those specific instances, while the unspecified term 'force' in art. 2(4) is meant to be broader, to address future developments in warfare, like cyber. However applying a thorough teleological interpretation, one must consider the preamble of the charter, which delineates the purpose of the charter, and specifically references armed force, when specifying the U.N. end goal as "*to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used*".[93] Evidently, when considering the preamble and the context of the charter, there is support for the notion that 'force' refers to conventional kinetic armed force. This however does not settle the matter, as subsequent practise of the agreement regarding interpretation of terms and its application also need to be considered.[94]

[92] Harrison Dinniss H., *Computer Network Attacks as a Use of Force in International Law* (2012), Cyberwarfare and the Laws of War, at 41–42; Huntley T.C., 'Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare', 60*Naval Law Review* (2010), at 17–18; United Nations, *supra* note 12.
[93] Harrison Dinniss, *supra* note 92, at 42; Roscini, *supra* note 88, at 45; United Nations, Charter of the United Nations, Preamble Para. 7, 1945.
[94] United Nations, *supra* note 20.

4.5 Art.2(4) and subsequent practice

VCLT art.31(3)(a) and (b) emphasises the importance to consider subsequent practise, in the interpretation of terms. While it is evident that the term 'force' originally referred to armed forces and would render the current prohibition of force inapplicable to cyber, there is no denial that ambiguities have developed over the decades after the signing of the charter. The clash over interpretation was particularly apparent during the Cold War. Three main interpretation had emerged. More authoritarian states had proposed on several occasions that force should be viewed as interference, where violation of sovereignty should constitute force. They suggested that instigating civil strife in another country should constitute force. This would expand the scope of force to non-kinetic actions, like propaganda, subversion. However, this is further from the original meaning of the term 'force' than even cyber-attacks, and did not gain any traction.[95] Furthermore, many former colonial states argued for a force as coercion interpretation, that views economic and political coercion as 'force'. If this notion was accepted, the scope of the prohibition would be more likely to include cyber, because economic coercion is also non-kinetic. It was however not accepted, as it would make the scope too broad, as there would remain little means and distinction between lawful and unlawful pressure.[96] The dominant interpretative practise during the 20th century was that 'force' is armed force view. Until very recently, western states have continuously promulgated that the interpretation that art.2(4) applies to armed force only. Other sceptical states have at least occasionally applied the prohibition in that manner.[97] This was particularly shown in the drafting negotiations of the declaration on friendly relations. The declaration referred to restraint of utilizing irregular forces and armed bands as force but did not acknowledge the proposition of USSR that states should restrain from utilizing economic coercion as force.[98] Furthermore the declaration on the definition of aggression, the declaration on the non-use of force, offered more evidence for art.2(4) scope as limited to armed force.[99] Therefore there is

[95] International Law Commission 'Summary Records of the Second Session, A/CN.4/SER.A/1950', in *Yearbook of the International Law Commission* vol. 1 (1950) , at 123; Special Rapporteur, Draft Code of Offences against the Peace and Security of Mankind, A/CN.4/25 Draft, vol. 2, 1950, p. 277; Waxman, *supra* note 79, at 429–430.
[96] Harrison Dinniss, *supra* note 92, at 43; Waxman, *supra* note 79, at 428–429.
[97] Fraser, *supra* note 87, at 90; Waxman, *supra* note 79, at 427.
[98] Harrison Dinniss, *supra* note 92, at 46–47; Kittichaisaree K., *Public International Law of Cyberspace* (2017), at 162; UN General Assembly, UN General Assembly Resolution 26/25, UN Doc. A/Res/26/25 'Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations', 1970.
[99] Fraser, *supra* note 87, at 91; Roscini, *supra* note 88, at 46.

sound basis to suggest that state practise until the 21st century deems the interpretation ofart.2(4) not applicable to non-kinetic coercion or force.

The subsequent state practise of interpretation and application of the terms, as per VCLT art.31(3)(a) and art.31(3)(b), however has been developing to extent. Despite the long-standing interpretation of force as armed force, states have been adapting their interpretation as cyber and their conceptualizations of it emerged. The figures bellow outlines a review of state practise, that encompasses all of the countries that are, or have been part of the GGE in the past. As the GGE member were chosen with the purpose of equitable geographical distribution, this should form a sample of that nature.[100] Figure 2. showcases the states that have either explicitly or implicitly endorsed the application of jus ad bellum to cyber. Explicit endorsement would constitute a direct statement by a governmental organ that art.2(4) and art.51 are applicable to cyber, or a statement classifying a cyber action in international relations as use of force. An implicit endorsement would be a statement of acceptance of jus ad bellum indirectly by a designated representative such as EU or other regional organization. It could also be a statement rejecting the creation of new norms and instead applying the UN charter in its entirety, without referring to art.2(4) specifically. Figure 3. showcase explicit and implicit objections to application of jus ad bellum. Explicit objection to the applicability of jus ad bellum to cyber, would constitute the statements specifying exactly that. An implicit objected was considered to be, a refusal to mention any jus ad bellum laws or principles, in combination with a demand for entirely new norms. This is certainly not a conclusive study of state practise and subsequent interpretation, as that is beyond the scope of this thesis. Furthermore, there is a level of nuance involved in the determination of endorsement, as states favour silence until more solid conclusions can be drawn from cyber warfare. Most states used the platform provided by GGE and conducted hearings to express their views.

Figure 2. Explicit or implicit endorsement		
Country	Application of jus ad bellum to cyber	Comment/Clarification of stance
Australia	Explicit endorsement[101]	Art.2(4) applies to cyber
Canada	Implicit endorsement[102]	Rejected 2017 proposed consensus

[100] UN General Assembly Resolution 56/19, *supra* note 55.
[101] Ministry of Defence, *Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace*, 2018 (available at https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html).
[102] General Assembly, 'A/C.1/73/PV.31', (2018), at 14–16.

Egypt	Explicit endorsement[103]	Art.2(4) applies to cyber
Estonia	Explicit endorsement[104]	Rejected 2017 proposed consensus
Finland	Explicit endorsement[105]	Cyber can reach armed attack threshold and bellow
France	Explicit Endorsement[106]	Art.2(4) applies to cyber
Germany	Explicit Endorsement[107]	Art.2(4) applies to cyber
Israel	Ambiguous case	Lack clear position, supports the west
Italy	Implicit Endorsement[108]	Represented by the EU. Art.2(4) and art.51 apply
Japan	Implicit endorsement [109]	Supports interpretation of applicability
Jordan	Implicit endorsement[110]	Art.2(4) applies to cyber
Morocco	Implicit endorsement[111]	Art.2(4) applies to cyber
Netherlands	Explicit endorsement[112]	Art.2(4) applies to cyber
Norway	Implicit endorsement[113]	Rejected 2017 proposed consensus
Qatar	Implicit endorsement[114]	Article 2.4. applies to cyber
Romania	Implicit Endorsement[115]	Represented by the EU in GGE. Art.2(4) and art.51 apply
Serbia	Implicit Endorsement[116]	Represented by the EU in GGE. Art.2(4) and art.51 apply
Spain	Implicit Endorsement[117]	Represented by the EU in GGE. Art.2(4) and art.51 apply
South Korea	Implicit endorsement[118]	Referenced use of force applicability
Switzerland	Explicit endorsement[119]	Art.2(4) and art.51 apply to cyber
UK	Explicit Endorsement[120]	Art.2(4) and art.51 apply in its entirety
US	Explicit Endorsement[121]	Art.2(4) and art.51 apply in its entirety

[103] United Nations, *supra* note 60, at 2–3.
[104] General Assembly, *supra* note 102, at 14–16; *President of the Republic at the Opening of CyCon 2019*, 2019 (available at https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/).
[105] UN General Assembly, *supra* note 77, at 10–11.
[106] Ministère des Armées, *International Law Applied to Operations in Cyberspace* (2019).
[107] German Parliament, *Antwort Der Bundesregierung Auf Die Kleine Anfrage Der Abgeordneten Stephan Thomae, Jimmy Schulz, Manuel Höferlin, Weiterer Abgeordneter Und Der Fraktion Der FDP* (2018).
[108] UN General Assembly, *supra* note 77, at 15–16.
[109] Ministry of Defence, *Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group* (2015).
[110] United Nations, *supra* note 60, at 2–3.
[111] *Ibid.*
[112] General Assembly, *supra* note 102, at 14–16; Ministry of Defence, *Diplomacy and Defense in Cyber Space*, 2018 (available at https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/).
[113] General Assembly, *supra* note 102, at 14–16.
[114] United Nations, *supra* note 60, at 2–3.
[115] UN General Assembly, *supra* note 77, at 15–16.
[116] *Ibid.*
[117] *Ibid.*
[118] United Nations, UN GAOR, 73rd Sess., 1st Comm. 19th Mtg. UN Doc. A/CA/C.1/73/PV.19, 2018, pp. 20–21.
[119] UN General Assembly, *supra* note 77, at 18–19.
[120] UN General Assembly, *supra* note 77, at 10–11.
[121] Markoff, *supra* note 74.

Figure 3. Explicit or implicit objection		
Country	Application of jus ad bellum to cyber	Comment/Clarification of stance
Argentina	Implicit objection[122]	Represented by UNASUR in GGE. UN charter applies, but need new non-first-use binding norms
Belarus	Implicit objection[123]	Wants new norms, inclusive deliberations
Botswana	Implicit objection[124]	Represented by movement of non-aligned countries (NAM) in GGE. Want the development of new norms to preserve peace
Brazil	Implicit objection[125]	Need for new norms
China	Explicit objection[126]	Non militarization of cyber
Colombia	Implicit objection[127]	Represented by UNASUR. UN charter applies, but need new non-first-use binding norms
Cuba	Explicit Objection[128]	Jus ad bellum does not apply
Ghana	Implicit objection[129]	Represented by NAM. Want development of new norms to preserve peace
India	Implicit objection[130]	Ambiguous case
Indonesia	Implicit objection[131]	Wants new norms
Kazakhstan	Explicit objection[132]	Rejects applicability, wants new norms
Kenya	Implicit objection[133]	Represented by NAM in GGE. Want development of new norms to preserve peace
Malaysia	Implicit objection[134]	Represented by NAM. Want development of new norms to preserve peace
Mauritius	Implicit objection[135]	New norms
Mali	Implicit objection[136]	New norms
Mexico	Implicit objection[137]	Peaceful use of cyber for development

[122] United Nations, UN GAOR, 71st Sess., 1st Comm. 19th Mtg. UN Doc. A/C.1/71/PV.19, 2016, pp. 11–12.
[123] General Assembly, *supra* note 102, at 22.
[124] UN General Assembly, *supra* note 77, at 13.
[125] *Ibid.*, at 22.
[126] UN General Assembly, *supra* note 67, at 11–12.
[127] United Nations, *supra* note 122, at 11–12.
[128] Delerue, *supra* note 62, at 307; Representaciones Diplomáticas de Cuba en El Exterior, *supra* note 63.
[129] UN General Assembly, *supra* note 77, at 13.
[130] P. W. Mehta, *India's National Cybersecurity Policy Must Acknowledge Modern Realities*, 2019 (available at https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/).
[131] General Assembly, 'A/C.1/73/PV.22', , at 15.
[132] UN General Assembly, *supra* note 64.
[133] UN General Assembly, *supra* note 77, at 13.
[134] *Ibid.*
[135] *Ibid.*
[136] *Ibid.*
[137] UN General Assembly, *supra* note 77, at 20.

Pakistan	Implicit objection[138]	Ambiguous statements
Russia	Explicit Objection[139]	Rejected art.2(4) and art.51 applicability
Senegal	Implicit objection[140]	New norms and peace
Singapore	Implicit objection[141]	Ambiguous statements, no reference to jus ad bellum
South Africa	Implicit objection[142]	New norms and peace
Uruguay	Implicit objection[143]	New norms and peace

Figure 2. and figure 3. showcase that the subsequent agreement on interpretation and subsequent practice in application of the UN Charter and jus ad bellum international law, remains divided. The international law commission tasked with the study of interpretation of the law conducted multiple reports on subsequent agreements and subsequent practice of interpretation. In para.115 of the first report, the special rapporteur emphasises that it is very difficult to determine practise and argued that *agreement,* as per VCLT art.31(3)(a) regarding interpretation should be most important.[144] Evidently, there is little agreement between the parties of the UN Charter. In the second report, the ILC outlined in para.19 that subsequent practice itself should be interpreted very carefully, with concern as to whether the parties are attempting to interpret the terms, or are instead motivated by other considerations.[145] This perhaps is a significant nuance, however both western and non-western states have additional conceptual and political considerations when interpreting art.2(4). Furthermore, the ILC also drew attention, in para.39 to the importance of specificity when considering subsequent practise.[146] The wests position is perhaps more explicit, but the explicitness is mostly confined within Europe and the US. In terms of specificity, non-western states have basis considering that 'force' has been historically interpreted as armed force. However as seen in the GGE, their legal arguments rarely refer to the specifics of the UN charter, or other legal use of force concepts. Often those states simply demand non-militarization and use political arguments claiming malicious intent by the west. The western interpretation is somewhat more specific,

[138] UN General Assembly, *supra* note 77, at 13.
[139] The Ministry of Foreign Affairs of the Russian Federation, *supra* note 64.
[140] UN General Assembly, *supra* note 77, at 13.
[141] *Ibid.*
[142] *Ibid.*
[143] United Nations, *supra* note 122, at 11–12.
[144] International Law Commission, First Report on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties, UN Doc. A/CN.4/660, 2013, p. 74.
[145] International Law Commission, Second Report on Subsequent Agreements and Subsequent Practice, UN Doc. A/CN.4/671, 2014, p. 11.
[146] *Ibid.*, at 18.

as some of the states have provided extensive statements on how jus ad bellum could be applied.[147] It could also be argued that for opinio juris could accepted custom, it has to be geographically diverse, consistent, and not objected to by other states.[148] Evidently the both sides are geographically diverse, but perhaps the western states are a bit more consistent. Both blocs also object to each other others interpretation, hence it cannot be accepted the way other modern customs comes into existence. There's also a controversial argument that specially affected states should be given special consideration in determining the content of customary law, as exemplified in the ICJ North Sea Continental Shelf Case, para.74.[149] It is difficult to determine if any states can be specially affected as cyber is so ingrained into most societies. Analysing records of attacks, it is evident that most affect states are in fact US, UK, Russia, China.[150]

This appears to be a difficult interpretative disagreement to resolve, as states have vastly different views. Perhaps so vastly, that it should be considered whether states are attempting to modify the treaty, rather than reinterpret. Subsequent practise cannot modify a treaty, meaning that it cannot assign such interpretation that would not be consistent with the purpose, object and the preparatory work of the law.[151] Therefore, in light of this, it warrants a further analysis of the preparatory work, and object of the UN Charter, in relation to art.2(4).

4.6 *Travaux préparatoires* of article 2(4) and the meaning of force

As subsequent practise of interpretation is divided, it becomes essential to determine the intended meaning of 'force' to deduce whether future warfare, such as cyber has been envisioned to be within the scope of the article. Considering the preparatory work, it appears that the signatories continuously rejected any deviation from defining 'force' as anything else

[147] Attorney General's Office, *Cyber and International Law in the 21st Century*, 2018; H. H. Koh, *International Law in Cyberspace*, 2012, U.S. Department of State Diplomacy in Action (available at https://2009-2017.state.gov/s/l/releases/remarks/197924.htm).
[148] Roberts and Sivakumaran, *supra* note 8, at 104–105; Thirlway H. 'The Sources of International Law', in M. Evans (ed.), *International Law* 4th (2014) , at 98–99.
[149] International Court of Justice, North Sea Continental Shelf Cases, Judgement, 20 February 1969; Roberts and Sivakumaran, *supra* note 8, at 95.
[150] Cyber Security Insiders, *List of Countries Which Are Most Vulnerable to Cyber Attacks*, 2020 (available at https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/); Kaspersky, *Cyberthreat Real-Time Map*, 2020 (available at https://cybermap.kaspersky.com/stats/).
[151] Moloo R., 'Changing Times, Changing Obligations? The Interpretation of Treaties over Time', 106*American Society of International Law* (2012), at 263.

than armed force. As the charter itself does not define 'force', it is to no surprise that the preparatory work also does not include a specific discussion of the exact meaning of the term.[152] However, as art.2(4) was perhaps the most significant article, the debate surrounding the proposed amendments sheds light on the perception of the states as to what the scope of it should be.[153] In the preparatory work, New Zealand proposed an amendment to art.2(4) to include, a sub-paragraph (4a), that *"All members of the Organization undertake collectively to resist every act of aggression against any member"*.[154] This amendment referred to 'aggression' rather than force, which resulted in a debate, culminating in a rejection. U.K. representative argued that the term 'aggression' is undefined, unclear, while the meaning of 'force' is *explicit*. This indicates that states at the time were certain of the meaning of force.[155] This meaning is often argued to be armed force, which would be in alignment with the customary roots of the prohibition of force stemming from the league of nations and the Kellogg-Briand pact that referred to outlawing *wars* of aggression, which at the time were entirely kinetic and conventional.[156] The formation of NATO also took place shortly after the creation of the charter. The NATO treaty used the same terminology of 'force', with no mention of economic or political coercion. NATO being a collective security alliance aimed at defence against wars, it indicates that 'force' was seen as armed force at the time.[157]

Furthermore, preparatory work also contains the participating Brazilian foreign minister's proposal to amend the article in order to include 'economic measures' in the prohibition of force, which was staunchly rejected.[158] Most scholars argue that this showcases that as economic coercion is excluded from the article, it means that the word 'force' only applies to armed, kinetic, conventional force.[159] This would constitute that the art.2(4), at least in its original intent, is only applicable to armed force; excluding cyber or other non-kinetic force.[160]

---

[152] Ruys T., 'The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are "Minimal Uses of Force Excluded from UN Charter Article 2(4)?', 108*The American Journal of International Law* (2014), at 163.
[153] Harrison Dinniss, *supra* note 92, at 43.
[154] *Summary Report of Twelfth Meeting of Committee I/1* (1945), Documents of the United Nations Conference on International Organization, at 342–343.
[155] *Addendum to Summary Report of Twelfth Meeting of Committee I/1* (1945), Documents of the United Nations Conference on International Organization, at 356.
[156] Harrison Dinniss, *supra* note 92, at 45.
[157] *Ibid.*, at 46.
[158] 'Summary Report of Eleventh Meeting of Committee I/1', in *Documents of the United Nations Conference on International Organization* vol. 6 (1945) , at 334, 559.
[159] Roscini, *supra* note 88, at 45.
[160] Ruys, *supra* note 152, at 163.

