E-JOURNAL OF LAW

The Law of Cyber Warfare In Terms of *Jus Ad Bellum* and *Jus In Bello*: Application of International Law to the Unknown?

Fatma TAŞDEMİR[*]

Gökhan ALBAYRAK[″]

Abstract

In this study, the relationship between cyber warfare and the norms of international law will be examined. Especially the position of cyber warfare in terms of *jus ad bellum* and *jus in bello* will be analysed. From this point of view, it can be said that the concepts of cyber armed attack, cyber armed conflict and the law of cyber warfare are included in the area of international law. Yet the difficulties about non-physical features of cyber space necessitates a detailed examination with regard to international law. In this respect, the law of cyber warfare is in some ways an application of international law to the unknown.

Keywords: Cyber space, cyber-attack, cyber warfare, armed attack, armed conflict.

[*] Assoc. Prof., Gazi University, Faculty of Economics and Administrative Sciences, tfatma@gazi.edu.tr

[″] Res. Assist. Dr., Gazi University, Institute of Social Sciences, albayrak87@gmail.com

Introduction

It is hard to give a comprehensive definition of cyber space. Yet cyber space can be defined as the world of web of computers where information is saved, shared and transmitted.[1] There are services to humanity as well as risks and threats in evolving cyber space. The spectacular developments in the computer technology differentiated threats to the national security and changed the nature of armed conflicts in the context of international law. Nowadays, the governments use social media for regime change and signals for espionage and start war on-line.[2] However, it is not certain which act is "cyber terrorism", what is "cyber-attack" and "cyber espionage" and what is "cyber warfare" in the global cyber space including civilians and armed forces in terms of international law. There is no specific international treaty about the law of cyber warfare. Despite the fact that an International Group of Experts prepared the Tallinn Manual which includes the rules about cyber warfare, it is not a binding set of rules in the nature of things. There is a problem emerging about the lacunae of international law with regard to cyber space and the application of the rules and principles of *jus ad bellum* and *jus in bello* designing for the kinetic attacks to cyber warfare.

In this article, the issue of cyber warfare is examined in terms of *jus ad bellum* and *jus in bello*. At first, it will be analysed that what type of cyber act constitutes "use of force" and what kind of cyber-attack forms "armed attack" within realm of *jus ad bellum*. In this regard, the problems of widening of the United Nations Charter's norms to cyber space will be discussed. Secondly, the subject of cyber armed attacks will be elaborated within the context of *jus in bello*. Especially the matters of the principle of distinction and targeting of civilians/hackers by armed forces of states and other groups will be examined.

I.The Cyber Space and The Examples of Cyber-Attacks

Cyber space is an area of information. It comprises the generated, saved and shared digital data. Cyber space has four sub-elements such as material space: place, distance, size and route.[3] It is not only a virtual world, it combines the systems and infrastructures enabling the flow of data. One of the important feature of this space is that it is a man-made space. Cyber space is fragmentable and its fragments can turn on/off with one click.[4]

Impressive cyber-attack events have occurred in cyber space over recent years. For instance, DDoS (distributed denial of service) attacks seeking the critical infrastructures of Estonia in the year of 2007 put a spotlight on cyber space. Estonia's accession to NATO in 2004 disturbed Russian ethnic minority and Russia itself. After that, the relocation of a bronze statute symbolizing the Soviet power and equal rights for Russian community in Estonia

[1] Peter W. Singer, Allan Friedman, *Siber Güvenlik ve Siber Savaş*. Translated by Ali Atav. (Buzdağı 2015) 28

[2] Priyanka R. Dev, 'Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response' (2015) 50(2) Texas International Law Journal, 380

[3] Rebecca Bryant, 'What Kind of Space is Cyberspace' (2001) 5 Minerva: An Internet Journal of Philosophy, 142

[4] Peter W. Singer, Allan Friedman, Ibid, 29-31

increased the uneasiness. Extensive protests started and this events named "Bronze Night".[5] Aftermath of Bronze Night cyber-attacks were carried out against the web sites of Estonian government, banks and media.[6] Estonian government claimed that attacks were made by Russia but there was no certain evidence. But Gervais alleged like many others that "Russian 'hacktivists' used massive DDoS attacks to target Estonia's web servers and bring web traffic to a halt"[7].

