The Dickson Poon
School of Law

LLM 7FFLA903 Dissertation Cover Sheet – 2015/16

Candidate Number	W05123
Dissertation Supervisor	Holger HESTERMEYER
Dissertation Title	Cyber Operations and the Use of Force within the Meaning of Article 2 (4) of the United Nations Charter
Word Count	14999
LLM Pathway/Specialism (if any)	General

Abstract

The evolution of the warfare technology has required a new understanding of the rules regarding the laws of war. In this context, whether cyber operations fall into the scope of the prohibition of the use of force within the meaning of the article 2(4) of the United Nations Charter has been discussed for a few years. Almost all commentators have agreed that cyber operations may constitute the use of force, however, they differ on the issue of under which circumstances the operations would qualify as such. Three main approaches, that are the instrument-based, the target-based, and the consequence-based, have offered different solutions considering different aspects of cyber operations. However, because they engaged with only one aspect of cyber operations, they have remained inadequate to deal effectively with the new challenges. There is a need for a more flexible approach which takes into consideration other characteristics of cyber operations. What this contribution hopes to demonstrate is the effectiveness of the intersection of the target-based and the consequence-based approaches, which have produced another one, that is what I called "the function-based approach".

Table of Contents

1. Introduction

No period in the history of human being has seen such an interdependent environment that we have been experiencing since the last quarter of the past century. The internet and communication technologies have extremely increased interdependency amongst different communities and nations. Not only between the people, but also between technical systems such interconnectedness has been increasing. On the one hand, the internet and these systems have become an indispensable part of daily life of human being as they significantly facilitate the life, saving time and energy. On the other hand, such interconnectedness has posed significant risks due to vulnerabilities the internet and these systems have.

Because of the vulnerabilities of these structures, they have become open to be attacked by anyone from anywhere in the world. Even a washing machine or a photocopy machine in an ordinary house could be a possible target of cyber operations, due to its connection to computer networks. Not only computers, but also other electronic devices have been invoked to launch cyber operations. CCTV cameras, for example, have been used as a kind of botnet for operating DDOS attacks.[1] More importantly, almost all critical national infrastructures (CNIs) of states are commanded and controlled through SCADA systems, that is the acronym for supervisory control and data acquisition, which "are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation."[2] Cyber operations targeting these systems can undoubtedly cause considerable consequences. In such an environment, cyber security has gained crucial importance for states to maintain their governmental, martial and societal functions. Cyber security has been also included into national security strategies of states as one of the prior issues to consider. Furthermore, states started to declare specific strategies regarding cyber security. Moreover, some states have established cyber command units within their army in order to defend their critical structures and security systems.[3] Although no state has yet claimed

[1] DDOS is the abbreviation for Distributed Denial of Service, that is briefly a type of attack which uses thousands of electronic devices as botnets in order to make a website unavailable, overflooding it. 'Kaspersky DDOS Intelligence Report Q3 2015 - Securelist' (*Securelist.com*, 2015) <https://securelist.com/analysis/quarterly-malware-reports/72560/kaspersky-ddos-intelligence-report-q3-2015/> accessed 17 August 2016.

[2] 'What Is SCADA? Webopedia Definition' (*Webopedia.com*, 2016) <http://www.webopedia.com/TERM/S/SCADA.html> accessed 17 August 2016.

[3] In 2009, the US established 'United States Cyber Command (USCYBERCOM)'. In 2013, the UK found 'The Joint Cyber Reserve' under the Joint Forces Command (JFC). China officially announced that it had a cyber unit called 'PLA Unit 61398' under the command of People's Liberation Army. NATO also has a cyber unit called Cooperative Cyber Defence Centre of Excellence. Russia announced that it would create a cyber military unit but it has yet introduced it officially.

responsibility for any attack, it is publicly known that these units also undertake offensive cyber operations. For these reasons, cyberspace has been seen as the fifth domain of warfare in addition to the conventional armed forces including land, naval and air forces, and space.[4]

Recent years have witnessed a number of serious cyber operations. In 2007, Estonia was imposed considerable cyber operations after the government's decision to relocate a Soviet-era memorial called the Bronze Soldier of Tallinn. The decision annoyed Russian ethnics living in Estonia and they rioted. Following the riots, a massive DDOS operations started to target the governmental websites, banking and financial systems, communication structures and internet service providers of Estonia. The cyber operations were supposedly originated from Russia[5], but disseminated throughout the world including more than 170 countries due to the nature of the operations. A three-week cyber operations, though they did not cause deaths, injuries or damages to properties, considerably affected the state's communication facilities, economic security and the society. Estonia, as the most wired country in the world , has experienced a chaos-like situation in those days.[6] Following these incidents, the NATO's Cooperative Cyber Defence Centre of Excellence was established in 2008.

In the same year, Georgia also suffered from a series of cyber operations carried out during the armed conflict of 2008 with Russia, who is believed to be behind the operations, though it has not claimed responsibility. As was in the Estonian case, DDOS methods were used against Georgian governmental websites, news and media sites and financial institutions for three weeks.[7] It was for the first time the cyber capabilities were used along with the conventional weapons in an armed conflict.

The most considerable cyber attack taken place so far was against Iran in 2010. The Stuxnet worm, designed by allegedly the US in cooperation with Israel, had spread worldwide and discovered in 2008 in so many computers.[8] The main purpose, however, was revealed when it hit the Natanz nuclear plant of Iran: to mitigate Iran's uranium enrichment program. It was so high-tech and sophisticated worm on record that it could identify the systems it was

[4] 'War in the Fifth Domain | The Economist' (*Economist.com*, 1 July 2010) <http://www.economist.com/node/16478792> accessed 17 August 2016.
[5] Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia' (*the Guardian*, 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 17 August 2016.
[6] Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe' (*WIRED*, 2007) <http://www.wired.com/2007/08/ff-estonia/> accessed 17 August 2016.
[7] Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, vol. 112 (Cooperative Cyber Defence Centre of Excellence 2010), p. 89.
[8] Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, USA 2013), p. 52.

involved and did not harm if the systems were not the real target, that is Natanz's SCADA system.[9] In details, the Natanz nuclear facility was not connected to the internet, but it had a SCADA system produced by Siemens. The Stuxnet worm was supposed to infect this system through a computer of an engineer working for the facility, which had been previously infected. In order to increase the possibility to reach an engineer of Natanz, the virus had been disseminated globally, but 60% of computers infected were in Iran.[10] The worm was designed to destroy centrifuges, which are one of the main components to be used in the process of uranium enrichment, by altering their running speed programmed through SCADA system.[11] Although the Iranian government has never officially announced what were the consequences, it was estimated one-fifth of the Iranian centrifuges were physically damaged and destroyed. Due to the destruction of centrifuges; it is believed the attack took back Iran's nuclear program for a few years.[12] It was the first time a cyber attack has ever caused physical damages to a property.

21st century has marked a significant developments and shifts on the method and means of warfare. The actors, the targets, the effects and the instruments of warfare of 21st century has been fairly different than that of 20th century. Cyber weapons have been added to conventional weapons of 20th century. Critical infrastructures of nations have gained vital importance and become much more vulnerable to attacks and exploitation. Electric power grids, water supply systems, banking and financial systems have been target of attacks. States have declared the protection of such infrastructures is crucial to their national security. Therefore, one must consider the developments in warfare technologies when it comes to interpret the rules regarding the laws of war.

There must be an answer of international law in the face of these new challenges. Since there is no international cyber-specific treaty regarding the laws of war, one considerable thing to do is to search for the applicability of the existing rules and how to apply them to cyber operations. The characterization of the new problem under the existing rules seems to be one of the most important issues that the law has to do. The response of international lawyers has

[9] Ibid. p. 45.
[10] William Maclean, 'UPDATE 2-Cyber Attack Appears to Target Iran-Tech Firms' (*Reuters*, 2010) <http://www.reuters.com/article/security-cyber-iran-idUSLDE68N1OI20100924> accessed 18 August 2016.
[11] Ralph Langner, 'To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve' [2013] Online: http://www. langner. com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge. pdf.
[12] 'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years' - Iranian Threat - Jerusalem Post' (*Jpost.com*, 2010) <http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years> accessed 18 August 2016.

been to deal with the new challenge under *jus ad bellum* and *jus in bello* frameworks.[13] The questions of this study fall into *jus ad bellum* framework: Can the existing *jus ad bellum* rules be applicable to the cyber operations? Do cyber operations constitute the use of force within the meaning of article 2 (4) of the United Nations (UN) Charter? If so, under which circumstances that cyber operations can qualify as the use of force? The other important *jus ad bellum* norms, the threat of the use of force and self-defence, will be excluded due to the narrow scope of the study.

There are three leading approaches in the literature with regard to the use of cyber force, namely, the instrument-based approach, the target-based approach and the consequence-based approach. Though they have contributed to the development of the field, each remained too focused on only one aspect of the cyber operations, which makes the approaches inflexible and fragile in some respects. The efficiency of the intersection of these approaches to deal more effectively with the cyber use of force is generally underestimated. Therefore, I will propose "the function-based approach" which is based mainly on the intersection of the target-based approach and the consequence-based approach. For this purpose, I will scrutinize the notion of force in international law, the applicability of the existing *jus ad bellum* rules, and three above-mentioned approaches in detail.

2. Conceptual Background

In the early terminology, the emphasize was on "information" and "computers" such as "information operations", "computer network operations (CNOs)" or "computer network attacks (CNAs)". Information operations is mostly referred to point out in terms of effecting the decision making process of a state through misinformation or espionage. The means used, however, do not necessarily to be cyber means. An agent's ordinary activity to misinform the adversary can be seen under the scope of information operations. Furthermore, the main purpose of the information operations is not to cause deaths, injuries or physical damages,

[13] *See* for one of the most the considerable works in the field: Michael N Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013). It is a product three years of work by twenty distinguished international lawyers first convened in 2009 in Tallinn, the capital city of Estonia, to identify the applicable law to cyber operations upon the request of NATO Cooperative Cyber Defence Centre of Excellence.

rather "to influence, disrupt, corrupt, or usurp the decision-making of adversaries".[14] Therefore, the term "information operations" does not seem appropriate to cover the operations carried out in recent years, considering their characteristics.