Some, however, counter that this could also indicate that the term 'force', at the time, could be thought to already include economic coercion, hence not requiring a specification.[161] This ambiguity would not follow the state perception at the time, and as subsequent practice of interpretation rejected economic coercion as part of the art.2(4) scope. Overall, it is evident that the rejected amendments indicate a support for a scope of art.2(4) that refers to armed force.

4.7 Jus ad Bellum Issue: Narrow interpretation of art.2(4) renders current prohibition of force inapplicable to cyber

Evidently, because the state subsequent interpretation is split, reviewing the preparatory work, a narrow interpretation has some basis in international law for a narrow interpretation that limits the customary prohibition codified in art.2(4) to armed force, and hence conventional weaponry and kinetic attacks. If such interpretation continues to gain ground, if more states accept it forming a solid majority, then it could leave an unregulated space. Wherein states and other actors, potentially have the cyber means to cause significant damage to other states, while the victim state has no lawful argumentation for condemning, or lawfully responding to said state via jus ad bellum. The damage done via cyber could potentially reach as high levels as a conventional attack, while remaining not use of force. Envision a malware that permanently melts down the operating microchips of jet plane fleet in the air, causing them to crash. This is akin to a conventional surface to air missile. But in the case of a narrow interpretation, the attack was a non-kinetic set of numbers that caused a malfunction, that could have been patched if detected.[162] There are other international laws such as state responsibility, non-intervention, that would be violated and give legal grounds for the victim seek resolution.[163] However, technically it could not lawfully respond with conventional forces in self-defence. Russia, Cuba, China appear to be leaning towards such an interpretation of the law of jus ad bellum, asserting that art.2(4) does not apply to cyber operations in its entirety. They support the traditional interpretation that art.2(4) applies to conventional armed forces and are setting a wide-reaching precedent that this does not include cyber.

[161] Harrison Dinniss, *supra* note 92, at 44.
[162] Kello, *supra* note 3, at 2.
[163] Haataja S., *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics* (1st ed., 2018), at 4–6.

While the states promoting such interpretation are key players in the international legal arena, it does not, yet, constitute an accepted norm. Jan Klabbers captures the process of interpretation superbly, stating that *"[t]he meaning of a treaty is not carved in stone at the moment of its conclusion: instead, debates continue, albeit no longer on what words to use in the treaty, but on how to give meaning to the words that are used. Whoever controls this process controls the meaning of the treaty, and therewith controls whether or not the obligations resting upon him are bearable or onerous, and controls whether the acts of States are faithful implementations of a text, or amount to breaches of that same text."*.[164] For such norm to be accepted, it has to stem from a negotiated outcome, often riddled with politics and power struggles, over establishing an argument based on reference to state practise and credible authority.[165] Interpretation can sometimes be less about finding the thorough, representative meaning of the law in the text, but rather finding and establishing what one believes is clearly, already there. That does not mean that any view is acceptable, because sources, and the support of other actors remains a check on the process.[166] Arguably Russia and China are on their way in achieving some of these criteria, as they have the political standing to take such an interpretative stand, have support of some states, and state subsequent practise can be referenced to their advantage. No states have so far declared a particular cyber-attack to be use of force, at most they have attributed cyber interference to a state. Therefore, in light of this issue, it warrants a further analysis of the *purposes* UN Charter, in relation to art.2(4). Furthermore, the interpretation of international courts may be the decisive in the legitimation of certain application or certain interpretations, by clarifying customary law that could allow the application if jus ad bellum to cyber.[167]

4.8 Art.2(4) in the light of its purpose, reinstating the teleological view

The subsequent practise is entrenched and divided. Reviewing the rejection of the variety of interpretations of 'force', and the perseverance of a narrow interpretation of art.2(4), it remains difficult to directly assume a full application of the prohibition of force to cyber operations,

[164] Ingo Venzke, *How Interpretation Makes International Law - On Semantic Change and Normative Twists* (2012), at 4.
[165] *Ibid.*, at 18–19.
[166] *Ibid.*, at 55; Paine J., *Book Review of 'How Interpretation Makes International Law: On Semantic Change and Normative Twists'* (2013), Australian Yearbook of International Law, at 121.
[167] Ingo Venzke, *supra* note 164, at 146–147.

in the exact same way it applies to armed force. However, the lacking interpretative legal basis for a direct scope of application, does not mean a dead end, or a victory for Russia and China. Interpreting the purpose of the UN charter, and customary law identified by jurisprudence, would provide legal basis for the western state interpretation. Interpretational changes have occurred in the past, and the charter has also been undeniably designed to be able to adapt. While signatories may have rejected the extension of the prohibition of force to economic coercion, it was made clear that the charters scope can be expanded regarding other areas. Returning to preparatory work, it has been stated that regarding art.2(4) the *"intention of the authors of the original text was to state in the broadest terms an absolute all-inclusive prohibition; the phrase 'or in any other manner' was designed to insure that there should be no loopholes"*.[168] The purpose of the charter itself, as in the preamble, is to save future generations from the scourge of war, and it can be argued that cyber can certainly be used in war, spark wars, and cause overwhelming damage.[169] However to make matters more ambiguous one could also argue that the purpose of saving future generations from war, actually proves that, that the Charter and art.2(4) outlawing armed force and conflict rather than all coercion, because at the time of its creation war was widely understood as armed force.[170] Particularly considering VCLT art. 31 para.1, that stresses the importance of the context of the treaty. However, in regard to VCLT art. 31 para.3 subsequent practise of interpretation must also be considered. Such matters have been particularly clarified in recent advisory opinions, which are not law, but clarify interpretation. The international court of justice's (ICJ) advisory opinion on the legality of the threat or use of nuclear weapons, clarified that the UN charter prohibition of the use of force applies regardless of the weapon employed.[171] While this doesn't indicate any thresholds or other criteria, it does indicate that if cyber may be regarded as a weapon and produced forceful effect, it is within the scope of the prohibition. This, to some extent, challenges the strict interpretation, that art.2(4) only applies to armed, or conventional, force.[172] Overall, Venzke's and Klabber's noted struggle for the interpretation of law, is very much exemplified here.[173] Therefore, a study of the case law by the ICJ may reveal further interpretative nuances and identification of customary law regarding the applicability of the prohibition of force to cyber operations.

[168] Ruys, *supra* note 152, at 164; , *supra* note 158, at 334–335.
[169] United Nations, *Charter of the United Nations, Preamble Para.1* (1945).
[170] Fraser, *supra* note 87, at 90–92.
[171] The International Court of Justice, *supra* note 19, at 39.
[172] Kittichaisaree, *supra* note 98, at 163.
[173] Ingo Venzke, *supra* note 164, at 4.

4.9 International court of justice, case law and the applicability of art.2(4)

4.9.1 Scale and Effects in "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)" ICJ case

The ICJ Nicaragua case was very revelatory, clarifying certain aspects of the meaning and scope of force as per art.2(4). It can be construed that in a way, the ICJ Nicaragua case strengthen the interpretation that the scope of 'force' is only applicable to armed force. In the case, Nicaragua proposed that the US partook in economic coercion against it. While Nicaragua did not pursue this as part of their main argument, the ICJ chose not to discuss economic coercion when considering art.2(4) violations and the context of the declaration of friendly relations. It referred to the declaration's statements about armed bands, but not economic coercion, indirectly indicating that the court does not believe the measures to be within the scope of 'force' and respective customary law. The judges however argued that they cannot consider an aspect of the case that is not appropriately pursued by Nicaragua.[174] However where the ICJ did consider the declaration on friendly relations, it presented a new codification of the interpretation regarding use of force customary law. Firstly, in para. 191 the court asserts that states acceptance of the declaration shows that they accept the notion that there are lesser forms and graver forms of force, particularly when distinguishing between an art.51 armed attack (the gravest form of attack against a state, warranting lawful self-defence) and general art.2(4) use of force.[175] The court proceeds in para.195 to affirm that the way to distinguish, what they ambiguously term *action by armed forces*, in addition to other criteria, has to rise to certain level, based on its *scale and effects*, to be considered an armed attack or a use of force.[176] This arguably offers a shift in categorization of force, and introduces a notion that focuses on the primacy of the consequences, as a determinant of 'force'. This is also supported further, when the court in para.195 interprets art.2(4) in a broader manner, ruling that *"assistance to rebels in the form of the provision of weapons or logistical or other support"* may be considered as use of force.[177]

[174] Harrison Dinniss, *supra* note 92, at 48.
[175] International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, 27 June 1986, p. para.191; Ruys, *supra* note 152, at 165.
[176] International Court of Justice, *supra* note 175, at para.195; Kittichaisaree, *supra* note 98, at 167.
[177] Huntley, *supra* note 92, at 16–17; International Court of Justice, *supra* note 175, at para.195; Ruys, *supra* note 152, at 166.

This ICJ case therefore forms the foundational legal basis for applicability of art.2(4) and the customary prohibition of the use of force to cyber warfare. The scale and effects approach has also been reaffirmed in other cases.[178] Most lawyers, particularly those from the west, regard the scale and effects to be the legitimate legal framework of applying art.2(4) to cyber operations and attacks.[179] Meaning that as long as a cyber-attacks damage is comparable to the *scale* and *effects* of a kinetic attack, it may constitute use of force.[180] Legal experts have taken that ICJ Nicaragua scale and effects approach as a gateway to applying to jus ad bellum law to cyber, because ICJ has the authority to identify and apply the law. The Tallinn Manual presents a thorough model of how the law would apply via scale and effects, which represents the view of many western states. Cases of inconvenience, where cyber operations restrict access to digital systems, would not constitute force, as there are no kinetic effects. However damaging infrastructure or materials with the scale of a kinetic attack would be use of force. Following from ICJ Nicaragua judgements, arming hacktivist groups that proceed to inflict cyber-attacks with kinetic effects, would also constitute use of force. While harbouring actors that utilize cyber in most cases would not be use of force, but certainly a violation of due diligence. Such application appears reasonable and resembles the application of the law to conventional means. It also renders a large portion of the jus ad bellum law sufficiently applicable.[181]

4.7 Jus ad Bellum Issue: If art.2(4) is applicable, it still does not cover non-kinetic attacks

Applying the ICJ established scales and effects framework does not encompass the entirety of the properties of cyber. Certain particularly damaging capacities of cyber would remain unregulated. Firstly, orders of effects, meaning, the consequences that are started by cyber-attacks but have been caused highly indirectly through a chain of events that is not necessarily possible considering conventional force. Primarily this concerns non-kinetic disturbance of critical infrastructure that are aimed to cause inconvenience but over time result in death. For

[178] International Court of Justice, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, 19 December 2005, paras.146,147.
[179] Boer L.J.M., 'Restating the Law 'As It Is': On the Tallinn Manual and the Use of Force in Cyberspace', 5*Amsterdam Law Forum* (2013), at 10.
[180] Roscini, *supra* note 88, at 46–48.
[181] Schmitt M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., 2017), at 328–332.

example, a cyber-attack against a drinking water cleaning facility, that halts water purification. This causes inconvenience, but also results in deaths.[182] A more extreme example could be an attack on a stock exchange, central back or financial institutions rendering them inoperable, causing panic, which brings about a targeted downturn in a state. At first sight this does not showcase any kinetic effects, and the scale arguably is only that of the attack on the institution. The overall consequences themselves, while broad, are not comparable to conventional attacks, per se.[183]

Several jus ad bellum issues have emerged. Firstly, the interpretation is strictly divided. The context, the preparatory work of the UN Charter, indicate that art.2(4) was not intended to be applied to cyber, and in such a narrow interpretation would leave an unregulated space. On the other hand, the purpose of the UN Charter and jurisprudence of its organs, indicate legal basis for the western interpretation of the applicability of art.2(4) to cyber. Such interpretation poses issues when applying art.2(4) to non-kinetic effects, but the law could still be applied in some manner consistent with the purposes of the UN charter. It is also essential to determine the applicability of self-defence which is an equally significant part of jus ad bellum laws.

5. International law regulating self-defence in cyber warfare

5.1 Determining whether cyber operations can constitute an armed attack warranting self-defence

Self-defence is part of customary law, a right that is codified in art.51 of the UN charter. It is one of the exceptions to the prohibition of the use of force, hence it is part of the jus ad bellum laws. Art.51 is as follows:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the

[182] Huntley, *supra* note 92, at 35; Roscini, *supra* note 88, at 76–77; Schmitt, *supra* note 181, at 343.
[183] Haataja, *supra* note 163, at 5–6.

Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."[184]

The terms of primary concern are 'inherent right' and 'armed attack'. The rest of the article deals with other legal duties the defending state has to the UN and particularly the security council. The art.51 exception in itself has sparked debates recently over its application to conventional warfare, therefore it is likely the application to cyber will at the very least encounter the same problems, but those may be exacerbated.[185] Furthermore, jurisprudence has outlined extensive criteria for art.51, which all need to be reasonably applied to cyber. For a use of force against a state to rise to an 'armed attack' it needs to meet certain criteria. It has to reach a certain damage threshold and as of, yet it has to be attributed. Overall the self-defense measures need to be necessary and proportional. The following sections will consider the applicability of these criteria to cyber, and any issues that are emerging.

5.2 Art.51 and armed attack cyber damage threshold

5.2.1 Damage threshold in *"Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)"* ICJ case

As showcased previously, in ICJ Nicaragua it has been justified, in para.191, there are lesser and graver form of attacks. The most grave would constitute an armed attack as per art.51. Meaning that a use of force needs to first and foremost rise to a grave threshold to constitute an attack against which self-defence can be used. In para.195 the court restates the general agreement on what may constitute an armed attack. Its criteria are drawn from the definition of aggression, and deem an armed attack as *"action by regular armed forces across an international border"* as well as *"the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein".* The scale and effects framework as justified in the ICJ Nicaragua case in para.195 is not only the framework used by western lawyers to apply the law to cyber operations, but it is also used to judge whether a use of force has reached that threshold of an armed attack in general. Para.195 also declares that *"It is also clear that*

[184] United Nations, Charter of the United Nations, Art.51, 1945.
[185] Korošec T. and Veber M.T., 'Right to Self-Defence against Non-State Actors in the Context of Fight against Terrorism', 76*Zbornik Znanstvenih Razprav* (2016), at 65–68.

it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked".[186] Determining the graveness of an attack sufficient to be an 'armed attack' is difficult and often is based on political decision and post-facto judicial interpretations.[187] In the case the US claimed to have come to the aid of El Salvador, by using collective self-defence. However, in para.232 this was judged as unlawful, on the basis that El Salvador at no point claimed that the Nicaragua's aid to insurgents in El Salvador is an armed attack. This highlights that the judgement of the gravity of an attack is retained by the states, and subject to judicial scrutiny and the definition above. In para.247, the ICJ also shows that arming and financing insurgent groups is not grave enough to constitute an armed attack. Overall it is evident that for a cyber-attack to constitute an armed attack, it has to reach a, relatively subjective, threshold of gravity that at a minimum is equivalent, via scales and effects, to the gravity of an armed attack conducted by regular forces. The gravity itself is judged by the state, and to some extent the international community.