Georgia experienced massive cyber-attacks to telecommunication systems, the web sites of government and media by Russian hackers during the South Ossetia War in 2008.[8] A virus named Stuxnet deactivated a number of uranium enrichment centrifuges of Iran in 2010.[9] Despite that there is no certain proof which country is responsible, the virus is frequently described as an American-Israeli cyber weapon by computer experts.[10] In 2012, Saudi Aramco, one of the biggest oil company in the world, suffered from outstanding cyber-attacks. A news in CNN reported that "in a matter of hours, 35,000 computers were partially wiped or totally destroyed".[11] At November 2012 the Israeli government "said it has been hit with more than 44 million cyber-attacks since it began aerial strikes on Gaza last week"[12]. Anonymous, a group of hackers, took responsibility for these cyber-attacks.

All these events show us that the facts similar to war and conflict can occur in cyber space. In this version of new wars[13] non-state actors join the conflicts and these conflicts take shape in non-material space instead of battlefronts.

II.Cyber Space and *Jus Ad Bellum*

1)The Norms on Kinetic Use of Force

The prohibition of use force became concrete as a norm in the Article 2/4 of the United Nations Charter: "All Members shall refrain in their international relations from t*he threat or use of force* against the territorial integrity or political independence of any state, or in any

[5] Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30(2) Berkeley Journal of International Law, 539

[6] Stephen Herzog, 'Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4(2) Journal of Strategic Security, 50-51

[7] Michael Gervais, op. cit. , 540

[8] John Markoff, 'Before the Gunfire, Cyberattacks', The New York Times, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html, accessed 8.9.2017

[9] BBC News, 'Stuxnet 'hit' Iran Nuclear Plans', 22 November 2010, http://www.bbc.co.uk/news/technology-11809827, accessed. 8.9.2017

[10] David A. Sanger, 'Obama Order Step Up Wave of Cyberattacks Against Iran', The New York Times, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, accessed 1.9.2017

[11] Jose Paglieri, 'The Inside Story of the Biggest Hack in History' CNN Tech, http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html, accessed 20.11.2017

[12] John D. Sutter, "Anonymous declares 'cyberwar' on Israel", CNN, 20 November 2012, http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html, accessed 2.10.2017

[13] See for the concept of new wars. Herfried Münkler, The New Wars, (Polity Press 2005)

other manner inconsistent with the Purposes of the United Nations"[14]. In fact this norm reflects international customary law[15] and this point is continuingly supported by the International Court of Justice (ICJ) in its several decisions and advisory opinions.[16] But the content of the prohibition is disputed. The prohibition of use of force is applicable only within the relations of the states[17] and the normative international law has not a precise definition of use of force and threat of force.[18]

The right of self-defence is the exception to the prohibition of use of force and this right stems from international customary law and the Article 51 of the United Nations Charter. This article reads as follows: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security"[19]. The meaning and scope of this article is very controversial. At first, the definition of armed attack does not appear in the Charter. Then, the expression of "if an armed attack occurs" sows discord among restrictionists and counter-restrictionists about the possibility of anticipatory self-defence within the context of the right of self-defence.[20]

2.Cyber Operations and *Jus Ad Bellum*

Are aforementioned principles on the use of force in the United Nations Charter applicable to cyber operations? Is there any cyber armed attack? What is the relationship between use of cyber force and cyber armed attack? How can cyber-attacks be attributed to states? These questions are open to argument.

Tallinn Manual[21] is the most helpful and important document in the sphere of norms about use of cyber force. It was prepared by the International Group of Experts, world-class academics

[14] United Nations Charter (1945), https://treaties.un.org/doc/publication/ctc/uncharter.pdf, accessed 23.11.2017

[15] Christine Gray, International Law and the Use of Force, (Oxford University Press 2000) 19

[16] See, Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 9); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 186–191 (June 27); Legality of Use of Force (Yugo. v. Belg.), 1999 I.C.J. 124 (June 2); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, 223-24 (Dec. 19); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J 226, 266 (July 8); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 131, 87 (July 9)

[17] Zakaria Dabone, 'International Law: Armed Group in a State-centric System' (2011) 93(882) International Review of the Red Cross, 398-399

[18] Yoram Dinstein, War, Aggression And Self-Defence, (Grotius Publications Limited 1988) 84

[19] United Nations Charter (1945), https://treaties.un.org/doc/publication/ctc/uncharter.pdf, accessed 23.11.2017

[20] Stanimir A. Alexandrov, Self-Defense Against the Use of Force in International Law, (Kluwer Law International 1996) 161

[21]Tallinn Manual on the International Law Applicable to Cyber Warfare, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf, accessed 4. 11. 2017; Michael N. Schmitt (Ed.),

on the *jus ad bellum* and *jus in bello* and it has 95 rules about cyber warfare.[22] NATO, the International Committee of Red Cross and the US Cyber Command were invited to provide observers to the drafting process. It is the well-known non-binding document about the norms of cyber warfare to date.