The most commonly quoted definition in the field is of CNA by the US DoD, the following which "actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves".[15] This definition acknowledges computer networks can either be the target and the instrument of the attacks.[16] What is the flaw of the definition is its focus on the "computer networks", which seems to exclude other networks to be targeted or to be used as a mean. A malicious software, for example, can be installed into a critical system through an agent without the need for a network.[17]

The literature review has shown that the terminology has gradually changed within decades. From the 90s to the millennium the term "information operations" was on use, while the "computer network operations or attacks" was of the next decade's popular term. From nearly 2010 until today, the use of the term "cyber" has considerably increased. Almost all activities in the cyberspace have been frequently called as cyber warfare in the media. The media use of "cyber warfare" is, however, generally over-broad, containing mere cyber espionage, cyber crimes or cyber activities which even do not amount to the use of force into the scope of cyber warfare. The Estonian operations, for example, has been called as World Web War I.[18] Cyber war has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[19] Theoretically, it can be either carried out stand-alone or in a traditional armed conflict in

[14] The U.S. DoD, 'Information Operations', *Dictionary of Military and Associated Terms*, (Washington DC 2010, as amended through 15 February 2016) p. 110.
[15] James E Cartwright, 'Joint Terminology for Cyberspace Operations' [2010] Joint Chiefs of Staff (JCS) Memorandum, Nov. p. 3.
[16] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014), p. 12.
[17] Ibid.
[18] Stephen Blank, 'Web War I: Is Europe's First Information War a New Kind of War?' (2008) 27 Comparative Strategy 227.
[19] Richard A Clarke and Robert K Knake, *Cyber War* (Harper Collins 2011), p. 6.

support of conventional forces. Nevertheless, there has yet been a stand-alone cyber war taken place so far.[20]

"Cyber operations" is a broader term to cover what has been meant by using "cyber war" in the media. The Tallinn Manual defines it as "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyber space."[21] This is a neutral definition which does not imply that the operation amounts to the use of force, nor armed attack within the meaning of article 51 of the Charter. Neither it implies whether the operation is legal or illegal.[22] Therefore, it will be frequently used in this study to refrain from some misunderstandings in legal respects. Although the definition is broad enough to cover most of the activities in the cyberspace, note that it does not refer to cyber crimes such as internet frauds, credit card thefts which are matters of domestic law. The focus of this study is the operations carried out by states or attributable to states.

As to cyber weapon, I will subscribe the following definition which "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems or living beings."[23] Computer code includes malicious software such as viruses, worms or trojan horses, and logic bombs. DDoS attacks, though not software, can be included into this definition, because they are carried out through computer codes as well. This definition not only covers physical damage on persons and properties, but also functional and mental damages. This is significant because most of the definitions ignore the functional damages which are caused through cyber means.

3. The Prohibition of the Use of Force in International Law

The 20th century witnessed two devastating world wars. In the wake of these wars, the international community sought to limit resorting to war. The Covenant of the League of

[20] Laurie R Blank, 'Cyberwar Versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace', in Jens David Ohlin, Kevin Govern, Claire Finkelstein (ed), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015), p. 85.
[21] The Tallinn Manual, p. 15.
[22] Janne Valo, 'Cyber Attacks and the Use of Force in International Law' (Master of Laws, University of Helsinki 2014), p. 6.
[23] Rid, p. 37.

Nations introduced some restrictions, however, it did not prohibit war in general. The Kellogg–Briand Pact was the first treaty which declared recourse to war illegal in the history, yet it did not come into force. Both of these treaties failed to prevent the Second World War. The UN Charter, eventually, prohibited the use of force "to save succeeding generations from the scourge of war".[24]

Article 2 (4) of the UN Charter provides that "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." The prohibition, as the ICJ stated in the *Nicaragua* case, is one of the norms of customary international law.[25] There are two main exceptions to the prohibition. The first is self-defence of states articulated in article 51of the Charter that allows member states to use force if an "armed attack" occurs against them. The second is the collective measures which are to be taken by the Security Council in the event of "any threat to the peace, breach of the peace, or act of aggression", pursuant to article 39 of the Charter.

The scope of the term "force" is one of the controversial issues in international law. Before interpreting this term, it would be useful to clarify briefly the other elements of the provision, considering the features of cyberspace. First, the term *their international relations* refers that the prohibition only covers the use of force by states or entities attributable to states.[26] As was mentioned above, states have a growing tendency for establishing a cyber unit under their regular armed forces. The attacks originating from these units against another state may constitute the use of force. If an attack is carried out by non-state actors, it should be attributed to a state. Indeed, identification and attribution of the attacks is highly crucial in order to response these attacks lawfully.[27] The assessments in this study, however, will be based on the assumption of the existence of attribution, because the attribution problem is beyond the scope of this study.

[24] Charter of the United Nations, 24 October 1945, 1 UNTS XVI, available at: <http://www.un.org/en/charter-united-nations/> accessed 30 June 2016.
[25] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, p. 17, para. 34.
[26] Albrecht Randelzhofer, Oliver Dörr, 'Ch.I Purposes and Principles, Article 2 (4)', in Bruno Simma (ed), *The Charter of the United Nations: A Commentary*, (Volume I, 3rd Edition, Oxford University Press, 2012) p. 214.
[27] Marco Roscini, 'Cyber Operations as a Use of Force' [2015] Research Handbook on International Law and Cyberspace, Edward Elgar Publishing 233, p. 4.

Second, the clause *against the territorial integrity or political independence of any state* was claimed to be one of the main element of the prohibition. In other words, if a use of force does not constitute a threat against the territorial integrity or political independence of a state, some argues, it would not be considered in breach of the principle. Regarding this argument, can one state claim that cyber operations do not constitute uses of force since they are transnational and have a unique feature which makes the boundaries of states meaningless to operate an attack, therefore, they do not affect the territorial integrity of a state? The answer must be negative. A similar approach brought into question by the UK in the *Corfu Channel* case. The UK claimed that its actions were not against Albanian territory and political dependence but to collect evidences regarding the explosion of its ships due to mines in Albanian waters. The court, however, rejected this claim stating that sovereignty is essential foundations of international relations.[28] Furthermore, the travaux préparatoires of the Charter shows that the purpose of this clause was never to restrict the scope of the prohibition. Moreover, it was added the to the text of article on the demand of some smaller states aiming to put particular emphasize on the state sovereignty.[29] Therefore, these two issues are not obstacles for cyber operations to qualify as the use of force. Nevertheless, what matters is how to interpret the notion of force.

The Notion of Force

The term "force" is employed in the UN Charter in a few times. The drafters of the Charter sometimes used it alone, while sometimes chose to use it with the adjective "armed". Since the Charter provides no definition for it, the abovementioned distinction has given rise to arise of different interpretations.[30] The main difference in the interpretations is seen on the issue of whether to include economic and political coercion under the use of force umbrella.[31] The other controversial issue is whether physical/kinetic force and effect is to be a criterion as to the determination of the existence of the use of force. The following headings will evaluate these two issues.

[28] Corfu Channel Case, (Albania v. The United Kingdom), Merits, Judgment of April 9th, 1949, ICJ Reports 1949, p. 35.
[29] Randelzhofer, Dörr, p. 215.
[30] Randelzhofer, Dörr, p. 208.
[31] Christine Gray, 'The Use of Force and the International Legal Order', in Malcolm Evans (ed), *International Law,* (4th Edition, Oxford University Press 2014) p. 621.

3.1. Armed, Economic or Political Force?

Vienna Convention on the Law of Treaties allows different interpretations of the treaty provisions. One is the textual interpretation which takes into consideration what the provision grammatically means in the context and assumes that the drafters have exactly reflected their intentions into the treaty text. Based on this, some commentators claim that the drafters of the UN Charter were absolutely aware of usage of the terms "armed" and "force". If the drafters had wanted, they could have employed the adjective "armed" before the "force" in article 2 (4), as they did in the preamble stating "armed force shall not be used" and in articles 41, 43, 44 and 46 stating "use of armed force".[32] Therefore, it is argued the prohibition is not restricted to the armed force, but it covers also economic and political coercion. This view is supported by some developing countries, but rejected by most of the international lawyers.[33]

The prevailing view is that the prohibition of the use of force encompasses only the armed force, even though article does not explicitly utilise the adjective "armed". The main argument of this view is the fact that the refusal of the Brazil's proposal to include "the threat or use of economic measures" into article 2 (4) in 1945, in the travaux préparatoires.[34] Secondly, the subsequent documents by the General Assembly such as the Declaration on the Friendly Relations and the Declaration on the Non-Use of Force are given proofs for this view.[35] Indeed, the former declaration evaluates the economic and political coercion clearly under the scope of the principle of non-intervention, but not under the prohibition on the use of force.[36] The latter also implicitly follows the distinction between the economic measures and the armed force.[37]

I am also convinced with the prevailing view. However, what really matters is to identify what constitutes an armed force. The adjective "armed" is defined in the Black's Law Dictionary as "equipped with a weapon" or "involving the use of a weapon".[38] Another

[32] Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification,' (2009) 1 Goettingen Journal of International Law 375, p. 382.
[33] Randelzhofer, Dörr, p. 209.
[34] Ibid.
[35] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012), p. 48.
[36] UN Doc A/Res/25/2625, 24 October 1970, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.
[37] UN Doc A/Res/42/22, 18 November 1987, Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations; *See* also Marco Benatar, p. 385.
[38] Bryan A. Garner (ed.), 'Armed', *Black's Law Dictionary*, 10th edn, (Thomson Reuters 2014), p. 129.

dictionary defines the adjective as "equipped with or carrying a weapon or weapons"[39]. Several dictionaries refer to the term "weapon" to define the adjective "armed". Therefore, it can be said "weapon" is the main characteristic of armed force. However, the ICJ held that the type of weapons employed does not really matter in determining the existence of armed force.[40] Nevertheless, the scope of the prohibition is not limited to direct use of force. The ICJ in the *Nicaragua* case held that arming and training of a group against the government of a state is regarded as the violation of the prohibition of the use of force. The court, however, stated merely supplying funds to rebellions, though it is a breach of non-intervention principle, does not amount to use of force.[41]

The second important issue is how to distinct armed force from economic coercion. In the cyber context, many commentators argue a cyber attack targeting a nation state's financial and banking systems may never fall under the scope of the use force unless its effects akin to the conventional weapons, claiming that economic coercion does not constitute use of force.[42] This interpretation, as shall be seen later, remains quite superficial and far from offering a sensible solution for the challenges posed by cyberspace. Although the object of the cyber attack is the economic structure of a nation state, characterizing it simply an economic coercion would be a failure. There is a consensus in international community on the fact that cyberspace can be used as a weapon. Since one of the main elements of the armed force is to employ weapon, cyber operations carried out through cyber weapons could also fit into the definition of the use of force. It is not to say, however, all forms of cyber operations targeting economic structures of states should be considered as uses of force, but to say, considering the employment of a weapon and its consequences, the attack can resemble an armed force rather than economic coercion.[43]

[39] 'Armed - Oxford Reference' <http://www.oxfordreference.com/view/10.1093/acref/9780195392883.001.0001/m_en_us1222947> accessed 27 July 2016.
[40] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, p. 22, para. 39.
[41] Military and Paramilitary Activities, para. 228, p. 119.
[42] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 212; Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30 Berkeley Journal of International Law 525, p. 537.
[43] Todd A Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2 (4) of the UN Charter' (1998) 30 Case W. Res. J. Int'l L. 567, p. 595.