5.2.2 Damage threshold accumulation in *"Oil Platforms (Islamic Republic of Iran v. United States of America)*

The case concerned the US retaliatory attacks against Iran's oil platforms, which were accused of being used as mining stations. Several US allied ships and the U.S. frigate Samuel B. Roberts struck mines. Therefore the U.S., in the case brought against in by Iran in the ICJ, argued that the damage inflicted upon the US constituted an armed attack, and the actions taken against oil platforms, constituted self-defence.[188] This case is significant because in para.64 it affirms that the damage threshold could potentially be reached by an accumulation of a series of attacks, rather than exclusively by single grave attacks.[189] That is because the ICJ considered the multiple incidences against the U.S. as perhaps constituting an armed attack in a cumulative manner. While in this case it was rejected on the grounds, that the force was not grave enough or the perpetrators were unclear, it reaffirms that attacks can be

[186] International Court of Justice, *supra* note 175, at para.195.
[187] Van Steenberghe R., 'Self-Defence in Response to Attacks by Non-State Actors in the Light of Recent State Practice: A Step Forward?', 23*Leiden Journal of International Law* (2010), at 183.
[188] American Society of International Law, *The World Court Finds That U.S. Attacks on Iranian Oil Platforms in 1987-1988 Were Not Justifiable as Self-Defense, but the United States Did Not Violate the Applicable Treaty with Iran*, 2013 (available at https://www.asil.org/insights/volume/8/issue/25/world-court-finds-us-attacks-iranian-oil-platforms-1987-1988-were-not).
[189] International Court of Justice, Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgement, 6 November 2003, at para.64.

accumulated.[190] This is a crucial aspect for cyber warfare. As outlined in the properties of cyber, cyber-attacks are often repetitive, adaptive, striking multiple targets, far more so than conventional force. This ruling gives grounds for a more inclusive incorporation of cyber properties within the current legal framework. The ICJ oil platform case also specifically referred to and affirmed the ICJ Nicaragua case specification of the scale and effects framework.[191]

In addition, the case of exemplifies the U.S. attempt at arguing for a lower damage threshold of an armed attack, where the mine attack of a single vessel could constitute an armed attack, but as this was rejected, it further solidifies that armed attacks must be of grave damage. The reasoning behind such legal position of the US was to ensure that a state has the capacity to respond to serious, but smaller scale attacks. As otherwise, with the strict interpretation of the ICJ, hostile actors can purposefully employ force below the threshold of an armed attacks, such as mining a ship, and face no immediate consequences.[192] This exemplifies the rarity of an armed attack. If a kinetic mining of a warship does not constitute and armed attack, it sets a precedent for cyber-attacks, like logic bombs placed in minor critical infrastructure, to more often than not, cannot constitute armed attacks. Especially considering that due to unfamiliarity and lack of consensus, a cyber-attack might have to cause even graver damage than what is expected of a kinetic attack, to constitute an armed attack. Furthermore, para.64 also outlines that *"it has not been established that the mine struck by the Bridgeton was laid with the specific intention of harming that ship, or other United States vessel"*. This establishes another criterion that should also be applicable to cyber, that of animus aggressionis, or intent to specifically harm an actor.[193]

5.3 Jus ad Bellum Issue: Difficulty of applying art.51 armed attack damage threshold to cyber

The application of the damage threshold to cyber faces two difficulties, cyber is non-kinetic and dispersed. Determining the damage threshold for conventional kinetic attacks is already a complex matter, attempts of which, Russia and China reject. Following from the rulings of the above cases it is evident that reaching the armed attack threshold, even considering

[190] *Ibid.*
[191] *Ibid.*, at para.51; Kittichaisaree, *supra* note 98, at 168.
[192] Waxman, *supra* note 79, at 438.
[193] International Court of Justice, *supra* note 189, at para.64; Roscini, *supra* note 88, at 77.

accumulated actions and kinetic damage, remains a rare occurrence. Studies of customary law and state practice of self-defence make it clear that an armed attack needs to be of significant intensity, inflicting substantial destruction on a state.[194] Reaching such a threshold via cyber is even more difficult, because cyber-attacks are more dispersed and operate in a different nature. In the oil platforms incident, the goal of sinking a single warship with mines was primarily to incapacitate the ship, cause inconvenience and deter the patrolling U.S. forces during the ongoing conflict in the region. If such an attack was conducted on a whole fleet, it would have arguably constituted an armed attack. Achieving such feat, even on a larger scale is much simpler with cyber. A man-in-the-middle cyber-attack that feeds false information to the radars of the ships could easily divert multiple ships away from the region, or a wipe of the software of the radars could possibly render them incapacitated for the same amount of time, that it would take to replace the damaged ship on with a new patrol. Despite achieving larger goal with a greater success, this would most likely be viewed as an even lesser form of force than the mining of a fleet of ships, because it was only a manipulation of virtual data. In fact, considering that there is no state practise or even evidence of a state considering categorizing a cyber-attack as an armed attack, it indicates that most cyber usage will fall below the threshold of an armed attack. This may be because there is unfamiliarity and lack of appropriate norms regarding cyber, making states expect higher amount of kinetic and non-kinetic damage to happen, than in the case of kinetic attacks. Or currently the incentive is to use cyber below the threshold of an armed attack, because it still manages to get the job done.[195] It appears that the damage threshold is even higher for cyber because it is non-kinetic, dispersed and states are not accustomed to it. Currently jus ad bellum law of self-defence cannot particularly account for the fact that cyber-attacks can achieve the same highly damaging goals of kinetic force, without reaching the damage threshold of an armed attack as outlined in the jurisprudence.

Further damage threshold issues regarding cyber concern intent and territorial integrity. The case also exemplifies the difficulties of determining targets and their respective ownership by a state. The attack on US owned Texaco Caribbean tanker, was not considered in the accumulation or an attack against the U.S., because it was not at the time flagged with an American flag.[196] While this is more of a peculiarity of the law of the seas, it draws attention

[194] Roscini, *supra* note 88, at 73.
[195] Kittichaisaree, *supra* note 98, at 172–173; Roscini, *supra* note 88, at 74–76.
[196] International Court of Justice, *supra* note 189, at para.64.

to instances of cyber-attacks against targets that provide critical networks needed for state infrastructure, but do not belong to said state. In such a case there is no state practise or judicial cases. It would follow that as with kinetic attacks on private companies beyond the borders of a state, as long as the private entity is based in a state, it would constitute an armed attack. However cyber, unlike conventional weaponry, is more interconnected, with private infrastructure supplying several states. If, Microsoft, a U.S. company is the target, and malware causes the meltdown of Microsoft based computers by over throttling CPU's in governmental computers causing them to be inoperable, this would be an armed attack against the U.S. because the private infrastructure is based in there. But what if the malware also spread to allied European states? It remains to be determined whether that would constitute an armed attack against all states that reach that certain scale.[197]

This also highlights the issue of intent. As showcased in the ICJ oil platforms case, for an attack to be considered as accumulated part of an armed attack, there has to be an intent by the attacker to use such force aggressively. Laying mines does not show sufficient intent, as any ship could have triggered it. However, such applicability becomes more ambiguous with indiscriminate cyber-attacks or ones that produce unintended orders of effect.[198] Attacks such as NotPetya, that were primarily aimed at, allegedly, specifically destroying Ukraine's governmental computers, have spread to most of western states causing kinetic damages and costing billions. This attack could have had an unintended effect and spread by accident, or the perpetrator purposefully made it to spread in order to mask the real target.[199] Either way if the perpetrator was brought forth to the ICJ, under current law, they would have a strong case of plausible deniability. Furthermore, states would not have been able to use self-defence even if it reached the damaged threshold, because the intent is very unclear. Such situations are not possible with kinetic force, even weapons that lack sufficient targeting possibility, like nuclear weapons or outlawed gases, can still be measured and deployed within a predetermined area, with minimal spread. Evidently, the damage threshold is difficult to apply to networks that are deeply intertwined with the state's security, but do not belong to the state or its jurisdiction. This is further exacerbated, considering the intent criterion. Cyber damage can be easily portrayed as unintended, its orders of effect as a complication.

[197] Roscini, *supra* note 88, at 75–76.
[198] *Ibid.*, at 76–77.
[199] Osawa, *supra* note 2, at 114–120.

5.4 Art.51, armed attack and traditional attribution standards

5.4.1 Attribution in *"Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)"*

Attribution is a further nuance of self-defense is particularly relevant to cyber. The ICJ jurisprudence outlines that an armed attack must also fulfill the criteria of attribution, where an attack can be proven to be conducted by a state or the state had effective control of the actor that conducted the attack. Attribution was already implied in the previously discussed para.195, where an armed attack has to be *"the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of ... actual armed attack"*. Send by or on behalf of a state implies that attacks need to have the involvement of a state. The paragraph also asserts that this can be taken to reflect customary law, at least at the time.[200] If an armed attack is conducted by mercenaries, terrorist groups or any actors that would be considered an NSA, the case determines that the acts have to be attributed to a high standard. In para.114 the ICJ outlined that Nicaragua argued the contras conducting armed force against it, were controlled by the U.S. to such an extent that those acts were essentially those of the U.S. Para.115 clarifies that this is an appropriate method, but was not the case in this instance, because the U.S. despite financing and training the contras, did not have *effective control* over them.[201] Effective control is a very high threshold. Articles on state responsibility offered insight into the terms meaning, by clarifying in art. 8 that *"The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.*" The commentary para. 3 further clarified in reference to ICJ Nicaragua, that the state has to be an integral part of that specific operation that is meant to be attributed to it. In the case of the ICJ Nicaragua, U.S. was not in charge of every use of force and international law violation the contras committed, therefore it could only be attributed very narrow specific incidents directly controlled by said state.[202] Evidently, an armed attack needs to be attributed to a state, whether it is directly conducted by it or on behalf of it by an NSA. The state should have effective control over the NSA.

[200] International Court of Justice, *supra* note 175, at para.195.
[201] *Ibid.*, at paras.114, 115.
[202] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001), Yearbook of the International Law Commission, at para.8(3).

5.4.2 The jurisprudence on the level of evidence regarding attribution and damage threshold

When categorizing an attack as an armed attack and invoking self-defence, a state must use a reasonable standard of evidence to demonstrate the level of damage and the attributability of the cyber-attack, which is codified in the international courts' jurisprudence. This jurisprudence differs between courts and particular cases, but not to a great extent. In the aforementioned ICJ Nicaragua case, para.109 proclaims in regard to contras, that *"there is no clear evidence of the United States having actually exercised such a degree of control"*. This signifies that evidence for attribution and in general needs to be clear. As this case dealt with an NSA, it follows that even with a narrow interpretation, the evidence threshold applies to cases of NSA cyber-attacks. Furthermore, in ICJ, *armed activities* case, regarding NSAs, the court continuously referred to the need of convincing evidence in paras. 72, 83, 91 and 210.[203] In the ICJ Oil platforms case, para.71, when attributing the laying of mines to Iran, the court proclaimed that the evidence was "*highly suggestive, but not conclusive"*, signifying that evidence needs to be conclusive. It also required conclusive evidence for the damage inflicted by the mines.[204] As this applied to mines, it would follow that this would apply to logic bombs and malware as well. The ICJ Corfu channel, which ruled on Albania's mining of the sea, also referred to conclusive evidence, leaving no room for reasonable doubt.[205] Overall the evidence needed for attribution must be clear, convincing and conclusive. Hence it is reasonable to assume that the same standard, unless the jurisprudence or customary law changes, should be required when attributing cyber-attacks in the case of self-defence.

5.5 Jus ad bellum issue: Traditional attribution requirements are too stringent for cyber

This warrants a return to the cyber revolution and restraint dichotomy. The level of difficulty of attributing cyber-attacks is a matter of debate. However, even if one takes the position of cyber restraint and believes that it is possible to deduce the perpetrator by analysing the geopolitical or regional rivalry, legal issues still persist.[206] Providing clear, convincing and

[203] International Court of Justice, *supra* note 178, at paras. 72, 83, 91, 210.
[204] International Court of Justice, *supra* note 189, at para.71.
[205] International Court of Justice, The Corfu Channel Case (United Kingdom v Albania), Judgement, 9 April 1949, pp. 17–18; Roscini, *supra* note 88, at 97–99.
[206] Valeriano and Maness, *supra* note 47, at 46–48.

conclusive evidence regarding the perpetrator of cyber-attacks is difficult. Firstly, the anonymity in cyber can cause technological issues of assessing the origin of the code.[207] Even if the initial technological issues are possible to be convincingly analysed, this may still be prevented by third party states through which the cyber-attack has passed, due to their sovereignty. Unlike missiles, airplanes and ships, that operate in international space, cyber operates in national infrastructure, and can pass through the jurisdiction of numerous countries. This allows for any non-cooperative nation involved in the chain of the attack, to potentially halt evidence collection.[208] Not only can this lead to inability to collect evidence, it could result in the inability to identify the perpetrator in general, which makes it difficult to get the support of the international community and to shame the hostile actor in legal terms. [209] Cyber warfare is also notorious for spoofing, which allows hostile actors to either fake the origin of an attack as a neutral state, or they can genuinely route the attack through the infrastructure of another state. The same is not entirely possible with kinetic, conventional weapons. There, of course, exists little jurisprudence regarding such elaborate masquerading of attacks.

Legal experts in the Tallinn manual agreed that the determination of the infrastructure from which an attack originates is not sufficient without other evidence to attribute the attack, favouring a reasonable evidence requirement.[210] In addition, there's also an issue of dual-use infrastructure, that can serve as a malicious weapon and as genuine peaceful tool. This introduces further uncertainties. Russia, and to an extent China, disapprove of countermeasures particularly because they do not involve attribution, and disapprove of the applicability of jus ad bellum law based on the evidence difficulty of attributing cyber-attacks.[211] Within the west there is also reasonable disagreement. The US has argued in the GGE process that "*high- confidence attribution of identity to perpetrators cannot be achieved in a timely manner, if ever".* [212] It also confirms that in some cases circumstantial evidence, relations between states, essentially a cyber restraint-based view, is regarded to be appropriate by some western states. On the other hand, Italy, Netherlands and Germany have voiced opinio

[207] Waxman, *supra* note 79, at 444.
[208] Huntley, *supra* note 92, at 34–35; Waxman, *supra* note 79, at 443–444.
[209] Huntley, *supra* note 92, at 34–35.
[210] Roscini, *supra* note 88, at 77.
[211] The Ministry of Foreign Affairs of the Russian Federation, *supra* note 64.
[212] UN General Assembly Resolution 66/152, UN Doc. A/66/152, 2011, at 17.

juris regarding the need of solid evidence when attributing.[213] This highlights the argument of legal scrutiny. Why should attribution evidence standards be lowered, on the merits that cyber-attacks are harder to prove. If evidence is lowered, this could increase conflict, by giving way to spoofing, and false attribution as a tool of cyber warfare.[214] Furthermore, states are also disincentivised to reveal findings of cyber-attack analysis, as this shows weakness, reveals technical weak points, and may reveal and proliferate cyber capabilities to other actors.[215] Overall it is evident that proving conclusive evidence for attribution of cyber-attacks is a difficult task, due to its anonymity, transboundary nature, and spoofing.

In the cases where convincing and conclusive evidence has been acquired, the attribution must be upon a state as outlined in the jurisprudence, in order to make self-defence lawful. If the evidence leads towards an NSA that operated independently within that state, it remains insufficient to attribute the armed attack and use self-defence, for the time being. There is general agreement that if an attack is conducted by a state organ, reaches the damage threshold, and is attributable via evidence, it is an armed attack attributable to that state. If it is not conducted by a state organ, one must refer to the ICJ jurisprudence on that matter.[216] Some experts argue that majority of cyber-attacks are conducted by NSAs because it proliferates more accessible capabilities.[217] In such a case, as in ICJ Nicaragua case, para.115, the attack committed by an NSA needs to be attributable to a state, meaning that a state must have had effective control over the NSA and the attack.[218] Proving this is already a strenuous and often unsuccessful deed regarding conventional warfare. It is further complicated when dealing with cyber. The equivalent of arming, training and directing NSAs in cyber, is a less involved matter, because cyber tools tend to be cheaper and easier to use. Also, unlike a gun, which can be used by one soldier at a time, cyber code can be used by many upon its release. A hostile state can publicly release malicious code, which can then be used by an NSA, however this would hardly count as arming a specific NSA. The interconnectivity of cyber domain, aspects such as the internet, make the coordination of cyber NSAs faster, cheaper and easier, while maintaining a low level of organization. It is very difficult to prove effective

[213] Advisory Committee on the Issues of Public International Law and Advisory Council on International Affairs, 'Cyber Warfare, No 77, AIV / No 22, CAVV', *Cyber Warfare* (2011), at 22.
[214] Roscini, *supra* note 88, at 100–101.
[215] Waxman, *supra* note 79, at 444.
[216] Schmitt, *supra* note 181, at 344.
[217] Roscini, *supra* note 88, at 80–81.
[218] International Court of Justice, *supra* note 175, at para.115.

control over an NSA when by nature of cyber it is dispersed network of cyber experts operating remotely and anonymously. Hence an NSA can be directed by a state, launch an attack that reaches the damage threshold but due to dispersed organization connected through cyber mainly, effective control criterion will either be an unprovable task, or the incident genuinely never reached it.[219] Overall it is evident that it is difficult to attribute state sponsored NSA attacks due to the nature of cyber dispersion. It essentially allows the conduct of attacks under a low level of organization that does not reach the effective control threshold. The only legal alternative available is to lower or remove the threshold of attribution.

5.6 Art.51, Armed attack, inherent right and attribution.

In contemporary self-defence and attribution debate, there are emerging legal interpretations and practise regarding NSAs. Those are the "inherent right" and "unable or unwilling" interpretations. The inherent right claims that that due to customary law there should be no need for attribution of armed attack. While the unable or unwilling claims to lower the attribution threshold to inability, unwillingness to stop terrorists constituting involvement. While these interpretations overlap significantly, the differ in their transformative scope. The application of jus ad bellum laws to cyber may be pushing towards these interpretations and exaggerating its issues. The following sections will analyse the interplay between these self-defence interpretations and cyber warfare.