Tallinn Manual sets out that states have sovereignty over their cyber infrastructures and activities within their territories. This means that states have jurisdiction to regulate, adjudicate and enforce on cyber activities within their territories.[23] There is a debate over which cyber act constitutes a violation of sovereignty. If there is a physical damage or injury to people due to cyber act, we can talk about the violation of sovereignty. But cyber act which does not constitute a physical damage or injury to people or intervention to internal affairs of other state is disputed in the context of *jus ad bellum*.[24]

a)The Arguments About Which Acts Do Constitute Use of Cyber Force

The prohibition on the use of force within the context of cyber space concerns whether a cyber operation made by a state or attributed to a state is a violation of the prohibition. The Rule 10 of Tallinn Manual expands the scope of the prohibition on the use of force. The Rule 10 reads as follows: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful"[25].

ICJ refused the literal interpretation of the concept of the use of force in the judgment of the Case Concerning Military and Paramilitary Activities in and Against Nicaragua. The Court held that "the arming and training of the contras can certainly be said to involve the threat or use of force" and "that the mere supply of funds to the contras … does not in itself amount to a use of force".[26] Furthermore ICJ ruled that "assistance to rebels in the form of the provision of weapons or logistical or other support" could be regarded as the use or the threat of force.[27] In this sense non-destructive cyber acts such as providing malicious software to rebels or training rebels for the use of this kind of software may constitute the use of force. The Rule 11 of Tallinn Manual suggests a formula for regarding an act as the use of force: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"[28]. Tallinn Manual adopted an effect based test

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (Cambridge University Press 2017)

[22] Terence Check, 'Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict, NATO-Centric Approach', (2015) 63 Cleveland State Law Review, 504

[23] Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis', (2014) 25 Stanford Law & Policy Review, 274

[24] Ibid, 274-276

[25] Tallinn Manual on the International Law Applicable to Cyber Warfare, 42-43

[26] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, prg. 228 (June 27)

[27] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, prg. 195 (June 27)

[28] Tallinn Manual on the International Law Applicable to Cyber Warfare, 45

and employed seven factors for determining process. Priyanka R. Dev listed and summarized these factors:

"1. Severity: Analyze the level of harm or damage that was caused to individuals and property, with an eye towards the scale, scope, and duration of consequences.

2. Immediacy: Analyze whether the act had more immediate effects or consequences; if a violated state was given the opportunity to avoid or forestall the consequences (i.e., the consequences were less immediate), it is less likely that the act should constitute a use of force.

3. Directness: Analyze how direct the causation between the initial act and resulting consequences is; the more direct, the more likely it should constitute a use of force

4. Invasiveness: Analyze the degree to which a network system was penetrated; the penetration of a classified system should fall closer to a use of force than that of a declassified system.

5. Measurability: The more quantifiable and identifiable the consequences, the more likely the act is to constitute a use of force.

6. Presumptive Legitimacy: Consider whether the act is presumptively unlawful; if the act is explicitly unlawful, then the act is more likely to constitute a use of force.

7. State Responsibility: The greater the state involvement in the act, the greater the threat to international stability and the more likely the act is to constitute a use of force."[29]

This model broadens the scope of the concept of use of force, but it is helpful for states to analyse the particular cases.[30] Nevertheless these factors may not be helpful for determining process at the time of incident.

b)The Arguments About Which Acts Do Constitute Armed Cyber-Attacks

It is a problematic issue that which acts do constitute armed attack in international law. In the age of new wars, the concept of armed attack broadens and it must be interpreted broadly and result-based.[31] Karl Zemanek argues that "the use of any device, or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfil the conditions of an 'armed' attack"[32]. This argument is accepted in the Tallinn Manual and the International Group of Experts agreed that any use of force killing or injuring people and destroying the property can be regarded as armed attack.[33]