3.2. Kinetic/Physical Force

At the time the UN Charter was designed, the armed force was unsurprisingly considered to be producing only kinetic force. Thus, the concept of armed force was instrumentally equated to the employment of conventional weapons. With the invention of the new weapons such as chemical and biological weapons, however, this view became obsolete. Although these weapons are not kinetic means and do not have any explosive effects, their use potentially causes horrendous impacts on human beings and property.[44] Therefore, the interpretation of article 2 (4) had to be expanded. Ian Brownlie, within his remarkable study "International Law and the Use of Force by States", has filled this gap. He advocated that even though the chemical and biological weapons are not kinetic as conventional weapons, their use could be "assimilated to the use of force on two grounds. In the first place the agencies concerned are commonly referred to as 'weapons' and as forms of warfare." The second and more persuasive argument of him is the fact that the use of such weapons causes to "destruction of life and property".[45] This brief explanation of his argumentation shows his contribution marks the shift from the instrument-based approach towards the consequent-based approach in the interpretation of the use of force. Thus, "physical means" requirement to identify the use of force has been changed with the "physical consequences" requirement, gaining much traction from the international community.[46] By the same token, with the development of cyber capabilities in the last two decades, the "physical consequences requirement" has become questionable.[47] Considering the cyber weapons' potential to cause not only physical damage, but also more adverse consequences than physical damage without physical destruction, it seems there is a growing need for another shift in the use of force interpretation. One purpose of the the function-based approach is to fill the deficiency of the consequence-based approach.

[44] 'Use of Nuclear, Biological or Chemical Weapons: Current International Law and Policy Statements - ICRC' <https://www.icrc.org/eng/resources/documents/misc/5ksk7q.htm> accessed 27 July 2016.
[45] Ian Brownlie, *International Law and the Use of Force by States* (Oxford Clarendon Press 1963) p. 362.
[46] Elaine Korzak, 'Computer Network Attacks and International Law' (Ph.D, War Studies Department of King's College London 2015) p. 63.
[47] Noah Simmons, 'A Brave New World: Applying International Law of War to Cyber-Attacks' (2014) 4 Journal of Law & Cyber Warfare 42.

4. Applicability of the Existing Law

The only existing international treaty regarding cyberspace is the 2001 Budapest Convention on Cybercrime of Council of Europe, dealing with specific crimes committed through computer networks such as infringements of copyright, computer-related fraud, child pornography and violations of network security.[48] The main purpose of the treaty is to increase co-operation between states parties in protecting their societies against cybercrimes. This treaty, however, is not applicable to cyber operations carried out by and between states. Cyber warfare has yet been subject of any international treaty. Indeed, there is no consensus in international community on whether there is a need for a cyber-specific treaty regarding the laws of war.[49]

In 1998, the Russian Federation initiated a draft resolution, which was later on adopted by UN General Assembly, regarding international security of information technologies and communications. That resolution, acknowledging new developments in information technology can potentially be a serious threat for security of states as well as international security, was to call upon member states to disclose their considerations on the new developing field.[50] Particularly after 2010, the number of member states submitting their assessments on the issue has considerably increased. It can be seen from their assessments they have all agreed on there is a growing need for international cooperation and common understanding in response to misuse of information technology and communications system by both states and non-state actors. They differ, however, on how the way of response of international law against this new threat should be.

The call for a cyber-specific treaty has mostly come from the Russian Federation[51]. In 2011, Russia, China, Tajikistan and Uzbekistan, member states of the Shanghai Cooperation Organisation, have jointly sent a letter to the UN[52], which was revised in 2015[53], drafting

[48] Convention on Cybercrime, Council of Europe, (adopted 23 November 2001, entered into force 01 July 2004) ETS No.185.
[49] Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations', In *2012 4th International Conference on Cyber Conflict – Proceedings*, Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds.), (Tallinn: NATO CCDCOE), p. 91.
[50] UN Doc A/Res/53/70, 4 January 1999.
[51] Alexandra Kulikova, 'Can a New UN Cyber Agreement Be a Win-Win for Russia, US?' (*russia-direct.org*, 28 August 2015) < http://www.russia-direct.org/analysis/can-new-cyber-agreement-among-un-experts-be-win-win-russia-us > accessed 28 June 2016.
[52] UN Doc A/66/359, 14 September 2011.
[53] UN Doc A/69/723, 13 January 2015.

international code of conduct for information security and seeking to encourage the member states to reach a consensus on the matter. The code of conduct emphasizes state sovereignty on cyber space and the prohibition of the use of cyber weapons as means of act of aggressions and in a way threating international peace and security.[54] Paradoxically, Russia and China, along with the US, are the most usual suspects of launching cyber operations taken place so far.

The call for a new treaty have also gained some supports from academy. The main argument of the authors arguing a cyber treaty is a must to challenge posed by cyber operations is the unique characteristics of cyber space.[55] As was mentioned above, cyber space totally removes the geographical proximity, which is essential for traditional warfare to some extent, to launch an attack. In addition, as regards to the consequences, cyber operations could potentially cause physical harm as kinetic weapons could do. Having admitted that, they point out cyber operations which do not have any physical consequences but significantly effect the functions of critical national infrastructures of states to show that existing international norms, specifically article 2 (4) of the UN Charter prohibiting use of force in international relations, remain inadequate in the face of new challenges.[56] The fact that the drafters of the UN Charter has never envisioned invention of the cyber space and its use as a mean of warfare push forward those authors to offer a new treaty. Secondly, they believe agreeing on a treaty will clarify the conceptual confusion between the terms such as "cyber crime", "cyber espionage/exploitation", "cyber use of force", "cyber attack". The consensus through a treaty on the definition of these notions, they argue, will remove the ambiguity, by not leaving their interpretation to states.[57] Thirdly, an international treaty would increase the collaboration between states in collecting evidence and enable states to investigate transnational cyber operations in cooperation with each other.[58]

Admittedly, these arguments are not totally unfounded. The need for collaboration amongst states have been consistently raised by states and it will apparently always exist with

[54] UN Doc A/69/723, 13 January 2015, p. 4.
[55] Davis Brown, 'Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, A' (2006) 47 Harvard International Law Journal 179.
[56] Benjamin Mueller, 'The Laws of War and Cyberspace on the Need for a Treaty Concerning Cyber Conflict' (June 2014) <http://www.lse.ac.uk/IDEAS/Home.aspx> accessed 24 June 2016.
[57] Oona A Hathaway and others, 'The Law of Cyber-Attack' [2012] 100 California Law Review 817; Duncan B Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 Lewis & Clark Law Review 1023 p. 881; Stephen Moore, 'Cyber Attacks and the Beginnings of an International Cyber Treaty' (2013) 39 North Carolina Journal of International Law and Commercial Regulation 223, p. 241.
[58] Hathaway, p. 878.

or without a convention and states will be seeking for it anyway[59]. A treaty can contribute its realisation. On the other hand, the challenges posed by cyber space could be dealt with a new understanding of the existing rules without having a treaty. The existing rules can still answer to new challenges if they are interpreted in a manner consistent with the purpose of the UN Charter by taking into consideration the evolving nature of warfare at the same time. Considering the practice of the UN, in its relatively short history, there have been new challenges which were never initially envisioned in the Charter. The UN peacekeeping mission can be the best example of how the charter has evolved in the face of new challenges. Although nowhere in the UN Charter expressly refer to it, the Charter has been seen flexible enough to cover peacekeeping operations. The more concrete argument comes from the ICJ. In its advisory opinion on *Nuclear Weapons*, the ICJ explicitly stated that type of weapons used is not a criterion to be applied for determining whether there is a violation of the prohibition of the use of force: "These provisions [articles 2 (4) and 51 of the UN Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons."[60]

Secondly, a new treaty cannot guarantee to solve the ambiguity problem, because the use of force is already one of the most controversial issues of international law.[61] The ambiguity has been existed and will always exist regarding the use of force[62]. It cannot totally be removed by simply agreeing on a treaty on cyberspace. In its assessment submitted to the UN, the US rightly put the following argument: "such ambiguities and room for disagreement do not suggest the need for a new legal framework specific to cyberspace. Instead, they simply reflect the challenges in applying the Charter framework that already exists in many contexts."[63] Therefore, the treaty should not be regarded as a magic wand to remove uncertainties.

The last and the most realistic argument is that the consensus on the need for a treaty does not seem to be reached in near future.[64] The risks and opportunities of cyberspace are

[59] UN Doc A/65/201, 30 July 2010, The Report by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.
[60] Legality of the Threat or Use of Nuclear Weapons, p. 22, para. 39.
[61] Christine D Gray, *International Law and the Use of Force* (Oxford University Press 2004) p. 26.
[62] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Intersentia 2014), p. 154.
[63] UN Doc A/66/152, 15 July 2011, p. 18.
[64] Michael N Schmitt, 'Cyber Operations and the Jud Ad Bellum Revisited' (2011) 56 Villanova Law Review 569, p. 36.

perceived by different states in different ways based on their technological development.[65] As was mentioned above, the legal paradigms of the Russian Federation and the United States differ on cyber space. The US has no hesitation over the applicability of the current international law rules on cyber space: "Despite the unique attributes of information and communications technologies, existing principles of international law serve as the appropriate framework within which to identify and analyse the rules and norms of behaviour that should govern the use of cyberspace in connection with hostilities".[66] The UK also holds the same view and has declared it several times: "The United Kingdom firmly believes that these principles [existing norms] apply with equal force to cyberspace and an unambiguous affirmation by States that their activities in cyberspace will be governed by these laws and norms would lay the foundations for a more peaceful, predictable and secure cyberspace."[67] Furthermore, it also clearly states its opposition to prospective attempts to agree on a treaty: "…the efforts of the international community should be focused on developing common understandings on international law and norms rather than negotiating binding instruments that would only lead to the partial and premature imposition of an approach to a domain that is currently too immature to support it."[68] Moreover, the Group of Governmental Experts (GGE) convened in 2013 and consisted of representatives of twenty countries, concluded that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment."[69] Two years later, in 2015, the GGE expanded its report and touched upon the issue of how the existing international rules apply to cyber space[70]. However, it was not more than superficially referring to the general principles of international law such as state sovereignty, non-intervention and peaceful settlement of disputes and the general principles of *jus in bello*. Therefore, the need for elucidation of how to apply the existing rules on cyberspace remains.[71] The next chapter will scrutiny this issue.