The inherent right interpretation sets forth that there is no need for attribution of armed attacks to states, allowing states to respond to NSAs in self-defence within the territory of an innocent state. This argumentation stems from customary law and state practise. The UN charter art.51 specifies that the charter will not impair the *inherent right* of individual or collective self-defence. The reference to inherent right is customary law stemming from the Caroline incident. The incident involved an attack by British forces in 1873, of a Canadian independence rebels ship, within the territory of the U.S. without attribution. The U.S. argued that this was unlawful, not because of lack of the attribution, but because self-defence may only be done if the attack is imminent. US Secretary of State, Daniel Webster, claimed that such an act of self-defence would be lawful if there was "*a necessity of self-defence, instant,*

[219] Delerue, *supra* note 62, at 320–321.

overwhelming, leaving no choice of means, and no moment for deliberation".[220] While this case set the precedent for necessity and imminence, which will be covered later, it also indirectly reaffirmed self-defence against NSAs without attribution, on the territory of a neutral state. It suggests that inherent right based on customary law includes a broader scope that allows to respond to an armed attack without attribution.[221] This would be particularly advantageous for cyber, as it eliminates the stringent attribution and evidence requirements that will be difficult to fulfil with cyber. Hence, if some states are arguing for such interpretation regarding conventional weaponry, support for this to apply to cyber will also develop, as it is even more difficult to attribute. Historically there has been very little state practise, where a victim state would invoke self-defence against an NSA without attribution, citing the inherent right. In fact, most practise has been the opposite, with attribution, especially during the cold war. In the age of the Caroline incident, there was not a fully codified or developed customary law of the prohibition of the use of force, or the requirement for attribution.[222] The usage of the inherent right as the sole justification has been utilized in some cases, like the U.S. invasion of Afghanistan, and Israel's incursion into Lebanon. However, it is important to note that in most cases states couple the justification with additional caveats, such as harbouring of terrorist's accusation against the neutrals state. These additional nuances later developed a somewhat diverging interpretation of the "unwilling or unable" with a greatly reduced threshold of attribution, but not an outright condoning of self-defence against NSA in any instance. This will be discussed in the next section.

5.7 Art.51, armed attack, unwilling and unable reduced attribution threshold.

The unwilling or unable is a variation of the inherent right interpretation and rests on the same principles. It starts with the inherent right interpretation, based on customary law stemming from the Caroline case, which allows self-defence against NSAs without attribution if the attack is imminent. Unwilling or unable builds upon that and deems it necessary that in the

[220] The Avalon Project, *British-American Diplomacy The Caroline Case, Enclosure 1-Extract from Note of April 24,1841*, The Yale Law School Lillian Goldman Law Library (available at https://avalon.law.yale.edu/19th_century/br-1842d.asp).
[221] Gray C. 'The Use of Force and the International Legal Order', in *International Law* 5th (2018) , at 627–629; Korošec and Veber, *supra* note 185, at 66.
[222] Tladi D., *An Assessment of Bethlehem's Principles on The Use of Force Against Non- State Actors in Self-Defence in the Light of Foundational Principles of International Law* (2012), at 1–4.

case of self-defence the neutral state was unable or unwilling to deal with the NSA. Particularly legally grounding, were the Security council resolutions in response to 9/11. Security Council resolutions 1368 and 1373 recognised '*the inherent right of individual and collective self-defence'* in response to 9/11.[223] It has been argued that these resolutions affirm that large scale terrorist attacks can constitute armed attacks, against which self-defence can be used without attribution or consent of the state.[224] Arguably, as per VCLT, subsequent practise should be more significant, most of which showed adherence to ICJ jurisprudence, and strict art. 51 interpretation, especially until 9/11.[225] Nonetheless this interpretation has been emerging, and received support by some states, lawyers and academics. That is because terrorism of NSAs has become a major issue, and the traditional attribution approach does not allow self-defence against independent NSAs. It is a dilemma where either the victims state does not have the right to defend their territory against an attack, or if it does, then it violates the territory of a neutral state. This perhaps even leads to self-defence actions against the initial self-defence, due to misunderstanding or one states rejection of the inherent right approach. Therefore, states have attempted to lower the attribution threshold to the state being unwilling or unable to deal with the NSA that attacked.[226] Such an approach would also be favourable for cyber and is likely to gain support. However, unwillingness and inability of a state to deal with cyber actors is difficult, because they are more dispersed and anonymous. Most states would arguably not be able to deal with cyber-attacks operating in their state.

The US, UK, Germany and some other western or NATO countries, have stressed the unable or unwilling approach, in letters to the UN, regarding the case of its fight against ISIS in Syria.[227] The foundational principle these countries use to justify their stance remains the

[223] UN Security Council Resolution 1368, UN Doc. S/RES/1368, 2001; UN Security Council Resolution 1373, UN Doc. S/RES/1373, 2001.
[224] Bethlehem D., 'Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by NonState Actors', (2011), at 3–4.
[225] Stemmet A., 'Book Review of 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice', 1 (2013), at 299.
[226] Paddeu F.I., 'Use of Force against Non-State Actors and the Circumstance Precluding Wrongfulness of Self-Defence', 30*Leiden Journal of International Law* (2017), at 94–99.
[227] Memorandum to the Foreign Affairs Select Committee, Prime Minister's Response to the Foreign Affairs Select Committee's Second Report of Session 2015-16: The Extension of Offensive British Military Operations to Syria, 2015, p. 16; UN Security Council, Letter from the Permanent Representative of the United States of America to the United Nations Addressed to the Secretary-General, UN Doc. S/2014/695, 2014; Letter Dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations Addressed to the President of the Security Council, UN Doc. S/2015/946, International Organization, 2015.

claim of inherent right to self-defence, rather than any new principles. The supporters also believe that the SC resolutions 1368 and 1373, also endorsed their view.[228] Other western and non-western countries provide more ambiguous opinio juris, regarding the unwilling or unable, often citing the SC resolutions 1368 and 1373, but only referring to the 'inherent right'. In such a way providing no explicit way of how the right should be applied in practise.[229] Furthermore several major cases are used to justify state practise of the unwilling or unable interpretation. Those are the, US invasion of Afghanistan, Israel's campaign in Lebanon, Turkish incursion against NSA in Northern Iraq, Pakistan attacks on PKK in Iraq, US, UK, France's air strikes and military campaign in Syria, Indian attack on NSA camp in Pakistan.[230] In jurisprudence, some judges, like ICJ judge Kooijmans' and Simma's in multiple separate opinions, have expressed the interpretation that inherent right should allow the use of self-defence against armed bands in a neutral state, especially considering the changing nature of warfare. Simma contends that the traditional interpretation has prevailed for a long time, but it must adapt considering the opinio juris.[231] Debates in academic arena also diverge, but this interpretation has supporters. Scholars argue that apart from the ICJ jurisprudence interpretation there's nothing in art.51 that limits its scope to states or acts attributable to states, arguing that at concurring with state practise, the definition of armed attack should be expanded to include NSAs.[232] Overall it is evident that there are legal basis for the inherent right of self-defence, and the unwilling or unable approach, within customary law, opinio juris and some state practise.

The inherent right and the unwilling or unable interpretation has frail legal basis and lacks sufficient state practise. Furthermore, it would result in a violation of sovereignty, especially if invoked regarding cyber. The security resolutions only reaffirmed that existence of the right to self-defence, it did not classify the 9/11 attacks as armed attack, only a threat to peace, and in no way suggested that force should be used on the territory of any state without its consent. Perhaps at best, it only suggested that acceptance of force against Afghanistan in the particular

[228] Bethlehem, *supra* note 224, at 770–775.
[229] UN Security Council, Letter Dated 11 January 2016 from the Permanent Representative of Denmark to the United Nations Addressed to the President of the Security Council, UN Doc. S/2016/34, 11, 2016.
[230] Enabulele A.O., 'Use of Force by International/Regional Non- State Actors: No Armed Attack, No Self-Defence', 1*European Journal of Law Reform* (2015), at 214–215; Van Steenberghe, *supra* note 187, at 187–191.
[231] Dam C. Van, 'Extraterritorial Law-Enforcement : Combating Non-State Actors', 18 (2013), at 24–25; Enabulele, *supra* note 230, at 213–214.
[232] Dam, *supra* note 231, at 23–25.

case of 9/11.[233] Even so the state practise is not conclusive. The invasion of Afghanistan rested on strong political support that stemmed from the fact that the U.S. claimed to have attributed the attacks to Afghanistan in a traditional manner. Rather than attributing it to the Taliban solely. Furthermore, the Turkish and Israeli incursions had been criticised.[234] The actions taken in Syria, and the unwilling or unable approach has been condemned by Syria itself, by claiming that Syria has a sufficient military campaign against ISIS and invited western forces to join it. It also referred to the relevant SC resolutions regarding ISIS, and the fact that they always constrain actions by refereeing to the UN charter, in which territorial integrity is of utmost status. As with everything, there are political nuances here that prevented the west from supporting the Syrian campaign, but it is still opinio juris nonetheless.[235] The overall disagreement on the matter is exemplified in SC resolution 2249, which refrained from explicitly endorsing the unwilling or unable interpretation Reaffirming territorial integrity and compliance with international law (Arguably the current self-defence law).[236] Therefore arguably the interpretation of art.51, armed attack and attribution has not changed because the state practise and opinio juris have not been universal enough. As per VCLT art.31 subsequent practise and customary law formation, practise has to be repeated over time and approved of by other states.[237]

Accepting such a transformative interpretation of the law would arguably make the principles of territorial integrity and sovereignty meaningless.[238] Applying the interpretation of inherent right and self-defence without sufficient attribution, would render all of the ICJ jurisprudence, state practise insignificant. Even the ICJ cases that came after 9/11, did not change the interpretation of attribution. However, stressing the ICJ jurisprudence too much may have constitutionalist limitations that will be explored later. The ICJ DRC v. Uganda case reaffirmed that an armed attack by an independent NSA is not possible, by reasserting that Uganda could not use Self-defence against armed groups in DRC, because they "*remained non-attributable to the DRC",* in para.146.[239] This jurisprudence essentially negates the

[233] Gray, *supra* note 221, at 629; , *supra* note 223.
[234] Tladi, *supra* note 222, at 6–11.
[235] UN Security Council, Identical Letters Dated 29 December 2015 from the Permanent Representative of the Syrian Arab Republic to the United Nations Addressed to the Secretary-General and the President of the Security Council, UN Doc. A/70/673– S/2015/1048, 2016.
[236] UN Security Council Resolution 2249, UN Doc. S/RES/2249, 2015.
[237] Van Steenberghe, *supra* note 187, at 186–187.
[238] Tladi, *supra* note 222, at 1–4.
[239] International Court of Justice, *supra* note 178, at para.146; Korošec and Veber, *supra* note 185, at 64–66.

unwilling or unable interpretation, because DRC was a perfect example of being unable, as a failed state at the time, to stop attacks against Uganda. This case could also be interpreted to imply that attacks can't be attributable to failed states.[240]Even when accepting the unable or unwilling attribution, it does not work with other jurisprudence principles. If a state was unwilling or complicit in allowing the NSA to operate within a state, as seen in the Articles on state responsibility commentary on ICJ Nicaragua case, it is agreed that a state is only responsible for the attacks it was involved in and contributed to. In the case of Nicaragua that does not of course make a state responsible for other acts that rise to an armed attack.[241] In such a way, acts committed by an NSA independently should not be the responsibility of the state. Allowing self-defense in such a case appears to be a very high penalty considering current jurisprudence.[242] Overall it is evident that the inherent right and the unwilling or unable approach is still developing, and will require more state practice, and acceptance from other states.

5.8 Jus ad Bellum Issue: Cyber promulgates the "inherent right" self-defence emerging interpretation and its difficulties

As discussed earlier, even taking the cyber restraint view and accepting that cyber attribution can be deduced in regional and balance of power scenarios, this still remains difficult when considering the high threshold of attribution needed for self-defense. This is even more so considering that NSAs add an additional level of complexity. As most cyber-attacks are propagated by NSAs, and their capacity is increasing, it can be expected that more states will adopt the unable or unwilling interpretation. Currently states, both western and non-western, place particular emphasis on the responsibility of stopping NSAs from using cyber infrastructure. This was reaffirmed in the consensus of the GGE 2013 report.[243] Hopefully these responsibilities will be accepted universally, and states will dedicate a serious effort in proactively constraining any NSAs from using cyber within their territory. Indirectly though, such norms may serve as part of the legal case when making justification for a state's unwillingness or inability to address the cyber NSAs. In such a case where an attack happens despite the widespread acceptance to prevent cyber NSAs from operating, unwilling or unable

[240] Barbour S.A. and Salzman Z.A., ''The Tangled Web': The Right of Selfdefence against Non-State Actors in the Armed Activities Case', 42*Journal of Urban Affairs* (2018), at 55–64.
[241] International Law Commission, *supra* note 202, at para.8 (3).
[242] Paddeu F.I., 'Use of Force against Non-State Actors and the Circumstance Precluding Wrongfulness of Self-Defence', 30*Leiden Journal of International Law* (2017), at 104–109.
[243] Roscini, *supra* note 88, at 80–82.

will be a stronger justification to rely upon. Furthermore, as cyber technologies are cheap, easy to proliferate, and their usage is very dispersed, it will be hard for any weaker state to deal with NSAs. Hence it will raise conflict. Considering these properties of cyber it is also crucial to discuss the principles of necessity that establish when precisely is it necessary for a state to respond in self-defense, even when attribution is achieved.

5.9 Self-defence and Necessity

The principle of necessity stems from customary law. The Caroline case once again serves as a thorough source of custom and practice. Again referring to the secretary of state Webster's remark "*a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation",* exemplifies the customary law rule of necessity.[244] There is agreement in the academic literature and most importantly, in opinio juris, that necessity is a foundational faction in the lawfulness of self-defence.[245] Arguably this principle can also be found in state practice long before the UN charter. The league of nations arguably did not outlaw war because it thought that necessity was such a strict principle of self-defence that legitimate and necessary war is bound to happen.[246] In art.15 of the covenant of the league of nations, the league specified that if the council fails to reach unanimous report, then "*the Members of the League reserve to themselves the right to take such action as they shall consider necessary for the maintenance of right and justice".*[247]

Necessity is not codified in the UN Charter, and primarily is based on customary law.[248] However, jurisprudence has come a long way in engraining the concepts. It can be construed from the UN charter art.51 that the necessity of self-defence is only allowed until the Security Council has taken necessary measures to maintain peace. Granted that the measures are successful, subjective as it may be, the state may not have the necessity criteria fulfilled any longer.[249] However in the instances that the Security council did act, it usually did not order

[244] The Avalon Project, *supra* note 220.
[245] Tsagourias N., 'Necessity and the Use of Force: A Special Regime', *Netherlands Yearbook of International Law* (2010), at 13–15.
[246] , *supra* note 13, at art.13, 17.
[247] *Ibid.*, at art.15.
[248] Gray C., *International Law and the Use of Force* (3rd ed., 2008), at 150.
[249] Tsagourias, *supra* note 245, at 19.

the cessation of individual state self-defence.[250] Post 9/11, the security council reaffirmed self-defence despite taking action, imposing sanctions.[251] The only time where the it could be implied that the security council attempted to suspend a state's necessity for self-defence, was the security council resolution 1701 regarding Israel's actions in Lebanon. [252] Therefore it can be construed that the necessity principle can be fulfilled irrespective of the Security Council's measures or their effectiveness.[253] Furthermore, the notion has been codified and its definition, clarified, in the ICJ jurisprudence.

5.9.1 Necessity in *"Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)"*

The ICJ Nicaragua case has reaffirmed in para. 194, that "*whether the response to the attack is lawful depends on observance of the criteria of the necessity and the proportionality of the measures taken in self-defence".*[254] This essentially means that given that there is sufficient evidence that an armed attack occurred and can be attributed, the self-defence must also be necessary. This criterion is strict, as the court ruled that even if the U.S. claim of collective self-defence on behalf of El Salvador, against Nicaragua, was justifiable, it would have not met the criteria of necessity. In para.237 the court argued that *"measures were only taken, and began to produce their effects, several months after the major offensive of the armed opposition against the Government of El Salvador".*[255] This reaffirms, that as exemplified in the Caroline case correspondence, actions in self-defence must be taken either immediately or when necessary to *stop* the attack. Such actions or, use of force, cannot be taken after the fact of the attack, no matter the damage.

5.9.2 Necessity in "Oil Platforms (Islamic Republic of Iran v. United States of America)

Proceeding from the conclusions of the ICJ Nicaragua case the ICJ oil platforms case builds upon it and expands on the necessity criteria. In para.76 the court expresses that *"Court is not*

[250] Tams C.J. and Devaney J.G., 'Applying Necessity and Proportionality to Anti-Terrorist Self-Defence', *Israel Law Review* (2012), at 97.
[251] Tsagourias, *supra* note 245, at 18–19.
[252] Tams and Devaney, *supra* note 250, at 97.
[253] Tsagourias, *supra* note 245, at 19.
[254] International Court of Justice, *supra* note 175, at para.194.
[255] *Ibid.*, at para.237.

satisfied that the attacks on the platforms were necessary to respond to these incidents. In this connection, the Court notes that there is no evidence that the United States complained to Iran of the military activities of the platforms, in the same way as it complained repeatedly of minelaying and attacks on neutral shipping, which does not suggest that the targeting of the platforms was seen as a necessary act."[256] This highlights that acts of self-defence, its targets, need to be necessary to use force against in order to force the adversary to cease its armed attack.