[29] Priyanka R. Dev, op. cit., 389

[30] Michael N. Schmitt, op. cit., 280; Priyanka R. Dev, op. cit., 389

[31] Michael N. Schmitt, ' 'Attack' as a Term of Art in International Law: Cyber Operations Context', (2012) 4th International Conference on Cyber Conflict, NATO CCD COE, 287-288

[32] Karl Zemanek, 'Armed Attack', (2017) Max Planck Encyclopedia of Public International Law, online edition, Ed.Rüdiger Wolfrum, Oxford University Press, prg. 21

[33] Tallinn Manual on the International Law Applicable to Cyber Warfare, 55

Organized cyber armed groups can carry out cyber-attacks against any state reaching the level of armed attack. These cyber-attacks trigger the right of self-defence of attacked state if other state which harbours the cyber-attackers is unwilling or unable to stop these acts.[34]

III. Cyber Space and *Jus In Bello*

Global cyber space became the integral part and means of modern armed conflicts. The use of cyber space as a weapon is not prohibited. This using should not be against the principles of distinction and proportionality such as other weapons. But cyber space is an amorphous space by its very nature. The seconds are important in cyber-attacks and it is hard to find perpetrators of cyber-attacks. These features of cyber warfare make things hard for the application of the norms of *jus in bello* to cyber space.

Civilians take an active role in modern armed conflict and they carry out defensive and aggressive cyber-attacks. This situation causes an uncertainty about the characterization of a person within the context of *jus in bello*. Who will be the legal targets in cyber space is the one of the hardest problem in the law of cyber warfare.

For instance, a British man named Junaid Hussain who is believed to have become the leader of a hacker group, CyberCaliphate, of ISIS in Syria was targeted by US drone strike in 2015.[35] Ido Kilovaty argued that "Hussain's death represents the first time a hacker was lethally targeted"[36]. It can be said that targeting of hackers will be the one of the important debate of *jus in bello* in future. For this reason, surveying of the norms of *jus in bello* related to cyber warfare is a must.

1.The Types of Armed Conflicts

Jus in bello, or international humanitarian law, which is a specific area of international law is applicable only in times of armed conflict. The Geneva Conventions of 1949, The Additional Protocols of 1977 and customary international humanitarian law are the most important norms of *jus in bello*. The main aims of *jus in bello* are the humanization of war and the protection of civilians.

There are two types of armed conflicts in *jus in bello*: International armed conflict and non-international armed conflict. However there is not a certain definition of the concept of armed

[34] See. Ashley s. Deeks, ' 'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense', (2012) 52 Virginia Journal of International Law, 483-550

[35] Caroline Mortimer, 'Junaid Hussain: British-born Isis hacker killed following US drone strike in Syria', Independent, 27 August 2015, http://www.independent.co.uk/news/world/middle-east/british-born-isis-hacker-killed-us-drone-strike-in-syria-kills-junaid-hussain-10474007.html, accessed 29.11.2017

[36] Ido Kilovaty, 'ICRC, NATO And The US-Direct Participation in Hacktivities- Targeting Private Contractors and Civilians Cyberspace Under International Humanitarian Law', (2016) 15(1) Duke Law & Technology Review, 2

conflict.[37] International armed conflict means an armed conflict between two or more states' armed forces (The Common Article 2 of the Geneva Conventions of 1949). As generally accepted, the scope, intensity and duration of the conflict do not matter with regard to international armed conflict.[38] For example, an armed conflict between the cyber armed forces[39] of two states would be an international armed conflict.

The Common Article 3 of the Geneva Conventions of 1949 and the Additional Protocol II to the Geneva Conventions include the norms about non-international armed conflict.[40] The Common Article 3 does not define non-international armed conflict and it refers the conflicts except that international armed conflict with a negative method.[41] The scope of this article is very disputable in the doctrine of international law. The International Criminal Tribunal for the Former Yugoslavia held that "whenever there is … protracted armed violence between governmental authorities and organized armed groups or between such groups within a State"[42]. The Additional Protocol II applies to high intensity armed conflicts between government forces and organized armed non-state actors.[43] The Parties to this conflict must be "under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol"[44]

2.The Concept of Direct Participation in Hostilities and Targeting Hackers

The area of today's wars becomes vague, the actors of these wars get more complicated and civilians are in the middle of the area of these wars. Along with the state armed forces, civilians participate modern war activities and sometimes civilians assist to the combatants as a result of loyalty. In these situations the protection of civilians and the principle of distinction weaken and when a civilian participate in hostility directly, this civilian lose protection and can be a legitimate target. But it is uncertain which act is deemed direct participation in hostilities. This characterization of acts is vital for civilians' lives. Furthermore the distinction of fighters and civilians in non-international armed conflict is important because the status of fighters is relatively continuous although the status of civilians who participate directly in hostilities is temporary.