[65] Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)' (2011) 36 Yale Journal of International Law 421, p. 449.
[66] UN Doc A/66/152, 15 July 2011, p. 18
[67] UN Doc A/68/156, 16 July 2013, p. 18.
[68] Ibid, p.19.
[69] UN Doc A/68/98, 24 June 2013, p. 2.
[70] UN Doc A/70/174, 22 July 2015, p. 12.
[71] Michael N Schmitt, 'International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed' (2012) 54 Harward International Law Journal 13, p. 14.

What is the argument of this chapter is not that cyberspace cannot be regulated[72] nor a new treaty may never be useful in addressing the new cyber threats, rather in the absence of the treaty to be possibly agreed in the foreseeable future, the existing rules should apply to cyberspace. If they are interpreted non-restrictively, in a manner considering the evolving nature of warfare, they still can address the needs and challenges arising out of cyberspace.

5. Applying the Existing Rules to Cyber Operations

Cyber operations can be categorized into three level in terms of their gravity under the *jus ad bellum* framework. First, the operations which fall short of the use of force threshold but violating the non-intervention principle such as mere intrusion to the cyber systems of another state or cyber espionage. Second, cyber operations reaching the use of force threshold, breaching article 2 (4) of the UN Charter. Third, cyber operations amounting to the level of armed attack, therefore, giving rise to the right of self defence pursuant to article 51 of the Charter.[73] The main purpose of this study is to examine the cyber use of force. Therefore, the non-intervention principle and self defence issues will be excluded from the scope of this contribution.

The literature review has shown there are three main approaches regarding the cyber use of force. The first is called the instrument-based approach which focuses on the type of weapon employed and compare it with the conventional weapons. The second is the target-based approach. According to this, if a cyber attack targets a CNI of a state, it is sufficient to be regarded as the use of force. The last and more supported one is the consequence-based approach which emphasises the effects of cyber operations. By analogy with the conventional weapons, if a cyber attack causes to loss of life, injury or destruction of property, it is considered to reach the use of force threshold. Each of the approaches has some shortcomings and remains inadequate to explain cyber use of force in some respects. Therefore, I will try to reconcile the target-based approach and the consequence-based approach in order to deal more effectively with the cyber use of force.

[72] Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501, p. 532.
[73] Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense' (2002) 38 Stanford Journal of International Law 207, p. 222.

5.1. The Instrument-Based Approach

The traditional interpretation of the use of armed force was highly intertwined with the weaponry. The weaponry of the time of the mid-twentieth century used to be understood somewhat explosive and destructive. Therefore, the instrumentality approach was suitable enough to identify the use of armed force. Pursuant to this early understanding of the use of force, the instrument-based approach evaluates new types of weapons in determining the existence of the use of force, comparing them with the conventional weapons which are inherently bear kinetic characteristic. Thus, cyber weapons comprising of non-physical computer codes hardly constitute a use of force, due to not having a coercive nature in themselves as the conventional weapons.[74] This approach finds a legal basis in the text of the UN Charter to some extent. In article 41, it is regulated that the measures not involving the use of armed force includes "complete or partial interruption of … telegraphic, radio, and other means of communication".[75] In this context, internet and computer networks, as means of communication, do not qualify as the use of armed force.

Woltag lists the rationales behind this approach. First of all, it is easy to characterize an act as being use of force by considering only its method of delivery,[76] without having to address its consequences.[77] Second, it is a useful tool to exclude economic coercion from the purview of the prohibition on the use of force. Third argument is indeed interlinked with the second one, the instrument-based approach can preclude unnecessary "expansion of the scope of the notion of force."[78]

However, the drawbacks of this approach outweighs its advantages. Firstly, cyber operations undoubtedly can cause physical damage, its consequences can be as destructive as that of the conventional weapons. The approach ignores the potential consequences of cyber operations. As Daniel B. Silver rightly argues, what matters in identifying the use of armed force is not because of weapons' "inherent lethality but because of the potential destructiveness of the way it is being used or the purpose for which it is deployed".[79]A nation-state must take some measures to tackle cyber operations in order to protect its national security. What the

[74] Hollis, 1041; Korzak, p. 67.
[75] The UN Charter, article 41; Hollis, 1041.
[76] Gervais, p. 538.
[77] Woltag, p. 142.
[78] Ibid.
[79] Daniel B. Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' (2002) 76 Int'l L. Stud. Ser. US Naval War Col. 73, p. 88.

instrument-based approach seems to offer nation-states is to wait for the beginning of a conventional attack against them, which is actually not acceptable for states.[80] This approach has also been criticised as being "rigid and inflexible"[81]. It rejects to update itself in the face of the evolution of the warfare technology. Only with the international agreements, this approach seems to offer, can new forms of weapons be included into the scope of the prohibition of the use of force.[82] Having considered its deficiency to answer the 'consequence problem', it would neither be meaningless to adopt the instrument-based approach in order to use it as a tool to distinct armed force from economic coercion. If this approach was to be adopted, the Stuxnet attack causing the physical destruction of centrifuges in Iran's nuclear facility would never be considered as the use of force, because it was not carried out through a rocket, but a computer malware.[83] The instrument-based approach, due to the reasons above, is far from being a solution to the challenges posed by cyberspace and too outdated to deal effectively with those challenges.

5.2. The Target-Based Approach

As its name refers, the target-based approach, also known as strict liability, focuses on the target of cyber operations rather than the characteristic of the weapon used or the consequences that cyber operations possibly cause. What matters is the characteristic of the target being attacked. If the target of a cyber attack is so important to a state, regardless of its consequences, the mere intrusion to the computer-based system of the target would be well enough to qualify as the use of force. The rationale behind this view is the reliance of the modern societies to computer networks and internet-based systems which are highly vulnerable to cyber operations from anywhere in the world by state and non-state actors. The protection of CNIs, Walter Gary Sharp, the leading scholar of the target-based approach, argues, has become too vital for nation-states, so that penetration of them would be "a demonstration of hostile intent" and should give the victim state to use its right to self-defence.[84] "Vitality" of the target system and "hostility" of the aggressor are on the centre of the Sharp's theory. Cyber

[80] Jensen, p. 208.
[81] Reese Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare' (2013) 101 California Law Review 1079, p. 1118.
[82] Ibid. p. 1118.
[83] Jeremy Richmond, 'Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict' (2012) 35 Fordham International Law Journal 842.
[84] Walter G Sharp, *Cyberspace and the Use of Force* (Aegis Research Corporation 1999) p. 130.

espionage, he continues, though not unlawful under international law, on CNIs is likely to be an implication of the hostile intent and trigger anticipatory self-defence.[85] Another commentator follows his line and claims that the armed attack criterion in article 51 of the Charter for self-defence can be disregarded in the face of new cyber challenges, "even if a CNA is not an armed attack under article 51 of the United Nations Charter. Due to the instantaneous nature of a CNA, the right to respond must accrue immediately, despite the traditional obstacles of attribution (determining the attacker's identity), characterization (determining the attacker's intent) and the inviolability of neutrals."[86]

The question of 'what are those critical national infrastructures?' is left to states in Sharp's theory.[87] Indeed, the UN adopts the same approach: "each country will determine its own critical information infrastructures".[88] Critical Infrastructures Protection Act of 2001 of the US defines CNIs as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[89] The US also referred CNIs in its International Strategy for Cyberspace published in 2011, highlighting particularly "energy, transportation, or financial systems, and the defense industrial base" sectors.[90] The European Union's definition is similar to that of the US: "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".[91] In the further resolutions, the EU has focused on the importance of the cyber structures and incorporated

[85] Ibid., p. 132.
[86] Jensen, p. 209; *see* for another similar view: Christopher C Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 European Journal of International Law 825, p. 855.
[87] Sharp, p.130.
[88] UN Doc A/Res/58/199, 30 January 2004, p. 4.
[89] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law 107–56—Oct. 26, 2001, <https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf> accessed 2 August 2016.
[90] 'International Strategy for Cyberspace: Prosperity, Security, And Openness in A Networked World' (*White House*, 2011) <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> accessed 2 August 2016, p. 19.
[91] Council Directive 2008/114/EC, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] L 345/75, art. 2.

them into critical infrastructures.[92] The Shanghai Cooperation Organisation adopts a broader definition of CNIs: "public facilities, systems and institutions attacks on which may cause consequences directly affecting national security, including that of individual, society and state".[93] The UK adopts the approach following "the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. … [CNIs] may be physical (e.g. sites, installations, pieces of equipment) or logical (e.g. information networks, systems)".[94]

The main characteristic of the definitions is the emphasize put on the national and economic security. An attack on a CNI is regarded a serious threat to national security of states.[95] The target-based approach finds some support from the declarations given by the officials of Russia and the US. In a speech in 1995, the former stated that "...from a military point, the view of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether it will be casualties or not... considering the possible catastrophic use of information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces... Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself".[96] Though responding with nuclear weapons to cyber operations is hardly to be deemed as proportionate in the context of self-defence, it is significant in terms of showing how important the CNIs for a nation's security. The US, within an executive order, declared "certain national infrastructures are so vital that their incapacity or destruction [through physical threats or cyber threats] would have a debilitating impact on the defense or economic security of the United States."[97] Considering

[92] European Commission COM (2011) 163 final, on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' [2011]; European Commission JOIN (2013) 1 final, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; European Parliament resolution P7_TA (2012) 0237, on critical information infrastructure protection – Achievements and Next Steps: Towards Global Cyber-security [2011/2284(INI)].

[93] The Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, 16 June 2009), *see* for an unofficial English translation: 'Shanghai Cooperation Organisation' (*NATO Cooperative Cyber Defence Centre of Excellence*) <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf> accessed 3 August 2016.

[94] 'The National Infrastructure' (*Cpni.gov.uk*, 2016) <http://www.cpni.gov.uk/about/cni/> accessed 2 August 2016.

[95] Nils Melzer, 'Cyberwarfare and International Law' (*Unidir*, 2011), p. 16. <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> accessed 23 July 2016.

[96] Roland Heickerö, 'Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations' (Defence Analysis, Swedish Defence Research Agency (FOI) 2010), FOI-R--2970—SE, p. 16. <http://www.highseclabs.com/data/foir2970.pdf> accessed 3 August 2016.