5.10 Necessity and additional components

The court highlights the immediacy as a crucial aspect of necessity. It follows that as proof that self-defense was necessary, actions taken must have been under the auspice of immediacy, as in the Caroline customary law case, and preferably before the security council takes action.[257] Furthermore, as per Caroline case customary law, necessity means "*leaving no choice of means, and no moment for deliberation"*.[258] Meaning that a state must have no alternative, however it is difficult to determine what alternatives the state must exhaust. Referring to the ICJ oil platforms case, the US not voicing concerns to Iran regarding mining by the oil platforms showcased a lack of necessity, and a non-exhaustion of means. Many lawyers agree that, lack of alternative means, the lack of *effective* alternatives. This has been showcased in the principle 3 of Chatham house consensus report on use of force in self-defence.[259] Judging necessity and such lack of effective alternatives, remains a comprehensive factual and political assessment. It could be argued, that considering the high threshold of an armed attack damage established by the ICJ, the sheer damage would immediately fulfil the necessity criteria and warrant an immediate forceful response to halt the attack. Granted that the actions are taken immediately.[260] As determined earlier reaching the damage threshold in cyber is very difficult. This notion has also been shown to be difficult to apply with conventional warfare, in state practise. In the Falkland island conflict the UK responded to the occupation after the fact of the occupation of the island by Argentina. Argentina's campaign was also not particularly damaging, as it resulted in no casualties, but it did remain a grave

[256] International Court of Justice, *supra* note 189, at para.76.
[257] Gardam J., *Necessity, Proportionality and the Use of Force by States* (2004), Necessity, Proportionality and the Use of Force by States, at 149–152.
[258] The Avalon Project, *supra* note 220.
[259] Chatham House, *Principles of International Law on the Use of Force by States in Self-Defence* (2005), at 7–8; Tams and Devaney, *supra* note 250, at 96.
[260] Gardam, *supra* note 257, at 149; Tams and Devaney, *supra* note 250, at 98.

violation of international law. Arguably in this case immediacy was not apparent anymore, however the self-defence was widely considered as lawful.[261] This could also become a precedent in cyber, as other wise, due to the instant nature of cyber, it would usually not be necessary to respond to cyber-attacks. The issue with necessity, its application and perception of validity, at least partially depends on the stance of the particular state regarding self-defence. States that accept notions such as anticipatory self-defence, accumulation of attacks or self-defence against imminent attack, may have wider interpretation of necessity.[262] However there is certain agreement that self-defence shouldn't be retaliatory or punitive, though applying this may also be difficult.[263] Furthermore there's also agreement that occupation as part of self-defence is not necessary. Such actions have been condemned in the past, when Israel occupied Lebanon during 1985-2000, and South Africa's occupation of Angola during 1981-1988. [264]

The necessity becomes more complex if one accepts the emerging norm of self-defence in the scope of unwilling and unable. In the case of an NSA attack, it would follow that actions by the host state becomes another alternative that needs to be exhausted in order to fulfil the necessity requirement. Just as per ICJ oil platforms, the victim state would probably have to express concerns to the host state, otherwise necessity may not be present.[265] Even states that support controversial international law stances, such as anticipatory self-defence, and inherent right of self-defence against NSAs, have condemned such actions by other states by referring to the lack of necessity present. This makes necessity perhaps the most important legal principle when considering self-defence against NSAs without attribution, or within the unable or unwilling scope.[266] Arguably necessity could in practise be achieved without requiring the host state to deal with the NSA. Necessity may be fulfilled if the host state supports or is unwilling to deal with the NSA, as in the case of Afghanistan, Taliban and Al-Qaeda. A variation of this would be if the state does not support the NSAs, but purposefully harbours them, failing due diligence. This is for example considered an act of aggression on the African Union.[267]

[261] Gardam, *supra* note 257, at 150–153.
[262] Gray, *supra* note 248, at 150.
[263] *Ibid.*
[264] *Ibid.*, at 155.
[265] Tams and Devaney, *supra* note 250, at 98.
[266] Gray, *supra* note 248, at 154.
[267] Tams and Devaney, *supra* note 250, at 99–100.

5.11 Jus ad bellum issue: Necessity is difficult to apply to cyberspace, immanence is hard to distinguish

The requirement of necessity is meant to affirm that actions taken in self-defense are a last resort. Fulfilling this requirement is very difficult regarding cyber warfare. Firstly, the victim state will have to make sure that the cyber-attack was not an accident, or cyber incident that was indiscriminate and through orders of effect reached a high threshold of damage. Unlike conventional warfare, where a state can reasonably judge whether a surface-to-air missile target was the original intention, with cyber the damage can spread by accident. Furthermore, in cyber, it can be argued that in many cases, a cyber-attack can be dealt with in cyber means.[268] For example, envision a case where malware is continuously spreading through critical military infrastructure, causing physical damage to radars, GPS receivers or satellites, rendering those components and the military equipment that relies on it, inoperable. As the virus spreads, the necessity criteria may appear to be fulfilled as the victim state must act in self-defense to stop the spread. If in such a case the victim state carried out targeted air strikes against the facilities from which the cyber operation was being carried out, the perpetrator could still, validly, argue that necessity criterion was not met. That is because it could be argued that the victim state, could have used a cyber remedy to stop the spread of the malware. It would remain hard to conclusively deduce whether the victim state truly had the capacity to stop the attack by blocking it via cyber means. Conventional responses therefore will become controversial. In addition, this also merits whether conventional responses can be proportionally carried out in response to a cyber-attack.

5.12 Self-defence and Proportionality

Proportionality is part of the customary law of self-defence and would also be applicable to cyber. The aforementioned correspondence *Caroline* case showcases the custom of proportionality, as Webster rightfully conveys it *"since the act justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it"*. [269] Once again the UN charter does not codify the principle of proportionality in any great depth. In addition, the

[268] Roscini, *supra* note 88, at 88–90.
[269] The Avalon Project, *supra* note 220.

principle of proportionality is highly intertwined with necessity, because unnecessary force is by definition not proportionate, while not proportionate force is unnecessary [270] In the case where necessity is fulfilled, proportionality serves as a principle to limit the scope and intensity of self-defence.[271] Proportionality can be viewed as quantitative proportionality or teleological proportionality. The latter would seem to allow for force necessary to stop or repel the attack, while the former would mean a use of force that is essentially equivalent to that of the initial armed attack. This principle is therefore difficult to apply, prior to taking actions, and can be interpreted differently after the incident. It becomes even more difficult when applying it to NSAs that can't be entirely attributed to a state. For example, Israel's incursion into Lebanon, its attacks on airport and the killing of civilians, have been criticised as disproportionate, but Israel used a teleological justification, where they resorted to the necessary force in order to stop the attacks unleashed upon them.[272] As it was condemn by many states and the UN, this sets out state practise that for self-defence against NSAs to be proportional, the host state infrastructure should not be targeted, and harm must not be done against civilians.[273] The aforementioned Turkey's invasion into Northern Iraq as a self-defence response to an NSA, also may set some precedents. The operation consisted of twenty times higher casualties for the PKK, the NSA in question, which was not particularly criticised as disproportional. This could showcase state practise that states, and other international law subjects are willing to accept differing proportionality standards when dealing with a highly malicious NSA. [274] Furthermore, it is useful to examine the ICJ jurisprudence as it provides codification of the notion of proportionality.

5.12.1 Proportionality in "Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)"

The case concerning armed activities on the territory of Congo determined, as examined earlier, that the self-defence by Uganda was not warranted as it was not attributable to DRC.[275] Therefore, the court did not delve into the nuances of necessity and proportionality. However, it noted, in para.147, that *"The Court cannot fail to observe, however, that the taking of airports and towns many hundreds of kilometres from Uganda's border would not seem*

[270] Gray, *supra* note 248, at 150.
[271] Tams and Devaney, *supra* note 250, at 101.
[272] Van Steenberghe, *supra* note 187, at 205–208.
[273] Tams and Devaney, *supra* note 250, at 105.
[274] *Ibid.*, at 104.
[275] International Court of Justice, *supra* note 178, at para.146.

proportionate to the series of transborder attacks it claimed had given rise to the right of self-defence, nor to be necessary to that end". [276] Such ruling highlights that there is a quantitative aspect to the approach of the ICJ, where repelling or stopping the attack is of primary concern.

5.12.2 Proportionality in *"Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)"*

The case of military and paramilitary activities in and against Nicaragua considered the significance of proportionality. In para.237 the court stated that *"Whether or not the assistance to the contras might meet the criterion of proportionality, the Court cannot regard the United States activities summarized in paragraphs 80, 81 and 86, i.e., those relating to the mining of the Nicaraguan ports and the attacks on ports, oil installations, etc., as satisfying that criterion.".* [277] This therefore appears to be a very direct violation of proportionality. It reveals that if a state is supporting an NSA that is carrying out attacks that constitute an armed attack, one cannot respond by a widespread campaign targeting critical infrastructure, of the host state. Thus, the court again favours a more of a quantitative proportionality framework.

5.13 Jus ad bellum issue: Proportionality is hard to adhere to in cyber

Proportionality in cyber warfare will require strenuous consideration when conducting self-defence. Applying the ICJ quantitative proportionality approach becomes difficult because matching the scale and effects of the initial cyber-attack in cyberspace is a hard factor to control for when carrying out cyber operations. A state may not have the same cyber capacity to implement a proportional response. In addition, due to the orders of effect, unforeseen consequences and adaptations of malware, the damage intended to be used as self-defence can rapidly become higher than anticipated. Even halting a mission can be difficult in such a case, consider a malware set to duplicate to governmental computers via a software, once it is set, without strict kill switches and oversight, it can become difficult to stop by the initiator. Operations like Stuxnet have successfully been implement and halted with kill switches at the command of its initiator, however it appears that such operations may take years to plan and require major financing. In addition, the Stuxnet code purposefully attacked within a closed network, in such a way making any spread outside less likely. Mustering such excellent

[276] *Ibid.*, at para.147.
[277] International Court of Justice, *supra* note 175, at para.237.

capability at the moment of necessity and immediacy may prove to be tricky.[278] This, in some cases, will undoubtedly pressure states to respond with kinetic measures. Determining how many inoperable chipsets, computers or weapons systems is equivalent to how many air strikes, mines, and bullets remains a conversion that a state should tread lightly upon.

[278] Roscini, *supra* note 88, at 89–91.

6 Fragmentation of international Law

The jus ad bellum international law regulating the use of force and self-defence in cyber warfare has been showcased to have multiple emerging issues. The interpretation of jus ad bellum laws appears to be strictly divided. If a narrower non-western interpretation gains more subsequent practise, it would render the jus ad bellum laws inapplicable to cyber, requiring new norms. If the western interpretation of jus ad bellum applicability gains widespread support, it would render the jus ad bellum law applicable. However, art.2(4) would arguably not apply to non-kinetic attacks. In addition, the self-defence principles of damage threshold, attribution, necessity and proportionality would also pose issues due to anonymity, dispersed nature, and proliferation of cyber capacity. Hence, perhaps the crucial dilemma persisting, is that of where the law may proceed to develop and what impact this may have upon the international order. The theoretical lens of constitutionalism and pluralism may provide an analytical approach to further analyse the factors from which issues of jus ad bellum international law emerged and the potential effects that those may have in the future of international legal order.

6.1 Constitutionalism

Constitutionalism is a theory that is based on legalist principles, those that want law to strive to be separate from politics. It is a legal theory that primarily emerged from German lawyers and philosophers. National constitutions have been emerging over the past several centuries in one form or another, however such a thinking reached international law only in the 20th century. Influential political and legal philosophers, for example Habermas, envisioned international law to be a more concrete separate sphere guiding international relations. Habermas proposed, what is now encompassed in constitutionalism, a clear three tier system of governance, with distinct global, regional and national levels. [279] This firstly, highlights the wish to separate the sphere of international law from its other components to the greatest extent possible. This doesn't necessary mean just the legal system of national systems, but to an extent from some of the political deliberation and interest that can influence law. This foundationally is a legalist perspective. Constitutionalism in itself has to be a legalist approach. A legalist view of international law perceives or understands that politics can

[279] Bianchi, *supra* note 26, at 44–45; Bogdandy A. von, 'Constitutionalism in International Law: Comment on a Proposal from Germany', 47*Harvard International Law Journal* (2006), at 223.

influence international law, but also believe that international law can be separated from politics, or infused by political legitimacy, to a sufficient extent for it to function and serve its purpose efficiently. Contrary to such position the anti-legalists argue that political principles and incentives primarily drive outcomes of international disputes, politicises law making and turns international law into a moral guise to cover further political interests.[280] Therefore constitutionalism primary objective is for international law to gain independent legitimacy that is not overridden by politics.

Constitutionalism seeks not only to separate international law from political, regional and national systems, it also wants international law to solidify as strict, order based, unified centralized system. As a constitutional international legal system is separated from politicized influence to the necessary level, it must then bring more order to international law and the international community. Constitutionalist lawyers, and in fact many other lawyers argue that the system of international law should centre around written or unwritten principles deemed to be central. This could be customary law principles, but most refer to the UN charter as the central constitutionalist foundation. Such a stance is warranted as the UN charter, akin to national constitutions, also sets itself to take precedence over other international law, it has formal superiority against other conflictual international agreements, that are also meant to be sources of law. [281] By signifying the UN charter as the constitutional document of the international legal order, it provides legitimacy to the system, because the UN charter has been and continuous to be formed by states, making it representative. In such a way it also aims to prevent any fragmentation that may happen, by referring actors back to the UN charter or the central constitutional codification of law. Therefore, this theory is particularly relevant in the case of cyber as we can see that states question the very scope of the UN Charter. Constitutionalism tries to depoliticise the international community, because the UN charter becomes the highest rank of legal force, not meant to be interfered with by politics, and in such a way becomes an indirect limit on state power. It simplifies the legal system, bringing predictability not only for lawyers, courts, but also for states themselves. As in national

[280] Hoffmann F. 'International Legalism and International Politics', in A. Orford and F. Hoffmann (eds.), *Oxford Handbook of the Theory of International Law* (2016) , at 973–975.
[281] Bianchi, *supra* note 26, at 48; Doyle M.W. 'The UN Charter - A Global Constitution?', in *Ruling the World? Constitutionalism, International Law, and Global Governance* (2009) , at 113–116; Petersmann E.-U., 'How to Reform the UN System? Constitutionalism, International Law, and International Organizations', 10*Leiden Journal of International Law* (1997), at 426.

systems, the UN Charter "constitution" becomes a check on the power of politics and states.[282] Furthermore, the constitutional approach towards international law has major components of liberal democratic legal thought, as it perceives certain international principles and laws to be constitutionalised, arguably beyond jus cogens norms, it aims to proliferate international courts, tribunals and making judicial review the primary and most effective way to apply the law and constrain power via judicial scrutiny. These legal principles in addition to the societal values that are perceived as fundamental to the international community such as legitimacy, human rights are the pillars around which international law should be constitutionalised.[283] Therefore, the core components of constitutionalism are based on seeking centralisation of international law around primarily the UN charter, avoiding fragmentation, limiting state and political power. It also theorises that international law should maintain the centrality of principles engrained in the UN charter and the values of the international community and ensure that the constitutionalized laws are applied effectively via increased judicial review and court authority.

6.2 Constitutionalism and the contemporary jus ad bellum legal order

Components of a constitutionalist thought can be seen within international law. However, constitutionalism has been facing challenges of fragmentation, disputation of the UN charter, and disregard for the 'constitutional' courts of the international legal order. It is evident that constitutional thought has been very influential in the development of international law. While the UN charter is not a constitution per se, as it lacks some of the necessary attributes of one. It is not a source of law in itself and does not constitute a sole unified legal system as in constitutional national systems. It does however have mechanisms of enforcement and the supremacy component.[284] The UN charter art.103 exemplifies the constitutional vision of the UN and international law, by stating that *"In the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail."*[285] The ICJ has in the past gained significant prominence, and its impact on the

[282] Bianchi, *supra* note 26, at 50–51; Hoffmann, *supra* note 280, at 975.
[283] Bianchi, *supra* note 26, at 56–60; Giegreich T., 'The Is and the Ought of International Constitutionalism: How Far Have We Come on Habermas's Road to a 'Well'Considered Constitutionalization of International Law"?', 10*German Law Journal* (2010), at 53–56.
[284] Doyle, *supra* note 281, at 113–114; Giegreich, *supra* note 283, at 37–41.
[285] United Nations, *supra* note 9.

application of international law has been arguably larger than initially expected. The UN charter and its courts codify and apply jus cogens and erga omnes obligations. The UN overall has become the main arena of deliberation and international change. There is merit to the constitutional view, that aims to unify the laws that regulate the conduct of states. It may be preferable to constitutionalise cyber interpretation of jus ad bellum laws, and other laws for that matter, to have a clear set of principles regarding what is lawful and unlawful.[286] Such way would make jus ad bellum law predictable and universalised. The constitutionalizing of the current proposed western interpretation of jus ad bellum, while having many issues, would still create a more predictable legal order in cyberspace. Perhaps constitutionalism of western norms is the only way forward, as non-western states demand for new norms of non-militarization would work in an ideal world, but cyber is already militarized. Such demands are akin to demands to not militarize land, sea and air. This would eliminate war in theory, but in reality, it would probably never happen. Furthermore, such constitutionalist approaches have been challenged in the past, but now more than ever, the debate surrounding cyber warfare has challenged the most fundamental, and arguably the most central principles to a vision of a constitutional order: the jus ad bellum jus cogens norms, from which states cannot derive.