---

[37] David E. Graham, 'Defining Non-International Armed Conflict: A Historically Difficult Task', (2012) 88 International Law Studies, 44

[38] David E. Graham, op. cit. , 44

[39] The armies of US, China, Iran and Israel formed cyber armed units. As an example see the website of US Army Cyber Command, http://www.arcyber.army.mil/, accessed 3.10.2017

[40] Fatma Taşdemir, Uluslararası Nitelikte Olmayan Silahlı Çatışmalar Hukuku, (Adalet Yayınevi 2009) 10-11, 197

[41] Arne Willy Dahl, Magnus Sandbu, 'The Threshold of Armed Conflict', (2006) 45 Military Law & Law of War Review, 370

[42] ICTY, The Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, prg. 70

[43] Arne Willy Dahl, Magnus Sandbu, op. cit. , 371

[44] The Article 1 of the Additional Protocol II

Determining which person is a civilian is complicated issue. Article 50 of the Additional Protocol I reveals that "a civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A 1), 2), 3) and 6) of the Third Convention and in Article 43 of this Protocol". In Rule 5 of the Customary International Humanitarian Law, a civilian is defined as "persons who are not members of the armed forces"[45]. A civilian enjoys protection against direct attack unless and for such time as he or she takes a direct part in hostilities.[46] This exception reflects customary international law.[47]

According to the Commentary of the Additional Protocol I " 'direct' participation means acts of war which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces"[48]. Acts such as selling weapons to armed groups, expressing sympathy to operations of armed groups are indirect participations in hostilities. But ascertaining the modalities of direct participation is not always easy.

In 2009, the International Committee of the Red Cross published an important study, named the Interpretive Guidance[49], about direct participation in hostilities. It is a result of an expert process under the responsibility of Nils Melzer. The Interpretive Guidance prescribes three criteria about who is deemed a civilian participating directly in hostilities. First criteria is threshold of harm. Accordingly a specific act must affect the military operations or military capacity of a party to an armed conflict or as an alternative way this act must inflict death, injury, or destruction on persons or objects protected against direct attack.[50] As Gary D. Solis puts it:

"Sabotage or other unarmed activities qualify, if they restrict or disturb logistics or communications of an opposing party to the conflict. Clearing mines, guarding captured military personnel, even computer attacks, meet this qualification. Violent acts specifically directed against civilians or civilian objects, such as sniper attacks or the bombardment of civilian residential areas, satisfy this requirement"[51].

In the context of cyber warfare, a civilian who develops a computer program affecting military infrastructure and applies this program participates directly in hostilities and loses the protection.[52] However writing only a program in itself is not a direct participation.[53] Second

[45] Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Humanitarian Law Vol I: Rules, (Cambridge University Press 2009), 17

[46] Article 51(3) of the Additional Protocol I, Article 13(3) of the Additional Protocol II

[47] Ido Kilovaty, op. cit. , 8

[48] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Ed. Claude Pilloud, Yves Sandoz, Christophe Swinarski, Bruno Zimmermann (Martinus Nijjhof Publishers 1987), prg. 1944

[49] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, (ICRC 2009).

[50] Interpretive Guidance, op. cit., 47

[51] Gary D. Solis, The Law of Armed Conflict: International Humanitarian Law in War, (Cambridge University Press 2010), 203

[52] David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) Journal of Conflict & Security Law, 279-297

criteria is direct causation. Interpretive Guidance points out that "there must be a direct causal link between a specific act and the harm"[54]. In pursuant of frequently used example, driving an ammunition truck to actual war zone by a civilian is a direct causal link and moving ammunition from the factory to a port for shipment to conflict zone is not a direct causal link. Last criteria is belligerent nexus. In respect to this criteria an act must be designed to cause harm to other party.