[97] The White House, 'Executive Order 13010 Critical Infrastructure Protection' (1996).

the state's concerns about vitality and vulnerability of CNIs to cyber operations, the target-based approach's focus on the protection and maintenance of CNIs can be seen reasonable.

However, there are also concerns and criticisms about the target-based approach. Merely penetration of a critical system is offered to be giving rise to anticipatory self-defence under this approach. This framework, firstly, has much been criticised for being over-inclusive.[98] Secondly, it would not be surprising to see an escalation in international relations, if this approach was to be adopted.[99] Though the supporters of this approach claim that the low threshold set for CNIs, allowing the use of the right of self-defence for target state will deter other states to make cyber espionage operations on CNIs[100], it does not seem a compelling argument. The idea of accessing remotely one state's critical information with the possibility of hiding its identity will always attract states. Consider a spy of a few decades ago, who used to try to access a secret library of an enemy state. The only thing he could do would be to take only one or two books with him. But in the 21st century, the entire library has become remotely accessible through cyber means. This analogy demonstrates how cyber espionage come in handy for states. Indeed, this story almost came true at the outset of the millennium. An operation against the US in 1999, investigated by the authorities under the name of Moonlight Maze, has extracted enormous data including "maps of military installations, troop configurations and military hardware design".[101] In 2003, the US experienced one more huge cyber espionage incident, Titan Rain, allegedly carried out by China, through which 10 to 20 terabytes data was stolen.[102] Considering these examples, I do not believe that states would give up employing such facilities that cyberspace enables them. Therefore, offering anticipatory self-defence against cyber espionage would not be a deterrence for states, rather would increase escalation. Furthermore, the presumption of hostility for the operations targeting CNIs may not always work. A CNI may be affected as a third party by a cyber operation without a hostile intent to it.[103] The Stuxnet attack, for example, spread indiscriminately throughout the world, however, thanks to its high tech designation, it only caused damages in Iran's nuclear facilities. The Stuxnet worm, however, should have penetrated critical computer systems of other nations. If those states acted on this ground, they

[98] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 47; Nguyen, p. 1120.
[99] Hathaway, p. 847.
[100] Sharp, p.132; Jensen, p. 228.
[101] 'Interviews - John Arquilla | Cyber War! | FRONTLINE | PBS' (*Pbs.org*, 2016) <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html> accessed 4 August 2016.
[102] Clarke and Knake, p. 58.
[103] Simmons, p. 57; Gervais, 538.

would resort to use self-defence against the US and Israel, claiming mere penetration without any harmful effect on them would constitute armed attack. While this shows that a penetration of CNIs is not always made with the hostile intent, it presents another difficulty, that is, attribution. Though it is far beyond the scope of this study, it is worth to mention with a few words. One state's technical capabilities can be exploited by another state to make an operation against other states.[104] It is not always easy to detect the source of cyber operations. A state may not be technically capable of detecting the source of attacks and may be in the need of other states. Assuming that states even have such technical infrastructures to detect the source and attribute it to another state, the process would take some time which can make the use of self-defence meaningless. It is not to say it should not be taken any measures against cyber espionage, but there is a need for refraining from acting in a rush, in order not to cause even worst consequences with little evidence regarding the attribution.[105] It should also be borne in mind espionage is not prohibited under international law, neither cyber espionage by analogy.[106] In conclusion, the target-based approach suggests a "dangerously overbroad" [107] framework to deal with cyber operations.

5.3. The Consequence-Based Approach

This approach, also known as the effect-based approach, is the most supported one amongst the others. The main focus of this approach is comparing the consequences of the cyber operations with that of the operations conducted through conventional weapons, rather than comparing the weapon used itself. Yoram Dinstein, a prominent scholar advocating this approach, states "what counts is not the specific type of ordnance, but the end product of its delivery to a selected objective."[108] The consequences of cyber operations may vary depending on the capabilities of the cyber weapon used and the nature of the target.[109] The effect may be simply to block access to a website through DDoS operations or to delete, alter or disrupt data based on a computer-system through malicious codes. The latter acts can cause wide-ranging

[104] Valo, p. 40.
[105] Gervais, p.541.
[106] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 66
[107] Nguyen, p. 1120.
[108] Yoram Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 Int'l L. Stud. Ser. US Naval War Col. 99, p. 103.
[109] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of transnational law 1998, p. 911.

consequences from breaking a computer to explosion of a photocopy machine, from loss of the financial data with its backups to shutting down an electrical power grid through disrupting its SCADA system, from derailment of a trains to crashing of planes, from opening a dam's gate to leaking of poisonous gases from a chemical plant or radioactive materials from a nuclear power plant.[110] There is no doubt that cyber operations can be so destructive as much as the conventional military operations. To sum up, cyber operations can cause to loss of life or injury of persons or damage to property as the conventional weapons do.

The answer of the consequence-based approach to the question of what kind of effects could constitute the use of force under article 2 (4) of the UN Charter is those which are the same with the conventional weapons could create, that are physical damages.[111] The legal adviser of the State Department of the US expressed the following views overlapping with the consequence-based approach in one of his speeches in 2012: "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force."[112] The text of the Tallinn Manual adopts the consequence-based approach as well: "A cyber operation constitutes a use of force when its scale and effects are comparable to no-cyber operations rising to the level of a use of force."[113] The Manual incorporates the main elements of this rule, that are "scale and effect", from the *Nicaragua* case. Though these elements were set as a threshold in the *Nicaragua* case for determining the existence of "armed attack" within the meaning of article 51 of the UN Charter, the International Group of Experts of the Manual have accepted them equally useful in determination of the use of force.[114] That being said, neither the *Nicaragua* case, nor the Tallinn Manual, though its commentary provides little guidance, elaborates these criteria. The commentary adopts eight criteria for states to evaluate whether an operation amounts to a use of force. Six of them were incorporated into the Manual from the well-known article by Michael Schmitt, a prominent scholar in this field, in 1999.[115]

---

[110] Clarke and Knake, p. 67.
[111] Buchan p. 212.; Gervais, p. 537; Hannah Lobel, 'Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict' (2011) 47 Tex. Int'l LJ 617, p. 626; Erki Kodar, 'Computer Network Attacks in the Grey Areas of Jus Ad Bellum and Jus in Bello' (2009) 9 Baltic YB Int'l L. 133, p. 139; Silver, p. 92.
[112] *See* for the printed version: Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal Online 2, p. 4.
[113] The Tallinn Manual, rule 11, p. 45.
[114] Ibid. p. 45.
[115] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', p. 914-915.

Severity is the first and the most significant criterion. Cyber operations physically harming people or property is accepted undoubtedly severe enough to amount to the level of the use of force. Beside this, there are some indications in the commentary regarding physical harm consequence as to being not a compulsory requirement for a cyber operation to qualify as a use of force. It is stated that should a cyber operation effects critical national interests, "the scope, duration and the intensity" of the consequences will have great impact on the evaluation of states with regard to severity.[116]

Immediacy is the criterion which takes into consideration the question of how soon were the consequences of a cyber operation occurred.[117] If the effects of the operation emerges in a short time, states would be more willing to call it as a use of force, comparing to the effects arising out weeks or months later.[118]

Directness factor seeks a clear causation between a cyber attack and the effects occurred, focusing on the chain of causation.[119]

Invasiveness is a criterion which is more interested in the nature of the target of a cyber operation. If the target is important enough to protect more than an ordinary infrastructure, the attack would be considered more invasive.[120] The commentary, however, notes that the important nature of the target will still not allow merely a penetration or cyber espionage to qualify as use of force.[121]

Measurability of effects factor concentrates on the visibility of the consequences of cyber operations. The more apparent, "quantifiable and identifiable" of the consequences a cyber operation, the more it would be described as a use force by states.[122]

Military character is a criterion which denotes the fact that the prohibition on the use of force within the meaning of article 2 (4) of the UN Charter is being armed force.[123] Therefore, it is stated the more a cyber operation is linked with a military operation, the more

[116] The Tallinn Manual, p. 48.
[117] Ibid., *supra note* 22, p. 51.
[118] Ibid., p. 49.
[119] Ibid., p. 49.
[120] Ibid., p.49.
[121] Ibid., p. 50.
[122] Ibid., p. 50.
[123] Ibid., p. 51.

it would be regarded as the use force. By the way, this is not one of the criteria of which Schmitt proposed. Schmitt argues that armed force is not necessarily a character of the use of force.[124]

State Involvement refers to the attribution of cyber operations to states. The identification of direct or indirect state involvement in a cyber operation will make the use of force evaluation easier.[125] Though Schmitt had not initially proposed this in 1999, he appended it into his criteria under the name of "responsibility" in his revisiting study in 2011.[126]

Presumptive Legality refers to a principle of international law. If an act is not prohibited by international law, it means it is permissible. Therefore, the operations which are not prohibited by international law such as "propaganda, psychological operations, espionage" will not be regarded as uses of force when they are carried out cyber means too.[127]

These criteria have been criticized by some commentators. In her detailed article on the Schmitt criteria, Katharina Ziolkowski, having examined all the criteria one by one, concludes that the-consequence-based approach is fair enough to deal with cyber operations and if it is adopted, there will be no need for any additional criteria.[128] In addition, she argues that some of the criteria such as directness and presumptive legitimacy cannot be regarded as legal criteria. Directness, though it can apply to the conventional operations as a legal criterion, she claims, it can hardly fit cyber operations which is operated remotely and shows its effects non-directly. As to latter, she gives Kosovo intervention in 1999 as an example, since it is not accepted legal, but legitimate. [129] That being said, Schmitt has never asserted that these are legal criteria. In contrast, he stated that they were to assist to states in assessing cyber operations with regard to the use of force.[130] In the commentary of the Tallinn Manual, the informal nature of the criteria was also acknowledged.[131]

---

[124] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', p. 908.
[125] The Tallinn Manual, p. 51.
[126] Michael N Schmitt, 'Cyber Operations and the Jud Ad Bellum Revisited', p. 577.
[127] The Tallinn Manual, p. 51.
[128] Katharina Ziolkowski, 'Ius ad bellum in Cyberspace-Some Thoughts on the "Schmitt-Criteria" for Use of Force', In *2012 4th International Conference on Cyber Conflict – Proceedings*, Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds.), (Tallinn: NATO CCDCOE), p. 308.
[129] Ibid., p. 303-305.
[130] Michael N Schmitt, 'The Use of Force in Cyberspace: A Reply to Dr Ziolkowski', In *2012 4th International Conference on Cyber Conflict – Proceedings*, Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds.), (Tallinn: NATO CCDCOE) p. 314.
[131] The Tallinn Manual, p. 48.