There are several limitations that constitutionalism, and the strive towards its goals within the current international legal system, presents. Especially when considering cyber warfare in the current legal order. These limitations are primarily the following:[287]

- Inability to sufficiently limit political and ideological influence over international law
- Cemented norms preventing urgent transformative change
- Difficulty accounting for alternative interpretations on compelling issues
- Legitimacy and legality overriding other justified authority
- Politization of constitutionalism increasing deviation and fragmentation

The constitutionalist goals are in the first place difficult to achieve, and often do not operate in dichotomies. The goal of constitutionalism to reduce the influence of political interests

[286] Petersmann, *supra* note 281, at 453–456.
[287] Bianchi, *supra* note 26, at 51–53; Koskenniemi M., 'Constitutionalism as Mindset: Reflections on Kantian Themes about International Law and Globalization', 8*Theoretical Inquiries in Law* (2007), at 13–20.

overriding law does not mean the elimination of anything political within the scope of law. It is more of an aim to reach a balance, or achieve common goals, where the law can operate and achieve its purposes with a consensus rather than an ideological division. These challenges to constitutionalism will be highlighted in the proceeding sections, when considering the effect cyber warfare and the changes accompanying it are having on international law.[288]

6.3 Constitutionalism and the transformation of cyber warfare

The constitutional order of international law has flaws that have been emphasised by the potentially transformative nature of cyber warfare. A limitation of a constitutional system is that it cements norms and constrains transformative changes in times of need. This also may push subjects of international law away from UN processes, and result in more fragmentation. In the section of cyber and whether it is a revolution of warfare, different properties of cyber and their potential to be harmful, has been explored. Evidently, cyber has transformative properties of uncertainty and capacity. The lack of cyber cases and the capacity of cyber technology to change so rapidly that it outstrips the understanding of its effects. This does not fit in well within a constitutional system that aims to cement norms. Arguably, the aim to centralize norms, may result in the inability to reach to urgent change in the international community. This may be the reason why the UN has only recently accepted deliberations regarding cyber, even though it was a topic of concern within the works of publicist, and substantial expertise has been forming in academia, years prior.[289] This may also be the reason why the UN or the ICJ cannot yet take a strict legal stance on cyber matters. If the ICJ released an advisory opinion on how jus ad bellum laws apply to cyber warfare, it may become obsolete considering how rapidly the capacity of cyber changes, and its additional properties of uncertainty. [290] This is comparable to how the ICJ allegedly refrains from taking a stance on conventional self-defence against NSAs dilemma.[291]

[288] Besson S. 'Whose Constitution(s)? International Law, Constitutionalism and Democracy', in *Ruling the World? Constitutionalism, International Law, and Global Governance* (2009) , at 296–299.
[289] Schmitt M.N., 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37*Columbia Journal of Transnational Law* (1999).
[290] Kello, *supra* note 3, at 6–7.
[291] Becker T. 'The Agency Paradigm: The Principle of Non-Attribution and Its Exceptions', in *Terrorism and the State: Rethinking the Rules of State Responsibility* (2006), at 70.

Furthermore, the proliferating effect of cyber empowers NSAs, which already poses a major difficulty for the vision of a constitutionalised order. The UN stance, and its jurisprudence, has remained relatively strict in its decision to maintain long established and cemented principles of attribution to states. This has proceeded to such an extent that as showcased, states are developing parallel interpretations and frameworks, such as the adherence to the primary principle of 'inherent right', and the unable or unwilling approach. Interpretations parallel to the UN process, of how the law applies to cyber, as exemplified, are also emerging. The western states are partaking in separate processes, such as the Tallinn manual deliberations, NATO, bilateral and institutional negotiations on cyber and other forums on cyber security and law.[292] While Russia, China and other nations attempt to transform the law outside of the UN, via different organizations such as the Shanghai Cooperation Organisation[293]. There's nothing condemnable of these actions, it is how international law works, but it is alarming, as the most fundamental jus ad bellum laws are at stake. The strict constitutional approach may be pushing states away from the UN process, or at least did so previously. Evidently, the constitutionalist aspects already present in the international legal order, inhibit a response to urgent issues, and may be pushing away certain states. This may also indicate that constitutionalism as a theory is being challenged by cyber. Perhaps solving the issues presented by cyber may be difficult by adhering to a constitutionalist worldview. The legal strain resulting from cyber technology may be thrusting states into a more pluralist approach. Yet, paradoxically, only a universalized constitutionalist regulation of cyber can make international relations stable, predictable and secure.

6.4 Constitutionalism and the politization of cyber and jus ad bellum

A constitutionalist approach is also under pressure regarding the differing politicised interpretation of cyber warfare and the applicable law. The differing conceptualizations of cyber and political interests seem to override the UN deliberations regarding cyber. In the section of cyber conceptualization, it was explored how states view cyber as different domains for security and political reasons. It is evident that the discussion over interpretation of cyber and the law, at the UN, has reach a stalemate, based on the ideological and geopolitical

[292] Council on Foreign Relations, *Brazil-EU Cyber Cooperation: Swinging Bridges on the Road to Stability in Cyberspace*, 2020 (available at https://www.cfr.org/blog/brazil-eu-cyber-cooperation-swinging-bridges-road-stability-cyberspace).
[293] UN General Assembly, *supra* note 64.

frontlines. Russia's and China's clear authoritarian wish to seclude their societies from any cyber interference on the basis of sovereignty, while completely denying the application of jus ad bellum laws, to a domain that clearly can cause serious damage, is a blow to the most fundamental international laws.[294] It is a political move, because their claim to perceive cyber as a domain meant to be peaceful, tries to reassert the position that Russia has only reasonable and peaceful intentions. It is also a strategical move to ensure that any conventional kinetic action to the cyber-attacks of these states, would be regarded as unlawful.[295] In regard to China, non-applicability of jus ad bellum to cyber, is a strategy to maintain, ensure its growth as a global power, and to equalize its capabilities with the U.S. conventional force, by expanding cyber.[296] Furthermore this also serves as a push against the liberal preferences of constitutionalism. Constitutionalists often return, rightfully so, to liberal values when gaps or ambiguities emerge in the law.[297]

Constitutionalism in itself requires the unity of values, the EU and North America are the most homogenous regions of values akin to no other in history. The U.S. therefore is also interpreting art.2(4) and art.51 based on their political and strategic interests. U.S. wants to ensure that they can utilize their superior conventional forces for deterrence. At the same time the US is the most vulnerable to cyber-attacks due to interconnectivity and its freer markets that are difficult to regulate. Therefore, the U.S. and other western states want a strict, constitutionalist, approach towards the codification of the interpretation of jus ad bellum laws regarding cyber. As per the constitutionalist legal theory, this would certainly bring more order, to international law and the community, as well as predictability and clearness for states and lawyers.[298] Beyond the self-interest of states, the constitutionalist international law approach in general, has basis in liberalism, which is also why western argumentation against Russia's interpretation of cyber often stems from general positions of freedom and human rights. They argue that cyber is not and should not be an information tool used for societal purposes, which the west often sees as authoritarian control of the citizenry, but rather a

[294] Burke-White W.W., 'Power Shifts in International Law: Structural Realignment and Substantive Pluralism', 56*Harvard International Law Journal* (2015), at 11–14.
[295] A. M. Sukumar, *The UN GGE Failed: Is International Law in Cyberspace Doomed as Well?*, 2017, Lawfare (available at https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well).
[296] Waxman, *supra* note 79, at 456.
[297] Giegreich, *supra* note 283, at 60–61; Koskenniemi, *supra* note 287, at 16–17.
[298] Waxman, *supra* note 79, at 448.

weapon that will be used by hostile actors and states.[299] Hence critics often state that constitutionalist view of international law often has a liberal hegemonic component. This does not necessarily have to be true, because constitutionalists encourage, just as the U.S. does in the GGE, that norms need to be universally accepted, which can be achieved via concessions in some cases. Constitutionalism is very ambitious, but the alternatives may be even more so, because more pluralistic regimes still have to deal with the same issues that require difficult institutional capacities that are often only present at institutions such as the UN.[300] Therefore, it is evident that, constitutionalism may be stagnating due to the controversy that cyber warfare is spurring. The political and strategic concerns are so overriding that concern over the legal basis, historical interpretation and state practise becomes a secondary issue. This may result in a more pluralistic legal order.

6.5 Constitutionalism and the difficulty of applying jus ad bellum and subsequent jurisprudence

As it is evident the state practise and opinio juris regarding art.2(4) and art.51 is divided and oppose one another. In addition, neither of the interpretations are sufficiently politically and geographically diverse to be deemed as a legitimate reinterpretation of the UN charter or customary law. This would warrant return to the textual historical meaning, and jurisprudence regarding said articles, especially if one adopts a constitutionalist view of the law. While constitutionalism would provide a common framework, it cannot be denied that there are several uncertainties and flaws within the application of the law as is. In the section analysing the preparatory work and the preamble of the charter, it was evident that there is bases for the term 'force' to be regarded as armed force only. However it is also clear that throughout the development of international law, jus ad bellum, considering the purpose of the UN charter and subsequent jurisprudence, the term 'force' could be interpreted more broadly based on the kinetic scale and effects rulings established in the ICJ Nicaragua and the ICJ nuclear weapons advisory opinion clarifying that 'force' applies to consequences rather than the means. This still leaves ambiguities as the current jurisprudence and UN charter does not clarify whether entirely non-kinetic effects could constitute force, leaving a major property of cyber unregulated. Regarding self-defence and art.51, while the jurisprudence shows that cyber could reach the damage threshold of an armed attack, it is evident that the 20th century

[299] Markoff, *supra* note 74.
[300] Bogdandy, *supra* note 279, at 241–242.

jurisprudence is not adapted to the efficiency of cyber operations, its domino effect and difficulties in deducing intention. Furthermore, the level of attribution and evidence required by jurisprudence is essentially impossible to achieve with cyber, even more so than conventional difficulties of attribution. The constitutionalist-like status of the UN charter and the UN system may also be preventing resorting to further clarifications by the ICJ or the international law commission on applicability of jus ad bellum to non-kinetic attacks. As rulings on such matters would unavoidably become part of the very same constitutionalist status, therefore if it is not sufficient at encompassing the properties of cyber, it may have severe consequences for the future of international law, peace and stability. Unlike national law, a stance taken by UN organs, cannot be simply repealed. Some pluralist, and many non-legalists believe that the reason the charter is followed is due to the retaliation potential based art.51 and security measures of the UN chapter VII, which results in security. But as new threats are emerging, such as cyber warfare and NSAs, states may feel like waiting for the UN Charter to develop outweighs the pressing security issues.[301] Critics have noted that the constitutionalist approach limits itself due to its resort to formalism and the utopian view of the present legal institutions.[302] While this may be a valid point of critique, constitutionalism has in the past, and in theory, offered a vision of the most predictable and stable international order. The alternative choice of pluralism may have even more caveats, as will be demonstrated in the next section.

6.6 Legal Pluralism

Legal pluralism is a theoretical approach towards international law that is in opposition to constitutionalism. The theory helps navigate the controversial norms that may deviate from a more constitutionalist centralised vision of international law. Legal pluralism is a legal perspective and a phenomenon that is in the very nature of international law. Historically legal pluralism was more apparent and prominent in national systems before the centralization of the state throughout the 18th and 19th centuries.[303] In contemporary form legal pluralism is often perceived as the struggle between state and non-state law, but overall it is better viewed as a way to understand the problems of legal centralization, as prescribed in legal

[301] Koskenniemi, *supra* note 287, at 14–15.
[302] *Ibid.*, at 23.
[303] Bianchi, *supra* note 28, at 228.

constitutionalism.[304] Legal pluralism in international law primarily focuses on the ongoing fragmentation, and accompanying emerging instruments such as soft law.[305] International law has fragmented in many ways, firstly into multiple distinct sphere such as trade law, environmental law and even sports law. Fragmentation is often based on adoption of new norms, instead of resorting to regulation by existing norms. Which may be precisely what non-western states are suggesting in relation to cyber.[306] Through the framework of legal pluralism, fragmentation is viewed more optimistically, because pluralists accept the notion that international law is a transnational network of different ideological and political norm systems.[307] Constitutionalism perceives fragmentation of international law as a serious flaw that needs to be combated in order to preserve the effectiveness of international law. Pluralism tries to explain the opposition between the fragmentation that can be seen with diverging interpretation of foundational laws, soft law, hybrid courts, emerging new norms and the movement to restore coherence to international law. It also tries to determine the effect a more pluralist legal system would have in an area of law. [308]

The emergence of pluralist views in a certain area of law is often very controversial and is common in both western and non-western legal thought and state practise. Different legal interpretation can emerge in response to new technology or significant events. This can be clearly seen the emergence of cyber. The lack of strict hierarchy in international law also tends to present opportunities for such changes.[309] States take actions that are unlawful under current international law but are considered justified or legitimate nonetheless, due to changing norms. This can be seen in the NATO intervention in Kosovo or the air strikes against Syria, that were carried to in the light of imminent humanitarian catastrophe. These actions have been deemed as unlawful, because they violate the principle of non-intervention but subsequently believed to be just and setting a future precedent for new norms in international law.[310] Therefore, in the case of jus ad bellum, pluralism appears to be an applicable

[304] *Ibid.*, at 229.
[305] Twining W., 'Normative and Legal Pluralism: A Global Perspective', 20*Duke Journal of Comparative and International Law* (2009), at 487.
[306] Koskenniemi, *supra* note 287, at 13.
[307] Hoffmann, *supra* note 280, at 976.
[308] Bianchi, *supra* note 28, at 231.
[309] Klabbers J. and Piiparinen T., *Normative Pluralism and International Law: Exploring Global Governance* (2013), Cambridge University Press; Koskenniemi, *supra* note 287, at 21.
[310] Klabbers and Piiparinen, *supra* note 309.

perspective to understand the potential effects the disagreement of the western and non-western states regarding the applicability of jus ad bellum laws to cyber warfare.

The primary components of the legal pluralism theory are that pluralistic legal systems would help situate the fragmenting legal order, result in higher representation, compliance and legitimacy. A legal pluralist transformation of international law would rely on the interconnected legal regimes that are based on their internal legitimate rational rules. The constrain of overarching laws as external factors would be limited, depending on the need for common principles and institutions to bridge the two systems. According to many legal pluralist this is not something that is unavoidable, but perhaps something that should be strived for, because it increases the fairness of the international legal system, makes it more representative and has the potential to take away some of the legal significance and influence states have.[311] Acknowledging genuine difference of interpretation arguably could enhance the legitimacy and effectiveness of international law. As states would be under the regulation of more tailored, representative norms, this would also increase compliance and the predictability of behaviour in times of tension or crisis. Of course, this does not mean that laws should be made separately, even in a pluralist view, the deliberations regarding law must attempt to reach the highest consensus possible.[312] Therefore, in a legal pluralistic theoretical approach it could be expected that a pluralist view on the applicability of jus ad bellum to cyber would provide somewhat separate regimes that would coexist, and would strictly adhere to their internal rules. However, as jus ad bellum laws are so paramount, it becomes crucial to investigate whether this area of international law could ever exist in plurality.

There are several limitations that legal pluralism, and the strive towards its goal within the current international legal system, presents in the current legal order. These are primarily the following:

- Politicization of international law
- Reduction of the necessity to cooperate
- Inapplicability to certain foundational laws
- Lack of institutional development to accommodate a plurality of regimes

[311] Hoffmann, *supra* note 280, at 976–977.
[312] Bianchi, *supra* note 28, at 232.

In a legal pluralist view it can be envisioned that the interpretative dispute over jus ad bellum laws and their applicability would result in a more pluralistic regime. However, this would be extremely difficult to navigate. As the western and opposing western states have used extensive efforts to continue deliberations outside of the GGE, it shows that potential for real fragmentation of the law. The new GGE is also accompanied by a parallel open working group set up by Russia and China, showcasing two opposing chambers of deliberation.[313] Given that all parties to the dispute refuse to offer concession in the upcoming UN GGE and the OWG process and state practise remains not sufficient to alter the interpretation or custom of jus ad bellum laws, then two parallel pluralistic interpretations of the law may coexist. There is also a possibility that the lack of consensus will result in a legal stalemate which will prevent formation of norms in cyberspace until a later time, leaving it relatively unregulated and unpredictable. A pluralistic regime would entail two coexisting interpretations of how jus ad bellum applies to cyber. A western bloc that asserts that cyber can be use of force and an armed attack, to which it can respond with conventional forces. In contrast to, non-western bloc that reject cyber as use of force or armed attack and condemns conventional responses to cyber incidents. Said bloc would also condemn any interference into their cyber sovereignty. Major inquiries remain as to whether such a regime is possible, if it would encompass the abuse prone cyber properties and manage to create a more legitimate, yet secure international legal order.

6.7 Legal pluralism and the ideological views of cyber warfare

Legal pluralism would serve as a more representative approach towards the different conceptualizations of cyber. It would also allow to regulate the diverging conceptualized spectrum of cyber properties. The main issue of pluralism that persists, is that it is not necessary to cover all aspects of cyber within jus ad bellum, and pluralism would not regulate crucial properties efficiently enough. Given that the interpretative division remains entrenched, this would result in two relatively equally legitimate legal orders. International law would have to reconcile two blocks, that disagree on what constitutes force, and the instances when self-defence can be used. Firstly, when it comes to different conceptualizations, assuming that a pluralistic system is possible, it would take into account

[313] Delerue, *supra* note 62, at 310–311.

the views of cyber by both blocs. This would form geographical fragmentation of the law where the interpretation of the law differs between regions.[314] Technically it would allow Russia, China and likeminded states to maintain their view of jus ad bellum non-applicability, strict cyber sovereignty and total non-interference view. This would form expectations to comply with such norms at least between these likeminded states. On the other side, western states would maintain their view that cyber can be and will be used for military purposes. It will maintain the right to respond to cyber as if it was force or an armed attack as per art.2(4) and art.51. Interestingly if Russia and China truly believed that cyber should not be used for military purposes, it would not use cyber-attacks against the west, hence they would never face a conventional response or the wests application of jus ad bellum to cyber. Perhaps reciprocally the west would even respect the oppositional non-western norms, and not interfere in their cyber sovereignty. This, of course is overly optimistic, idealistic and a naïve view, because Russia and the aforementioned non-western states have used cyber-attacks and will continue to do so.[315] Furthermore, the way Russia envisions sovereignty is contradictory, because they cannot claim cyber to not be a use of force, while at the same time proclaiming that cyber should not be used to interfere with their sovereignty, because sovereignty is primarily a concept employed to prevent or condemn the use of force against other states. UN Charter art.2(4) and art.51 are based on territorial integrity and political independence, which are core principles of sovereignty. Therefore, if one wants actors to not interfere with one's sovereignty one should accept cyber as use of force.[316]

Pluralistic cyber jus ad bellum regimes do not necessitate that opposing states with different interpretations obey the exact principles of their opposing regime that they reject. That is the nature and meaning of a pluralist system.[317] This is especially evident when comparing cyber jus ad bellum to more pluralistic areas of the law like *'responsibility to protect'*, the emerging western norm that states have responsibility to intervene in other states, despite their sovereignty, to stop ongoing crimes against humanity, genocide. This has been opposed by many non-western states. Some western states intervened based on this notion despite

[314] *Ibid.*, at 311.
[315] Euractiv, *Georgia Reports Massive Cyber-Attack 'Carried out by Russia'*, 2020 (available at https://www.euractiv.com/section/eastern-europe/news/georgia-reports-massive-cyber-attack-carried-out-by-russia/).
[316] Fassbender B. 'Sovereignty and Constitutionalism in International Law', in *Sovereignty in Transition* (2003) , at 128–134.
[317] Bianchi, *supra* note 28, at 230–232.

opposition by non-western states, making it evident that in regard to cyber jus ad bellum fragmentation, the western bloc would continue to respond to cyber-attacks with conventional force.[318] Hence irrespective of how persistently Russia objects to the application of jus ad bellum to cyber, the conventional advantage of U.S. will remain. Therefore, in a pluralist legal order, the west would respond with force to cyber originating from Russia or China, in all cases viewing it as a violation of art.2(4), meanwhile Russia would continue to conduct cyber-attack against the west because they would maintain that it is not use of force. Therefore, it appears that a pluralist regime would allow to solidify the ideological conceptions of cyber into international norms, but it would not change the conduct of states from what it is now. It would arguably make it even more chaotic and unpredictable. This perhaps shows that Russia and China are stalling norm development and the efficient application of international law, in order to use the ambiguity to wage cyber operations against the west in a legal vacuum for as long as possible. It also indicates that the only real way to achieve a real change in behaviour in international relations is for a certain norm to be universalised in a constitutionalist approach.

6.8 Legal pluralism, the reconciliation of cyber properties and neglect of long-standing legal principles

Acceptance of both of the interpretations in a pluralistic manner would not account for some crucial properties of cyber. Russia's proposed norms of non-militarization and non-interference in cyber, can become obsolete because cyber is developing so rapidly, that it has potential to become the cheapest and most effective tool of warfare. [319] The non-militarization of cyber as a norm primarily focuses on states, and while Russia and China agreed in the earlier GGE's that states should not allow NSAs to use their infrastructure, therefore their proposed norms say little about the broader proliferation of cyber capacity of NSAs.[320] Since all states accept that NSAs will be a threat regarding cyber, then they reject the very strict cyber 'restraint' view that only states can utilize high capacity cyber operations. Meaning that states believe the possibility of NSAs to carry out high level cyber operations is real. Therefore, the non-militarization and non-interference norms that Russia and China propose

[318] Harold Hongju Koh, *Syria and the Law of Humanitarian Intervention (Part II: International Law and the Way Forward) By Harold Hongju Koh*, 2013, Ejiltalk (available at https://www.ejiltalk.org/syria-and-the-law-of-humanitarian-intervention-part-ii-international-law-and-the-way-forward/).
[319] Kello, *supra* note 3, at 6–7.
[320] CCDCOE, *supra* note 57; General Assembly, *supra* note 59; Henriksen, *supra* note 56, at 3.

disregard the major contemporary issue of the threat of NSAs and self-defence against NSAs. Particularly considering how much easier it is for states to support NSAs with cyber means. Russia claims that attribution in cyber is often impossible, and instead of working on a set of norms for a sufficient level of evidence for attribution, they deny the applicability of the law itself. However, if the law is left with no attribution standards, no feasible accepted way of attributing attacks, then cyber becomes a very attractive tool to militarize for states and NSAs, which goes against the norms Russia proposes. Furthermore, the non-applicability of jus ad bellum laws, and non-militarization does not consider the orders of effect of cyber-attacks, that can spread unintentionally and cause widespread damage. Therefore, a pluralistic existence of both interpretations, and particularly the persistence of the non-western interpretation would only introduce even more uncertainty as to how the international community is supposed to respond to cyber NSAs and orders of effect of cyber-attacks.

Inability of the pluralistic regime to account for the aforementioned properties of cyber would result in increased instability, because of the inability to apply the law consistently. This is because jus ad bellum laws like the prohibition of the use of force and self-defence are jus cogens norms. These norms are universal norms that cannot be deviated from by states, because it is accepted that without these norms there would be grave conflict in the world.[321] The presence of a pluralistic set of interpretation of jus ad bellum laws, would strictly speaking imply, that western states cannot use self-defence within or against the states that reject such interpretation. This would leave states without a clear framework to distinguish appropriate principles when responding to cyber-attack attacks with kinetic and non-kinetic effects. Furthermore, accepting the existence of the Russian and Chinese interpretation would create a geographical area where long standing legal principles previously codified as part of the jus ad bellum laws, like necessary damage thresholds, intention, attribution, level of evidence, necessity and proportionality, would be inapplicable. Such a predicament would raise tensions in any sort of cyber crisis, where a state or an NSA, utilizes cyber operations. That is because the opposing non-western bloc would deem any interference by western states on the basis of the applicability of jus ad bellum, as a grave violation. While the west would deem any denial by Russia or China to use self-defence, as an unacceptable suggestion. This also highlights one of the major issues with pluralism. The fact that pluralistic regimes attempt to address the same global issues, but with diluted and segregated institutional capacity. It would be very

[321] Roberts and Sivakumaran, *supra* note 8, at 101–102.

difficult to formally reconcile any issues between these two pluralistic regimes without adherence to the very same constitutionalist institutions such as the UN.[322] Fragmentation and pluralism take away the ability to apply international law from judicial bodies that are most appropriate for it. Arguably that is one of the main reasons to resort to constitutionalism to ensure a central medium to resolve legal conflicts, even if interpretations diverge.[323] This would inherently raise tensions, increase conflict and go against the purpose of the UN Charter. This perhaps highlights the obvious peculiarity of pluralism, that it has the potential to destroy universality that brings predictability and stability to the international legal community needed to prevent war. Therefore, as it is evident that the coexistence of two parallel interpretations in a pluralist system, would increase the unpredictability and tensions between the already present division between western and some non-western states. It makes international relations, chaotic and very difficult to deal with scenarios that are likely to happen due to the properties of cyber, without immediately violating one of the blocs' interpretation of the law. Hence constitutionalism and universalised acceptance of the applicability of the jus ad bellum international law to cyber warfare may be the most appropriate path forward.

[322] Bogdandy, *supra* note 279, at 241–242.
[323] Dunoff and Trachtman, *supra* note 28, at 6–8.

7. Conclusion

Cyber warfare remains an area that requires a tremendous academic effort to study and aid in the understanding of how this domain may affect peace, security and international law. This thesis attempted to contribute to this matter, by utilizing a multidisciplinary qualitative approach that considered international law, and the effects of politics and technology upon it. To demonstrate the emerging jus ad bellum issues of international law applicable to cyber, the thesis had to begin with the fundamental conceptualization of cyber and its properties. The analysis of the differing conceptualization of cyber warfare should serve to illuminate the bases of the ongoing struggle between western and some non-western states in international law. It showed that western states view cyber as a very technical, technological tool of warfare, while the global powers of Russia and China view it as primarily a society impacting tool. The properties of cyber and its potential to revolutionise warfare were crucial to determine, in order to highlight the challenges that jus ad bellum international law may be facing. Through such analysis, the uncertainty and the capacity of cyber has been highlighted. These stem from the lack of thorough case studies, and the very scientifically complex nature of cyber. In addition, the properties of instantaneousness, uncertainty of expectations and collateral damage have also been demonstrated as alarming factors of cyber warfare. Furthermore, it has been argued that cyber has the potential to proliferate malicious capacity to hostile non-state actors. These properties serve as the crucial point of reference when considering the jus ad bellum laws regulating the use of force and self-defence.

The analysis of the international law regulating the use of force outlined a multitude of emerging issues. The first and perhaps the most key legal issue is the divided interpretation of the applicability of the art.2(4) to cyber. Due to the aforementioned differing conceptualizations of cyber as information space meant for societal transformation, Russia, China and other non-western states interpret the prohibition of the use of force inapplicable to cyber. The political reasoning behind these decisions is also crucial for legal experts to understand. As highlighted in the thesis, the rejection of jus ad bellum applicability serves to prevent conventional responses from the west to malicious cyber-attacks, and to secure control over their population. The west interprets the law to be applicable to cyber due to their security culture and interconnectedness in cyber. While the political and strategic influences remain significant, there are also legal basis for the interpretation of both sides. Art.2(4) interpreted, as per VCLT, shows that while the textual meaning of force is not indicative of its scope, the

UN charters context and preamble, shows that the original intention of the article was to apply it only to armed conventional force. Hence it arguably would not cover cyber warfare. Historic state practice also shows that force was intended to mean armed force, however contemporary state subsequent practise is evolving. Many states have implicitly or explicitly accepted that jus ad bellum applies to cyber, but it appears that there is no clear geographically diverse majority that supports the applicability. Considering most affected countries also offers little insight, as Russia, China and US are the states that are most affected by cyber-attacks. Preparatory work of art.2(4) also indicates that the prohibition was intended to apply to armed force. Therefore, the second jus ad bellum issue is that there is a case to be made that art.2(4) does not apply to cyber due to its transformative non-kinetic nature. This however will not set international law at a dead end because state practise is still developing and there are also significant legal bases for the applicability of art.2(4) to cyber warfare. Revisiting the purpose and preparatory work for the UN charter there is clear indication that the prohibition of use of force should be all inclusive and expand with new technology. Especially considering case law and jurisprudence that establishes that the primary concern of art.2(4) is the scale and effects or the kinetic consequences, rather than the source, expanding it to cyber. However, this still introduces a third issue, as the jurisprudence affirms that the, if art.2(4) did apply, it would only encompass non-kinetic attacks. Further studies should perhaps attempt to explore, the legal principles that could be invoked to address entirely non-kinetic effects of cyber-attacks.

The analysis of the international law regulating self-defence outlined additional jus ad bellum issues in respect to cyber. If the scale and effect jurisprudence and state practise renders the jus ad bellum laws applicable to cyber, then further issues persist with regards to self-defence criteria outlined in case law. Case law shows that if a cyber-attack reached a certain level of grave damage akin to that of a kinetic attack carried out by regular forces it could constitute an armed attack warranting self-defence. However, the first significant jus ad bellum issue is that of reaching this established threshold with cyber warfare is very difficult because cyber properties make it non-kinetic, dispersed and more effective in some cases. Furthermore, as networks are intertwined within different jurisdictions, and cyber-attacks have many unintended and indirect effects it will be difficult to gauge the damage. The second issue stemming from the jurisprudence is attribution. Currently attacks need to be attributed to a state with clear and conclusive evidence. However, these requirements are too stringent for cyber, because cyber is anonymous, transboundary and prone to spoofing. Attribution

becomes particularly difficult when attacks are carried out by independent non-state actors, therefore international law would have to accept a more controversial emerging norm based on some customary law, that allows self-defence with inability or unwillingness of states to deal with NSAs as a sufficient level of attribution. In cyber this would cause a very unstable environment prone to conflict. A third jus ad bellum issue is that of necessity. Necessity is a crucial customary principle of self-defence that would be difficult to apply to cyber. That is because it is impossible to prove whether a state had alternative cyber means to deal with an attack before resorting to self-defence. Even a malicious denial of having such alternatives would be plausible, and hard to discredit. The fourth and final jus ad bellum issue concerned the customary principle of proportionality in self-defence. That is because judging the proportional kinetic response to cyber-attacks is an uncertain matter, while any cyber response in self-defence carries the risk of having unintended or domino effects. Proportionality becomes a challenging principle.

After consideration of the strict division of interpretation regarding jus ad bellum between western and some non-western states, as well as the genuine difficulty of applying art.2(4) and art.51 to cyber warfare, it becomes essential to consider the future of international law in cyberspace. That is where the resort to constitutionalism and pluralism provided insight into the reasons and outcomes regarding the regulation of cyber warfare. Analysis of the current international legal order and the strive to centralise it further showcased several issues. The constitutionalist approach adopted by western states, while just, has difficulties in accounting for diverging opinions, and transformative change such as cyber warfare. This jolts some non-western states to create and urge the adoption of different norms in a more pluralistic manner. Pluralism serves well in accommodating different political and legal stances of western and non-western states. However, the existence of separate interpretative regimes regarding such fundamental laws as jus ad bellum, would make it difficult to navigate, and raise tensions. In fact, it can be argued that it would contribute little to stability because the conduct of states would remain as it is now, not in tandem. Therefore, cyber should remain under the magnifying glass of legal experts. Future conflicts should be dissected to draw conclusions on how legal principles of conclusive evidence, attribution, proportionality and necessity may work in cyberspace. Subsequent practise of interpretation and application should be at the forefront of legal studies in order to help the international community reconcile its concerns over such a transformative matter and reach a consensus for the sake of peace and stability.

8. Bibliography

Addendum to Summary Report of Twelfth Meeting of Committee I/1 (1945), Documents of the United Nations Conference on International Organization.

Advisory Committee on the Issues of Public International Law and Advisory Council on International Affairs, 'Cyber Warfare, No 77, AIV / No 22, CAVV', *Cyber Warfare* (2011).

American Society of International Law, *The World Court Finds That U.S. Attacks on Iranian Oil Platforms in 1987-1988 Were Not Justifiable as Self-Defense, but the United States Did Not Violate the Applicable Treaty with Iran*, 2013 (available at https://www.asil.org/insights/volume/8/issue/25/world-court-finds-us-attacks-iranian-oil-platforms-1987-1988-were-not).

Attorney General's Office, *Cyber and International Law in the 21st Century*, 2018.

Baker, Roozbeh Rudy B., 'Customary International Law in the 21st Century: Old Challenges and New Debates', 21 *European Journal of International Law* (2010) 173–204.

Barbour, Stephanie A. and Salzman, Zoe A., '"The Tangled Web': The Right of Selfdefence against Non-State Actors in the Armed Activities Case', 42 *Journal of Urban Affairs* (2018) 1–17.

Barriga, Stefan and Grover, Leena, 'A Historic Breakthrough on the Crime of Aggression', 105 *The American Journal of International Law* (2011) 517–533.

Baumard P., *Cybersecurity in France* (2017), Springer.

BBC, *US 'Launched Cyber-Attack on Iran Weapons Systems'*, 2019 (available at https://www.bbc.com/news/world-us-canada-48735097).

Becker T., 'The Agency Paradigm: The Principle of Non-Attribution and Its Exceptions', in *Terrorism and the State: Rethinking the Rules of State Responsibility* (2006) 43–78.

Besson S., 'Whose Constitution(s)? International Law, Constitutionalism and Democracy', in *Ruling the World? Constitutionalism, International Law, and Global Governance* (2009) 381–407.

Bethlehem, Daniel, 'Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by NonState Actors', (2011) 1–8.

Bianchi A., 'Constitutionalism and Global Governance', in *International Law Theories: An Inquiry into Different Ways of Thinking* (2016) 44–71.

Bianchi A., 'Legal Pluralism', in *International Law Theories: An Inquiry into Different Ways of Thinking* (2017) 227–245.

Black's Law Dictionary, *What Is Force?* (available at https://thelawdictionary.org/force/).

Boas T.C., 'Weaving the Authoritarian Web: The Control of Internet Use in Nondemocratic Regimes', in J. Zysman and A. Newman (eds.), *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology* (2006) 373–391.

Boer, Lianne J.M., 'Restating the Law 'As It Is': On the Tallinn Manual and the Use of Force in Cyberspace', 5 *Amsterdam Law Forum* (2013) 4–18.

Bogdandy, Armin von, 'Constitutionalism in International Law: Comment on a Proposal from Germany', 47 *Harvard International Law Journal* (2006) 223–242.

Burchard H. Von Der, *Merkel Blames Russia for 'Outrageous' Cyberattack on German Parliament*, 2020 (available at https://www.politico.eu/article/merkel-blames-russia-for-outrageous-cyber-attack-on-german-parliament/).

Burke-White, William W., 'Power Shifts in International Law: Structural Realignment and Substantive Pluralism', 56 *Harvard International Law Journal* (2015) 1–79.