Ziolkowski continues stating these criteria are too flexible for states to manoeuvre in their decision making process.[132] Another commentator emphasizes this point by illustrating how these criteria can be turned around itself, taking the Schmitt's evaluation on the cyber operations against Estonia. Schmitt claims that the Estonian cyber attacks would qualify as the use of force given that, he argues, they were severe enough to affect essentially the entire society and to disrupt adversely the government functions and the economy. The effects were felt immediately and directly. Because some of the targets of the operations were intended to be protected more, it can be said that the operations were invasive. He concludes that if the operations had been attributed to the Russian government, they would have been amounted to the use of force threshold.[133] Reese Nguyen approaches to the same facts by using the same criteria but from a different point of view and reaches a different conclusion. She argues the operations were not that much severe given that there were no human-being and property being physically damaged and the DDOS operations denied the access to the government websites only for few hours. Second, the effects of the operations were not direct but generally secondary in nature. Third, she rejects that the operations were invasive due to the absence of any penetration of the critical systems which are designed to be highly protected. Fourth, the consequences were unquantifiable because there was no "concrete injury or damage". Last, the operations as being merely interrupting the communication systems are not forbidden by the prohibition of the use of force, therefore they were presumptively legitimate.[134] So, she concludes Estonian attacks were not in breach of the prohibition of the use of force, applying the Schmitt criteria.

Nguyen further proposes another framework called CPS-focused approach, which can also fall under the consequence-based approach, putting emphasize on cyber physical systems.[135] CPS is a cyber physical system which is controlled and commanded by computers.[136] She argues that irreversible disruption or physical damage to CPSs will constitute a use of force. The main contribution of this approach is its inclusion "irreversible disruption" into the scope of the use of force. However, her understanding of "irreversible disruption" is totally based on physical damage criterion: "cyber attacks that do not threaten or result in physical effects should not constitute force under the *jus ad bellum*, because such attacks are

[132] Ziolkowski, p. 308.
[133] Michael N Schmitt, 'Cyber Operations and the Jud Ad Bellum Revisited', p. 577.
[134] Nguyen, p. 1123.
[135] Ibid., p. 1124.
[136] Ibid., p. 1084.

largely reversible."[137] Though this approach took the consequence-based approach a step further in dealing with cyber operations, it restricts itself by overemphasizing physical damage as if it is the main requirement for a cyber attack to qualify as the use of force. Secondly, whereas she criticises the target-based approach due to its CNI concept as being over-inclusive, the CPS concept seems to be broader than CNI, because CPS is any system controlled and commanded by computers, regardless of critical nature of the system.[138] Furthermore, while states have declared their CNIs in advance, there is no such a state which have announced what are its CPSs. Therefore, it does not seem to be practical in current situation.

5.4. Towards the Function-Based Approach?

The literature is based on the main three approaches which have contributed to the development of the field of the cyber operations under international law, particularly *jus ad bellum*. But each of them has itself remained inadequate to fully answer to the challenges posed by cyberspace. The instrument-based approach mostly ignores the new technologies developed in the weapon industry. Accordingly, it rejects the notion of "cyber weapon", therefore it is obsolete in the cyber context. The target-based approach's main flaw is its being too broad. As for the consequence-based approach, it is too focused on the physical damage to ignore other significant effects of the cyber operations. Therefore, there is a need for another approach which intersects the target based approach and the consequence-based approach. Though recent academic studies draw attention to this need, they generally refrain from scrutinizing the issue. I conceptualize "the function-based approach" to offer a better solution in determining a cyber operation whether it qualifies as the use force, which narrows the target-based approach and broadens the consequent-based approach's scope.

Cyber operations, as was mentioned earlier, can potentially have wide ranging effects from a mere penetration of a computer-based system to destroying the building which operates depending on that system. Between these two extremes, there can be other significant consequences of cyber operations such as disabling air defence control system of a state, shutting down its electrical power grids, making inoperable its financial and banking systems, incapacitating critical infrastructures in general. These results, though they may be without

[137] Ibid., p. 1127.
[138] Ibid., p. 1128.

physical damages, can be extremely serious threats for a state's national security, economic security, functioning of public services such as public health, communication, transportation or supply chain. Considering the reliance of modern societies to computer networks, and their interconnectedness with each other, it would hardly be surprising to anticipate cyber operations can cause a chaos in a society even without resulting in any physical damage.[139] To keep critical infrastructures functioning has become vital for the maintaining of societal activities of all kinds in the 21st century. Therefore, ignoring the significance of the functionality of CNIs, rather focusing only physical effects of cyber operations will always have to limp in dealing with the threats cyberspace poses.

An evolutionary interpretation of article 2 (4) of the UN Charter should also cover such effects that significantly disruptive to the CNIs. The function-based approach argues that what matters is the functionality of CNIs in the cyber context, rather than their physical components. Incapacitating a CNI for a long time can be equally destructive as bombing it via conventional weapons. Furthermore, the consequences of a cyber operation totally malfunctioning a CNI can be more severe than a missile destroying some physical parts of the CNI. Therefore, it is not building itself but the functions of the CNI that matters to states. That being said, the function-based approach does not neglect the physical damage caused by cyber operations. It accepts that every cyber operation that qualifies as the use of force under the consequence-based approach will also qualify so under the function-based approach. It takes the CNI concept from the target-based approach, but it does not accept every intervention to the CNIs qualifies as prohibited use of force. There are two main reasons to incorporate the CNI concept. As well as their vitality to modern societies, the other reason is more practical, that is, wide use of the concept by states and international organizations.[140]

The only contribution the instrument-based approach could make for the function-based approach may be found if one considers the definition of cyber weapons. Turning back to the definition of cyber weapons adopted in this study, it can be seen that the criterion for qualifying as a weapon is not only to cause physical harm, but also functional harm: "Computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems or living beings."[141] The recent cyber strategies of some

[139] Stephenie Gosnell Handler, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48 Stan. J. Int'l L. 209, p. 231.
[140] Melzer, p. 14.
[141] Rid, p. 37.

states emphasize how important the functionality of the critical systems as well.[142] The US Cyber Strategy of 2011 states "we will work to build a consensus … among those who view the functioning of these systems as essential to the national and collective interest."[143] The Framework for Improving Critical Infrastructure Cybersecurity of the US starts with explicitly stating the following "the national and economic security of the United States depends on the reliable functioning of critical infrastructure."[144] Disruption of CNIs has been seen as real threats to the national and economic security. In the US Department of Defense (DoD) Cyber Strategy of 2015, the term "destructive" is always employed with the term "disruptive". For example, "A disruptive, manipulative, or destructive cyber attack could present a significant risk to U.S. economic and national security."[145] One of the strategic goals of the DoD is stated to "be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber attacks of significant consequence."[146] The UK also points out the significance of functionality: "The growing use of cyberspace means that its disruption can affect nations' ability to function effectively in a crisis."[147] The Russian Federation highlights the significance of threats which result in "disruption of the normal functioning of information and telecommunication systems and of storage reliability for information resources"[148] As was stated above, a Russian official indicated that loss of life, injury or physical damage to property is not necessary to respond in self defence against cyber attacks: "…Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether it will be casualties or not … and Russia retains the to use nuclear weapons against…"

Considering the approaches of states, though there has yet been state practice regarding cyberspace, it can be clearly seen they will unlikely to restrict themselves to physical damage caused by cyber operations in determining whether the operations amount to the use of force.

---

[142] *See* for the Cyber Security Strategy Documents of States: 'Cyber Security Strategy Documents' (*CCDCOE*, 2014) <https://ccdcoe.org/strategies-policies.html> accessed 12 August 2016.
[143] The White House, 'International Strategy for Cyber Space', p. 9.
[144] National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure' (The US Department of Commerce 2014), p. 1.
[145] The US Department of Defense, 'Cyber Strategy' (2015), p. 2.
[146] Ibid., p. 14.
[147] Cabinet Office of the United Kingdom, 'The UK Cyber Security Strategy Protecting and Promoting the UK in A Digital World' (2011), p. 17.
[148] 'MFA of Russia | 01/10/2000 | National Security Concept of the Russian Federation' (*Archive.mid.ru*, 2000) <http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/36aba64ac09f737fc32575d9002bbf31!OpenDocument> accessed 12 August 2016.

Significant disruption of CNIs also come to the fore when they evaluate cyber operations under *jus ad bellum* framework. This approach gains some support also from the academy. Though the terms used by commentators differ such as "severely disrupting"[149], "large-scale disruption"[150], "incapacitating CNIs"[151], "high-level disruption"[152], "massive, medium to long-term disruption"[153], the purpose of all seems to be the same. *Significant disruption*, which is adopted by most of states, seems proper and sufficient as a criterion in order to satisfy the concerns arising out of the flaws of the consequence-based approach. Moreover, it is argued significant disruption of CNIs may amount to the level of "armed attack" giving rise to the self-defence.[154]

It is almost clear a mere penetration of CNIs should be excluded from the scope of the prohibition of the use of force for the reasons given above. It should be recalled if the target of a cyber operatiion is not a CNI, it will not be regarded as the use of force unless it results in a physical destruction. If the target is a CNI, the first thing to consider is whether there is a loss of function on the CNI. Should the answer be positive, the second consideration must be how significant that functional loss. Indeed, it directs us to the main question: What constitutes a significant disruption to the CNIs?