CCDCOE, *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at*

the UN General Assembly, 2017, Nato Ccdcoe (available at https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html).
Chatham House, *Principles of International Law on the Use of Force by States in Self-Defence* (2005).
Clausewitz C. von, *On War* (1989), Princeton University Press.
Council on Foreign Relations, *Brazil-EU Cyber Cooperation: Swinging Bridges on the Road to Stability in Cyberspace*, 2020 (available at https://www.cfr.org/blog/brazil-eu-cyber-cooperation-swinging-bridges-road-stability-cyberspace).
Crootof, Rebecca, 'Change Without Consent: How Customary International Law Modifies Treaties Rebecca', 41 *Yale Journal of International Law* (2016) 238–299.
Cryer R. et al., *Research Methodologies in EU and International Law* (2011).
Cyber Security Insiders, *List of Countries Which Are Most Vulnerable to Cyber Attacks*, 2020 (available at https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/).
Dam, Chris Van, 'Extraterritorial Law-Enforcement : Combating Non-State Actors', 18 (2013) 17–29.
Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (2019).
Delerue, François, 'Reinterpretation or Contestation of International Law in Cyberspace?', 52 *Israel Law Review* (2019) 295–326.
Doyle M.W., 'The UN Charter - A Global Constitution?', in *Ruling the World? Constitutionalism, International Law, and Global Governance* (2009) 113–149.
Duhaime's Law Dictionary, *Physical Force Definition*, 2020 (available at http://www.duhaime.org/LegalDictionary/P/PhysicalForce.aspx).
Dunoff J. l. and Trachtman J.P., 'A Functional Approach to International Constitutionalization', in *Ruling the World? Constitutionalism, International Law, and Global Governance* (2009).
Enabulele, Amos O., 'Use of Force by International/Regional Non- State Actors: No Armed Attack, No Self-Defence', 1 *European Journal of Law Reform* (2015) 209–229.
Euractiv, *Georgia Reports Massive Cyber-Attack 'Carried out by Russia'*, 2020 (available at https://www.euractiv.com/section/eastern-europe/news/georgia-reports-massive-cyber-attack-carried-out-by-russia/).
Farwell, James P. and Rohozinski, Rafal, 'Stuxnet and the Future of Cyber War', 53 *Global Politics and Strategy* (2011) 23–40.
Fassbender B., 'Sovereignty and Constitutionalism in International Law', in *Sovereignty in Transition* (2003) 115–143.
Fisher, Elizabeth et al., 'Maturity and Methodology: Starting a Debate about Environmental Law Scholarship', 21 *Journal of Environmental Law* (2009) 213–250.
Fitzmaurice M., 'The Practical Working of the Law of Treaties', in M. D. Evans (ed.), *International Law* 5th (2018) 138–173.
Fraser, Adeo, 'From the Kalashnikov to the Keyboard: International Law's Failure to Define a 'Cyber Use of Force' Is Dangerous and May Lead to a Military Response to a 'Cyber Use of Force'', 15 *Hibernian Law Journal* (2016) 86–113.
Gardam J., *Necessity, Proportionality and the Use of Force by States* (2004), Necessity, Proportionality and the Use of Force by States.
General Assembly, 'A/C.1/73/PV.22', .
General Assembly, 'A/C.1/73/PV.31', (2018).
General Assembly, UN General Assembly Resolution 70/174, UN Doc. A/Res/70/174, 2015.
German Parliament, *Antwort Der Bundesregierung Auf Die Kleine Anfrage Der*

Abgeordneten Stephan Thomae, Jimmy Schulz, Manuel Höferlin, Weiterer Abgeordneter Und Der Fraktion Der FDP (2018).
Giegreich, Thomas, 'The Is and the Ought of International Constitutionalism: How Far Have We Come on Habermas's Road to a 'Well'Considered Constitutionalization of International Law"?', 10 *German Law Journal* (2010) 31–62.
Grant J.P., Barker J.C. and Parry C., *Parry and Grant Encyclopaedic Dictionary of International Law* (2009).
Gray C., *International Law and the Use of Force* (3rd ed., 2008).
Gray C., 'The Use of Force and the International Legal Order', in *International Law* 5th (2018) 614–651.
Haataja S., *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics* (1st ed., 2018).
Hammes, T., 'Fourth Generation Warfare Evolves, Fifth Emerges', 87 *Military Review* (2007) 14.
Harold Hongju Koh, *Syria and the Law of Humanitarian Intervention (Part II: International Law and the Way Forward) By Harold Hongju Koh*, 2013, Ejiltalk (available at https://www.ejiltalk.org/syria-and-the-law-of-humanitarian-intervention-part-ii-international-law-and-the-way-forward/).
Harrison Dinniss H., *Computer Network Attacks as a Use of Force in International Law* (2012), Cyberwarfare and the Laws of War.
Hemsley, Kevin and Fisher, Ronald, 'A History of Cyber Incidents and Threats Involving Industrial Control Systems', 542 *IFIP Advances in Information and Communication Technology* (2018) 215–242.
Henriksen, Anders, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace', 5 *Journal of Cybersecurity* (2019) 1–9.
Herpen M.H. Van, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (2016).
Hoffmann F., 'International Legalism and International Politics', in A. Orford and F. Hoffmann (eds.), *The Oxford Handbook of the Theory of International Law* 1st (2016) 955–985.
Hoffmann F., 'International Legalism and International Politics', in A. Orford and F. Hoffmann (eds.), *Oxford Handbook of the Theory of International Law* (2016) 955–988.
Huntley, Todd C., 'Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare', 60 *Naval Law Review* (2010) 1–40.
Ingo Venzke, *How Interpretation Makes International Law - On Semantic Change and Normative Twists* (2012).
International Court of Justice, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, 19 December 2005.
International Court of Justice, Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgement, 6 November 2003.
International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, 27 June 1986.
International Court of Justice, North Sea Continental Shelf Cases, Judgement, 20 February 1969.
International Court of Justice, The Corfu Channel Case (United Kingdom v Albania), Judgement, 9 April 1949.
International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001), Yearbook of the International Law

Commission.
International Law Commission, First Report on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties, UN Doc. A/CN.4/660, 2013.
International Law Commission, Second Report on Subsequent Agreements and Subsequent Practice, UN Doc. A/CN.4/671, 2014.
International Law Commission, 'Summary Records of the Second Session, A/CN.4/SER.A/1950', in *Yearbook of the International Law Commission* vol. 1 (1950) 1–321.
Kaldor, Mary, 'In Defence of New Wars', 2 *International Journal of Security and Development* (2013) 1–16.
Kaspersky, *Cyberthreat Real-Time Map*, 2020 (available at https://cybermap.kaspersky.com/stats/).
Kello, Lucas, 'The Meaning of the Cyber Revolution Perils to Theory and Statecraft', 38 *International Security* (2013) 7–40.
Kello L., *The Virtual Weapon and International Order*, The Virtual Weapon and International Order (1st ed., 2017).
Kellogg F.B. and Briand A., General Treaty for Renunciation of War as an Instrument of National Policy, 1928.
Kittichaisaree K., *Public International Law of Cyberspace* (2017).
Klabbers J. and Piiparinen T., *Normative Pluralism and International Law: Exploring Global Governance* (2013), Cambridge University Press.
Koh H.H., *International Law in Cyberspace*, 2012, U.S. Department of State Diplomacy in Action (available at https://2009-2017.state.gov/s/l/releases/remarks/197924.htm).
Korošec, Tina and Veber, Maruša Tekavčič, 'Right to Self-Defence against Non-State Actors in the Context of Fight against Terrorism', 76 *Zbornik Znanstvenih Razprav* (2016) 41–68.
Koskenniemi, Martti, 'Constitutionalism as Mindset: Reflections on Kantian Themes about International Law and Globalization', 8 *Theoretical Inquiries in Law* (2007) 9–36.
Kovacs E., *Maersk Reinstalled 50,000 Computers After NotPetya Attack*, 2018, Security Week (available at https://www.securityweek.com/maersk-reinstalled-50000-computers-after-notpetya-attack).
Lorenzo Carrazana, 'The Economics of Cybersecurity and Cyberwarfare: A Case Study' (2018) (available at ECON Colloquium).
Markoff M.G., *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2017, United States Department of State (available at https://www.state.gov/explanation-of-position-at-the-conclusion-of-t…rmation-and-telecommunications-in-the-context-of-international-sec/).
Mehta P.W., *India's National Cybersecurity Policy Must Acknowledge Modern Realities*, 2019 (available at https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/).
Memorandum to the Foreign Affairs Select Committee, Prime Minister's Response to the Foreign Affairs Select Committee's Second Report of Session 2015-16: The Extension of Offensive British Military Operations to Syria, 2015.
Ministère des Armées, *Éléments Publics De Doctrine Militaire De Lutte Informatique Offensive* (2019).
Ministère des Armées, *International Law Applied to Operations in Cyberspace* (2019).
Ministry of Defence, *Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace*, 2018 (available at

https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html).
Ministry of Defence, *Diplomacy and Defense in Cyber Space*, 2018 (available at https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/).
Ministry of Defence, *Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group* (2015).
Moloo, Rahim, 'Changing Times, Changing Obligations? The Interpretation of Treaties over Time', 106 *American Society of International Law* (2012) 261–264.
Münkler H., 'Old and New Wars', in M. D. Cavelty and V. Mauer (eds.), *The Routledge Handbook of Security Studies* (2010) 190–199.
National Cyber Security Centre, *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, 2018 (available at https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed).
Nye, J., 'Normative Restraints on Cyber Conflict.', 1 *Cyber Security Project* (2018) 331–342.
Osawa, Jun, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', 24 *Asia-Pacific Review* (2017) 113–131.
Paddeu, Federica I., 'Use of Force against Non-State Actors and the Circumstance Precluding Wrongfulness of Self-Defence', 30 *Leiden Journal of International Law* (2017) 93–115.
Paddeu, Federica I., 'Use of Force against Non-State Actors and the Circumstance Precluding Wrongfulness of Self-Defence', 30 *Leiden Journal of International Law* (2017) 93–115.
Paine J., *Book Review of 'How Interpretation Makes International Law: On Semantic Change and Normative Twists'* (2013), Australian Yearbook of International Law.
Petersmann, Ernst-Ulrick, 'How to Reform the UN System? Constitutionalism, International Law, and International Organizations', 10 *Leiden Journal of International Law* (1997) 421–474.
Pompeo M.R., *The United States Condemns Russian Cyber Attack Against the Country of Georgia*, 2020 (available at https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/).
President of the Republic at the Opening of CyCon 2019, 2019 (available at https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/).
RDDC, Joint Doctrine for Military Cyberspace Operations, September, 2019.
Representaciones Diplomáticas de Cuba en El Exterior, *Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.*, 2017 (available at http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information).
Roberts A. and Sivakumaran S., 'The Theory and Reality of the Sources of Law', in M. D. Evans (ed.), *International Law* 5th (2018) 89–119.
Roguski P., *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, 2020, Just Security (available at https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/).
Roscini M., 'Cyber Operations and the Jus Ad Bellum', in *Cyber Operations and the Use of Force in International Law* (2014) 43–116.

Ruys, Tom, 'The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are "Minimal Uses of Force Excluded from UN Charter Article 2(4)?', 108 *The American Journal of International Law* (2014) 159–210.
Schmitt, Michael N., 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37 *Columbia Journal of Transnational Law* (1999).
Schmitt M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., 2017).
Shackelford, Scott J., 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27 *Berkeley Journal of International Law* (2009) 192–251.
Shelton D., 'International Law and 'Relative Normativity'', in M. D. Evans (ed.), *International Law* 4th (2014) 137–165.
Solis, Gary D., 'Cyber Warfare', 219 *Military Law Review* (2014) 1–19.
Special Rapporteur, Draft Code of Offences against the Peace and Security of Mankind, A/CN.4/25 Draft, vol. 2, 1950.
Statute of the International Court of Justice, 1945.
'Summary Report of Eleventh Meeting of Committee I/1', in *Documents of the United Nations Conference on International Organization* vol. 6 (1945) 1–717.
Summary Report of Twelfth Meeting of Committee I/1 (1945), Documents of the United Nations Conference on International Organization.
Van Steenberghe, Raphaël, 'Self-Defence in Response to Attacks by Non-State Actors in the Light of Recent State Practice: A Step Forward?', 23 *Leiden Journal of International Law* (2010) 183–208.
Valeriano B. and Maness R., Cyber War Versus Cyber Realities, 2015.
Väljataga A., *Joint Air & Space Power Conference*, 2019, CCDCOE (available at https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf).
Stemmet, Andre, 'Book Review of 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice', 1 (2013) 297–302.
Sukumar A.M., *The UN GGE Failed: Is International Law in Cyberspace Doomed as Well?*, 2017, Lawfare (available at https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well).
Sukumar A.M., *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, 2017 (available at https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well).
Tams, Christian J. and Devaney, James G., 'Applying Necessity and Proportionality to Anti-Terrorist Self-Defence', *Israel Law Review* (2012).
The Avalon Project, *British-American Diplomacy The Caroline Case, Enclosure 1-Extract from Note of April 24,1841*, The Yale Law School Lillian Goldman Law Library (available at https://avalon.law.yale.edu/19th_century/br-1842d.asp).
The Covenant of the League of Nations, 1919.
The International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996.
The Ministry of Foreign Affairs of the Russian Federation, *Convention on International Information Security*, 2016.
The Ministry of Foreign Affairs of the Russian Federation, *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere*, 2017 (available at https://coe.mid.ru/en_GB/sotrudnicestvo-v-sfere-pravoporadka/-/asset_publisher/jYpWpmrO5Zpk/content/otvet-specpredstavitela-prezidenta-

rossijskoj-federacii-po-voprosam-mezdunarodnogo-sotrudnicestva-v-oblasti-informacionnoj-bezopasnosti-a-v-krutskih-n?inhe).
The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (2019).
Thirlway H., 'The Sources of International Law', in M. Evans (ed.), *International Law* 4th (2014) 91–117.
Tladi D., *An Assessment of Bethlehem's Principles on The Use of Force Against Non- State Actors in Self-Defence in the Light of Foundational Principles of International Law* (2012).
Tsagourias, Nicholas, 'Necessity and the Use of Force: A Special Regime', 41 *Netherlands Yearbook of International Law* (2010) 11–44.
Tselikov, Andrey, 'The Tightening Web of Russian Internet Regulation', *SSRN Electronic Journal* (2014).
Twining, William, 'Normative and Legal Pluralism: A Global Perspective', 20 *Duke Journal of Comparative and International Law* (2009) 473–518.
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 Recent. A/69/723, 2015.
UN General Assembly, UN GAOR, 65th Sess., 1st Comm. 15th Mtg. UN Doc. A/C.1/65/PV.15, 2010.
UN General Assembly, UN GAOR, 67th Sess., 1st Comm. 17th Mtg. UN Doc. A/C.1/67/PV.17, 2012.
UN General Assembly, *UN GAOR, 68th Sess., 1st Comm. 20th Mtg. UN Doc. A/C.1/68/PV.20* (2013).
UN General Assembly, UN GAOR, 72nd Sess., 1st Comm. 19th Mtg. UN Doc. A/C.1/72/PV.19, 2017.
UN General Assembly, UN GAOR, 72nd Sess., 1st Comm. 20th Mtg. UN Doc. A/CA/C.1/72/PV.20, 2017.
UN General Assembly, UN General Assembly Resolution 26/25, UN Doc. A/Res/26/25 'Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations', 1970.
UN Security Council, Identical Letters Dated 29 December 2015 from the Permanent Representative of the Syrian Arab Republic to the United Nations Addressed to the Secretary-General and the President of the Security Council, UN Doc. A/70/673–S/2015/1048, 2016.
UN Security Council, Letter Dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations Addressed to the President of the Security Council, UN Doc. S/2015/946, International Organization, 2015.
UN Security Council, Letter Dated 11 January 2016 from the Permanent Representative of Denmark to the United Nations Addressed to the President of the Security Council, UN Doc. S/2016/34, 11, 2016.
UN Security Council, Letter from the Permanent Representative of the United States of America to the United Nations Addressed to the Secretary-General, UN Doc. S/2014/695, 2014.
United Nations, Charter of the United Nations, Art. 1, 1945.
United Nations, Charter of the United Nations, Art. 103, 1945.
United Nations, Charter of the United Nations, Art.2(4), 1945.
United Nations, Charter of the United Nations, Art.51, 1945.
United Nations, Charter of the United Nations, Chapter I: Purposes and Principles, 1945.
United Nations, Charter of the United Nations, Chapter VII: Action with Respect to Threats

to the Peace, Breaches of the Peace, and Acts of Aggression, 1945.
United Nations, Charter of the United Nations, Preamble Para. 7, 1945.
United Nations, *Charter of the United Nations, Preamble Para.1* (1945).
United Nations, 'UN GAOR, 69th Sess., 1st Comm. 19th Mtg., UN Doc. A/C.1/69/PV.19', (2014) 1–18.
United Nations, UN GAOR, 71st Sess., 1st Comm. 19th Mtg. UN Doc. A/C.1/71/PV.19, 2016.
United Nations, UN GAOR, 73rd Sess., 1st Comm. 19th Mtg. UN Doc. A/CA/C.1/73/PV.19, 2018.
United Nations, Vienna Convention on the Law of Treaties, Art. 31, 1969.
United Nations, Vienna Convention on the Law of Treaties, Art. 32, 1969.
United Nations Office for DIssarmament Affairs, *Group of Governmental Experts*, 2020 (available at https://www.un.org/disarmament/group-of-governmental-experts/).
US Joint Staff, *Cyberspace Operations* (2018), Joint Publication.
UN General Assembly Resolution 56/19, UN Doc.A/RES/56/19, January, 2002.
UN General Assembly Resolution 58/32, UN Doc. A/RES/58/32, 2003.
UN General Assembly Resolution 66/152, UN Doc. A/66/152, 2011.
UN General Assembly Resolution 68/98, UN Doc. A/Res/68/98, 2013.
UN Security Council Resolution 1368, UN Doc. S/RES/1368, 2001.
UN Security Council Resolution 1373, UN Doc. S/RES/1373, 2001.
UN Security Council Resolution 2249, UN Doc. S/RES/2249, 2015.
Waxman, Matthew C., 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', 36 *Yale Journal of International Law* (2011) 421–460.