It depends on the nature of the CNI targeted. It is argued the disruption should not be temporary, but for a long-term. Shutting down an electrical power grid or denying access to the banking systems for a few hours would not be regarded as uses of force. But if the operations on these targets were maintained for a long time such as days or weeks, they would certainly qualify as uses of force[155] due to the significant disruption on the functionality of the targets. The cyber operations carried out against Estonia in 2007 had wide ranging targets and

---

[149] Roscini, *Cyber Operations and the Use of Force in International Law,* p. 55.
[150] Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace' (2012) 6 Strategic Studies Quarterly 126, p. 138.
[151] Melzer, p. 16.
[152] Siobhan Gorman and Julian E Barnes, 'Cyber Combat: Act of War' (*WSJ*, 2011) <http://www.wsj.com/articles/SB10001424052702304563104576355623135782718> accessed 13 August 2016.
[153] Ziolkowski, p. 299.
[154] "…cyber attacks on the controlling information technology for a nation's infrastructure that had a significant impact on the functioning of that infrastructure (whether or not it caused immediate large-scale death or destruction of property) would be an armed attack for Article 51 purposes, just as would a kinetic attack that somehow managed to shut down the system without such immediate secondary effects." William A Owens, Kenneth W Dam and Herbert S Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academies Press 2009), p. 254; *See* for the similar view, Melzer, p. 16; Brown and Poellet, p. 137.
[155] Herbert S Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 J. Nat'l Sec. L. & Pol'y 63, p. 74.

effects. The websites of parliament, presidency, ministries, other state agencies and political parties were denied to access and defaced. Public and private internet service providers were targeted. The services provided by the banks and news organisations were affected. The cyber operations lasted in three weeks. Considering the Estonian government's and society's high dependency on the internet, the consequences of the operations were perceptible.[156] Based on this information, an author concludes Estonian attacks amounted to the use of force.[157]

However, viewing the situation in more detail, it can be seen the cyber operations against Estonia would hardly be deemed as the use of force. First of all, the operations were not carried out unceasingly. The first phase of operations, 27 to 29 April, was mainly emotional, simple and uncoordinated. The second phase, consisting of four waves, however, was more sophisticated and coordinated. There were almost five days without attacks between the waves. In other words, the Estonian targets were not prevented from functioning in the entire three weeks. In details, the online services of Hansapank and SEB Eesti Ühispank, the two largest banks of the Estonia, were denied to access for only ninety minutes.[158] Though some economic damage occurred in the wake of the operations, the disruptions were not significant enough to amount to the use of force. Secondly, the government and other websites were not long-term but temporarily unavailable and the consequences of the operations against these websites were not critical nor significant.[159] Thirdly, despite some of the internet communication technology (ICT) infrastructures were affected to some extent, traditional CNIs were not targeted.[160] Lastly, article 5 of the North Atlantic Treaty, regarding collective defence, was not really taken into consideration to invoke against Estonian attacks.[161]

Although the duration of cyber operations matters in evaluating the operations with regard to the use of force, the disruption does not have to be "long-term" to qualify as significant disruption. In 2007, an unexpected incident happened in Syrian deserts. The Syrian government were secretly building a nuclear facility in cooperation with the North Korean government in the middle of a desert near Turkish border. Israelis detected the building under construction and took it as a serious threat against themselves and planned an operation called

[156] Tikk, Kaska, Vihul, p. 33.
[157] Michael N Schmitt, 'Cyber Operations and the Jud Ad Bellum Revisited', p. 577.
[158] Tikk, Kaska, Vihul, p. 22.
[159] Ibid., p. 25.
[160] Ibid., p. 21.
[161] Ibid., p. 26.

"Operation Orchard".[162] Seven Israeli jets easily entered the Syrian airspace without warning and destroyed the facility by dropping bombs and safely turned back to their base with no anti-aircraft attack against them by Syrians. What was behind the success of the operation was a cyber attack prior to the involvement of the jets into the operation. The air defence system of Syria had totally been inactivated by Israelis through cyber operations. For this reason, Syrians had never been aware of the enemy jets flying over their aerial territory.

Despite the fact that the cyber attack targeting the Syrian air defence system was a matter of a few hours in one night, it would qualify as the use of force. Defence infrastructures are also amongst the most important CNIs.[163] Considering the nature of the defence structures, incapacitating them through cyber operations allowing an enemy state to make operations over its aerial territory would be deemed a significant disruption even if the attacks are not a long-term nor do not themselves cause a physical damage. The loss of function of air defence system in Syrian case is so significant that the target state lost "its ability to conduct military operations". [164] An example given by the US DoD in 1999 exactly overlaps such incident happened in Syria: "If a coordinated computer network attack shuts down a nation's air traffic control system … it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack." [165] For the above reasons, the cyber attack against Syria, regardless of its duration and lack of physical damage caused by itself, would surely amount to the use of force under the function-based approach.

When it comes to the financial and economic infrastructures, most of the authors easily concludes that cyber operations targeting these infrastructures would not constitute the use of force, because, they argue, economic and political coercion is excluded from the scope of the prohibition. This approach, actually, is to refrain from challenging the real problem that new technologies have brought into question. Economic security, along with the national security, is one of the most important priorities of states to protect, as we have seen when analysing

[162] Peter W Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know* (Oxford University Press 2014), p. 127.
[163] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 58.
[164] The U.S. Department of Defense Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (1999), p. 18.
[165] Ibid., p. 18.

CNIs.[166] Considering the aspect of being CNI of economic and financial systems, one must be more meticulous in evaluating cyber operations targeting these systems. One commentator rightly questions "the manipulation of a state's economic data may have serious repercussions on the state's economic and political well being, which may not translate into immediate death or destruction, but may nevertheless be serious in view of the reliance of modern states on information technology. This can have the same effect as the one which can be produced by the physical destruction of a state's economic institutions. Why should the physical destruction of a state's main economic institutions be a use of force and not their functional paralysis?"[167]

Admittedly, it is not always easy to distinguish between armed force and economic coercion. The line between these two sometimes can be very slight.[168] Within the developments in cyberspace, drawing that line have become much more difficult. Nevertheless, there seems to be some differences in nature between traditional economic coercions and the operations against economic infrastructures of states through cyberspace. Traditional economic coercions such as boycotts, trade sanctions, severance of economic relations, embargo, unfair tax practises can be characterized as external[169] measures for the states against which the coercion imposed by another state unilaterally or other states collectively. What draws attention here is that the economy is used as a tool to compel a state to do or not to do something. In the event of cyber operations against economic structures of a state, the economy is a direct target, but not a mean.[170] Cyber operations is directly involved within the territorial sovereignty of the target state. The means are cyber weapons, which are considered to be new forms of armed forces. The use of weapon, as was mentioned above, is at the heart of the definition of "armed force". To that effect, a question is rightly raised: Do the cyber operations targeting economic and financial infrastructures of a state fit more into the definition of economic coercion or armed force?[171]

---

[166] *See* also Marco Roscini, 'World Wide Warfare-Jus ad bellum and the Use of Cyber Force' (2010) 14 Max Planck Yearbook of United Nations Law 85, p. 117-119.
[167] Nicholas Tsagourias, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force', *Yearbook of International Humanitarian Law Volume 15, 2012* (Springer 2014) <http://link.springer.com/chapter/10.1007/978-90-6704-924-5_2> accessed 15 August 2016, p. 22.
[168] Todd C Huntley, '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' (2010) 60 Naval L. Rev. 1, p. 26.
[169] Silver, p. 82.
[170] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p. 62.
[171] Vida M Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places' (2005) 51 Naval L. Rev. 132, p. 155.

Under the function-based approach, the cyber operations significantly disrupting the functions of economic and financial infrastructures, as them being CNIs, would qualify as uses of force. It could also be argued that there is an "interpretive reorientation"[172] regarding economic security in understanding of major powers. Considering the national and cyber strategies of states, it has been declared by most of the states, including the P-5 countries, that they would respond cyber operations targeting their economy under the regime of self-defence. The function-based approach is to fill the gaps regarding economic security of states, left by the consequence-based approach and the instrument-based approach and to prevent possible escalations the target-based approach may cause.

One may propose to set criteria such as scope, duration and intensity to tackle the determination of significant disruption, however, it may not always helpful. The examples given above have shown that different functions of each particular CNI would require a *case-by-case* determination of *significant disruption* on the functions of CNIs.

6. Conclusion

Within the development of new technologies in cyberspace, one more threat has emerged that human-being has to face. The cyber methods and means of warfare posed challenges to the classical understanding of the rules regarding *jus ad bellum* framework. While the use of force is already one of the most controversial issues of the public international law, it has become much more sophisticated within the involvement of cyber weapons. The question of how sufficient the existing rules for cyberspace will remain unless a new cyber-specific treaty concerning the laws of war is accepted by states. It seems difficult for states, however, to reach a consensus on a cyber-specific treaty due to their different legal approaches to cyberspace. In these circumstances, what becomes much more important is to search how to apply the existing rules to cyberspace. This study has focused on the application of one existing rule, that is article 2 (4) of the UN Charter.

The UN Charter has evolved over time to answer new challenges, when its plain words have remained inadequate in different respects. The use of force concept was restricted to the use of conventional kinetic weapons until chemical and biological weapons were proved to

[172] Waxman, p. 437.

create the same consequences such as deaths, injuries or damage to property not through kinetic force, but shock waves. Thus, the scope of the prohibition had to expand in the face of new challenges. The shift from the instrument-based approach to the consequence-based approach in understanding of the prohibition has been largely accepted. The consequences, it has been argued, should have required physical damages on living or non-living things. Cyber operations, however, can cause significant consequences with no physical damage on critical national systems, considering the dependency of modern societies on the internet and computer based systems. There was a need for another shift in the understanding of the prohibition to answer the challenges cyberspace has posed. The target-based approach might have been a candidate to make this shift, but it was too broad in scope, therefore it did not gain much support.

Considering CNIs' vitality for a state and the society, this contribution has focused the function of CNIs. It has advocated that the function of CNIs has become much more important than merely physical damages to the buildings. If a cyber attack significantly disruptive to the function of a CNI, notwithstanding a physical damage has occurred or not, it should also constitute a use of force within the meaning of article 2 (4) of the UN Charter. This approach is an intersection of two main approaches given above. It fills the gap left by the consequence-based approach and reduces the scope of the target-based approach. Though it is not entirely new in this regard, it offers a better solution, taking into consideration the reliance of modern societies to the internet and computer-based systems, and the characteristics of cyber operations. Function-focused approaches would be expected to make the shift needed.

BIBLIOGRAPHY

Table of Cases

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986

Corfu Channel Case, (Albania v. The United Kingdom), Merits, Judgment of April 9th, 1949, ICJ Reports 1949

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996

Treaties

1945 Charter of the United Nations

2001 Budapest Convention on Cybercrime, Council of Europe

1969 Vienna Convention on the Law of Treaties

The UN Documents

UN Doc A/Res/25/2625, 24 October 1970, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations

UN Doc A/Res/42/22, 18 November 1987, Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations

UN Doc A/Res/53/70, 4 January 1999, Resolution Adopted by The General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security

UN Doc A/Res/58/199, 30 January 2004, Resolution Adopted by The General Assembly Creation of a global culture of cybersecurity and the protection of critical information infrastructures

UN Doc A/65/201, 30 July 2010, The Report by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

UN Doc A/66/152, 15 July 2011, Report of the Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security

UN Doc A/66/359, 14 September 2011, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General

UN Doc A/68/98, 24 June 2013, Note by the Secretary-General, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

UN Doc A/68/156, 16 July 2013, Report of the Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security

UN Doc A/69/723, 13 January 2015 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

UN Doc A/70/174, 22 July 2015, Note by the Secretary-General, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Documents Including Military Manuals, Cyber Strategies and Legislations

The European Union

Council Directive 2008/114/EC, [2008] L 345/75

European Commission COM (2011) 163 final

European Parliament resolution P7_TA (2012) 0237, [2011/2284(INI)]

European Commission JOIN (2013) 1 final

The United States

Cartwright JE, 'Joint Terminology for Cyberspace Operations' [2010] Joint Chiefs of Staff (JCS) Memorandum, Nov

The US Department of Commerce, National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure' (Washington DC 2014)

The US Department of Defense, 'Cyber Strategy' (Washington DC 2015)

The US Department of Defense, 'Information Operations', *Dictionary of Military and Associated Terms*, (Washington DC 2010, as amended through 15 February 2016)

The U.S. Department of Defense Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (Washington DC 1999)

The White House, 'International Strategy for Cyberspace: Prosperity, Security, And Openness in A Networked World' (2011)

The White House, 'Executive Order 13010 Critical Infrastructure Protection' (1996)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001

The Shanghai Cooperation Organisation

The Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, 16 June 2009), *see* for an unofficial English translation: 'Shanghai Cooperation Organisation' (*NATO Cooperative Cyber Defence Centre of Excellence*) <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf> accessed 3 August 2016.

The United Kingdom

Cabinet Office of the United Kingdom, 'The UK Cyber Security Strategy Protecting and Promoting the UK in A Digital World' (London 2011)

'The National Infrastructure' (*Cpni.gov.uk*, 2016) <http://www.cpni.gov.uk/about/cni/> accessed 2 August 2016.

The Russian Federation

'MFA of Russia | 01/10/2000 | National Security Concept of the Russian Federation' (*Archive.mid.ru*, 2000) <http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/36aba64ac09f737fc32575d9002bbf31!OpenDocument> accessed 12 August 2016.

Books

Brownlie I, *International Law and the Use of Force by States* (Oxford: Clarendon Press 1963)

Clarke RA and Knake RK, *Cyber War* (HarperCollins 2011)

Dinniss HH, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012)

Garner BA, *Black's Law Dictionary*, 10th Edition, (Thomson Reuters 2014)

Gray C, *International Law and the Use of Force* (3rd edition, Oxford University Press 2008)

Owens WA, Dam KW and Lin HS, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academies Press 2009)

Rid T, *Cyber War Will Not Take Place* (Oxford University Press, USA 2013)

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

Schmitt MN, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)

Sharp WG, *Cyberspace and the Use of Force* (Aegis Research Corporation 1999)

Singer PW and Friedman A, *Cybersecurity: What Everyone Needs to Know* (Oxford University Press 2014)

Tikk E, Kaska K and Vihul L, *International Cyber Incidents: Legal Considerations*, vol 112 (Cooperative Cyber Defence Centre of Excellence 2010)

Woltag J-C, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Intersentia 2014)

Chapters in Edited Books

Arimatsu L, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations', In *2012 4th International Conference on Cyber Conflict – Proceedings*, Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds.), (Tallinn: NATO CCDCOE)

Blank LR, 'Cyberwar Versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace', in Jens David Ohlin, Kevin Govern, Claire Finkelstein (ed), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015)

Gray C, 'The Use of Force and the International Legal Order', in Malcolm Evans (ed), *International Law,* (4th Edition, Oxford University Press 2014)

Randelzhofer A, Dörr O, 'Ch.I Purposes and Principles, Article 2 (4)', in Bruno Simma (ed), *The Charter of the United Nations: A Commentary*, (Volume I, 3rd Edition, Oxford University Press 2012)

Schmitt MN, 'The Use of Force in Cyberspace: A Reply to Dr Ziolkowski', In *2012 4th International Conference on Cyber Conflict – Proceedings*, Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds.), (Tallinn: NATO CCDCOE)

Katharina Ziolkowski, 'Ius ad bellum in Cyberspace-Some Thoughts on the "Schmitt-Criteria" for Use of Force', In *2012 4th International Conference on Cyber Conflict – Proceedings*, Christian Czosseck, Rain Ottis, Katharina Ziolkowski (eds.), (Tallinn: NATO CCDCOE)

LL.M Thesis

Valo J, 'Cyber Attacks and the Use of Force in International Law' (Master of Laws, University of Helsinki 2014)

PH. D Thesis

Korzak E, 'Computer Network Attacks and International Law' (Ph.D, War Studies Department of King's College London 2015)

Journal Articles

Antolin-Jenkins VM, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places' (2005) 51 Naval L. Rev. 132

Benatar M, 'Use of Cyber Force: Need for Legal Justification, The' (2009) 1 Goettingen J. Int'l L. 375

Blank S, 'Web War I: Is Europe's First Information War a New Kind of War?' (2008) 27 Comparative Strategy 227

Brown G and Poellet K, 'The Customary International Law of Cyberspace' (2012) 6 Strategic Studies Quarterly 126

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 212

Dinstein Y, ‘Computer Network Attacks and Self-Defense’ (2002) 76 Int’l L. Stud. Ser. US Naval War Col. 99

Gervais M, ‘Cyber Attacks and the Laws of War’ (2012) 30 Berkeley Journal of International Law 525

Handler SG, ‘The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare’ (2012) 48 Stan. J. Int’l L. 209

Hathaway OA and others, ‘The Law of Cyber-Attack’ [2012] California Law Review 817

Heickerö R, ‘Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations’ (Defence Analysis, Swedish Defence Research Agency (FOI) 2010) User Report FOI-R--2970--SE

Hollis DB, ‘Why States Need an International Law for Information Operations’ (2007) 11 Lewis & Clark Law Review 1023l

Huntley TC, ‘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’ (2010) 60 Naval L. Rev. 1

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

Joyner CC and Lotrionte C, ‘Information Warfare as International Coercion: Elements of a Legal Framework’ (2001) 12 European Journal of International Law 825

Kodar E, ‘Computer Network Attacks in the Grey Areas of Jus Ad Bellum and Jus in Bello’ (2009) 9 Baltic YB Int’l L. 133

Koh HH, ‘International Law in Cyberspace’ (2012) 54 Harvard International Law Journal

Langner R, ‘To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve’ [2013]

Lessig L, ‘The Law of the Horse: What Cyberlaw Might Teach’ (1999) 113 Harvard Law Review 501

Lin HS, ‘Offensive Cyber Operations and the Use of Force’ (2010) 4 J. Nat’l Sec. L. & Pol’y 63

Lobel H, ‘Cyber War Inc.: The Law of War Implications of the Private Sector’s Role in Cyber Conflict’ (2011) 47 Tex. Int’l LJ 617

Melzer N, *Cyberwarfare and International Law* (UNIDIR 2011)

Moore S, ‘Cyber Attacks and the Beginnings of an International Cyber Treaty’ (2013) 39 North Carolina Journal of International Law and Commercial Regulation 223

Morth TA, ‘Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2 (4) of the UN Charter’ (1998) 30 Case W. Res. J. Int’l L. 567

Mueller B, ‘The Laws of War and Cyberspace on the Need for a Treaty Concerning Cyber Conflict’ (June 2014)

Nguyen R, ‘Navigating Jus Ad Bellum in the Age of Cyber Warfare’ (2013) 101 California Law Review 1079

Richmond J, ‘Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict’ (2012) 35 Fordham International Law Journal 842

Roscini M, ‘World Wide Warfare-’Jus Ad Bellum’and the Use of Cyber Force’ (2010) 14 Max Planck Yearbook of United Nations Law 85

—— ‘Cyber Operations as a Use of Force’ [2015] Research Handbook on International Law and Cyberspace, Edward Elgar Publishing 233

Schmitt MN, ‘Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework’ (1999) 37 Columbia Journal of transnational law 1998

—— ‘Cyber Operations and the Jud Ad Bellum Revisited’ (2011) 56 Villanova Law Review 569

—— ‘International Law in Cyberspace: The Koh Speech and the Tallinn Manual Justaposed’ (2012) 54 Harward International Law Journal 13

Silver DB, ‘Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter’ (2002) 76 Int’l L. Stud. Ser. US Naval War Col. 73

Simmons N, ‘A Brave New World: Applying International Law of War to Cyber-Attacks’ (2014) 4 Journal of Law & Cyber Warfare 42

Tsagourias N, ‘The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force’, *Yearbook of International Humanitarian Law Volume 15, 2012* (Springer 2014)

Waxman MC, ‘Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)’ (2011) 36 Yale Journal of International Law 421

Web Sources

‘Armed - Oxford Reference’ <http://www.oxfordreference.com/view/10.1093/acref/9780195392883.001.0001/m_en_us1222947> accessed 27 July 2016

‘Cyber Security Strategy Documents’ (*CCDCOE*, 6 June 2014) <https://www.ccdcoe.org/strategies-policies> accessed 31 August 2016

Davis J, ‘Hackers Take Down the Most Wired Country in Europe | WIRED’ <http://www.wired.com/2007/08/ff-estonia/> accessed 31 August 2016

Gorman S and Barnes JE, ‘Pentagon: Online Cyber Attacks Can Count as Acts of War - WSJ’ *Wall Street Journal* (31 May 2011) <http://www.wsj.com/articles/SB10001424052702304563104576355623135782718> accessed 31 August 2016

Interview with John Arquilla, 'Cyber War!' (24 April 2003) <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html> accessed 31 August 2016

'Kaspersky DDoS Intelligence Report Q3 2015 - Securelist' <https://securelist.com/analysis/quarterly-malware-reports/72560/kaspersky-ddos-intelligence-report-q3-2015/> accessed 31 August 2016

Katz Y, '"Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years" - Iranian Threat - Jerusalem Post' <http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years> accessed 31 August 2016

Kulikova A, 'Can a New UN Cyber Agreement Be a Win-Win for Russia, US? | Russia Direct' (*www.russia-direct.org*) <http://www.russia-direct.org/analysis/can-new-cyber-agreement-among-un-experts-be-win-win-russia-us> accessed 28 June 2016

Maclean W, 'UPDATE 2-Cyber Attack Appears to Target Iran-Tech Firms | Reuters' <http://www.reuters.com/article/security-cyber-iran-idUSLDE68N1OI20100924> accessed 31 August 2016

Traynor I, 'Russia Accused of Unleashing Cyberwar to Disable Estonia' *The Guardian* (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 31 August 2016

'Use of Nuclear, Biological or Chemical Weapons: Current International Law and Policy Statements - ICRC' (12:44:35.0) <https://www.icrc.org/eng/resources/documents/misc/5ksk7q.htm> accessed 27 July 2016

'War in the Fifth Domain | The Economist' <http://www.economist.com/node/16478792> accessed 31 August 2016

'What Is SCADA? Webopedia Definition' <http://www.webopedia.com/TERM/S/SCADA.html> accessed 31 August 2016