It is necessary to emphasize that the notion of direct participation in hostilities is different from the notion of continuous combat function. The notion of continuous combat function is about the members of organized armed groups. When a person become a member of an organized armed group belonging to non-state party in armed conflict, this person ceases to be a civilian status. A member of an organized armed group constitutes a legal target during membership in an armed conflict. The rule about direct participation in hostilities does not apply to the members of organized armed groups who are in continuous combat function.

The notion of direct participation in hostilities appears in the Tallinn Manual. According to the Tallinn Manual, some cyber acts may form direct participation in hostilities. For example, a cyber-operation disrupting the enemy's command and control is a direct participation[55], but "designing malware and making it openly available online, even if it may be used by someone involved in the conflict to conduct an attack, does not constitute direct participation"[56]. However some cyber acts make a dispute among the International Group of Experts such as to steal funds by using cyber means. Emily Crawford notes:

"In some instances, systems are hacked simply for criminal, malicious, or mischievous reasons, with no nexus to the armed conflict; sites and networks are targeted simply because they can be. In such a case, the appropriate response would lie with domestic law enforcement, rather than under the law of armed conflict"[57].

In addition to all these, Logan Liles points out that unlike the physical world "it is hard to assess the time frame in which a non-State cyber operator actually participates in hostilities"[58] and it is hard to ascertain direct participants in hostilities in cyber space.

Conclusion

The emerging law of cyber warfare has several disputed subjects and more studies on this legal domain must be written. In some ways the law of cyber warfare is an application of international to the unknown because of the non-physical features of cyber space. Finding the

[53] Sean Watts, 'Combatant Status and Computer Network Attack' (2010) 50(2) Virginia Journal of International Law, 429

[54] Interpretive Guidance, op. cit. , 51

[55] Tallinn Manual on the International Law Applicable to Cyber Warfare, 119

[56] Ibid, 120

[57] Emily Crawford, 'Virtual Battlegrounds: Direct Participation in Cyber Warfare' (2013) 9(1) I/S: A Journal of Law and Policy for the Information Society, 17

[58] Logan Liles, 'The Civilian Cyber Battlefield: Non-State Cyber Operators' Status under the Law of Armed Conflict' (2014) 39, North Carolina Journal of International Law and Commercial Regulation, 1114

perpetrators of cyber-attacks, searching the location of cyber organized groups, determining the time of cyber acts are not an easy task. The norms of *jus ad bellum* and *jus in bello* came into existence in compliance with kinetic wars. Yet the fact of cyber warfare as an aspect of "new wars" necessitates the adaptation of international law norms to this new area of application. The clarification of the application of international law to cyber warfare needs more time, events, articles and studies on this subject. Abovementioned arguments on the law of cyber warfare can light the way for future application of international law.

BIBLIOGRAPHY

Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. (Dec. 19)

Arne Willy Dahl, Magnus Sandbu, 'The Threshold of Armed Conflict', (2006) 45 Military Law & Law of War Review

Ashley s. Deeks, ' 'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense', (2012) 52 Virginia Journal of International Law

BBC News, 'Stuxnet 'hit' Iran Nuclear Plans', 22 November 2010, http://www.bbc.co.uk/news/technology-11809827, accessed. 8.9.2017

Caroline Mortimer, 'Junaid Hussain: British-born Isis hacker killed following US drone strike in Syria', Independent, 27 August 2015, http://www.independent.co.uk/news/world/middle-east/british-born-isis-hacker-killed-us-drone-strike-in-syria-kills-junaid-hussain-10474007.html, accessed 29.11.2017

Christine Gray, International Law and the Use of Force, (Oxford University Press 2000)

Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Ed. Claude Pilloud, Yves Sandoz, Christophe Swinarski, Bruno Zimmermann (Martinus Nijjhof Publishers 1987)

Corfu Channel (U.K. v. Alb.), 1949 I.C.J. (Apr. 9)

David A. Sanger, 'Obama Order Step Up Wave of Cyberattacks Against Iran', The New York Times, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, accessed 1.9.2017

David E. Graham, 'Defining Non-International Armed Conflict: A Historically Difficult Task', (2012) 88 International Law Studies

David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) Journal of Conflict & Security Law

Emily Crawford, 'Virtual Battlegrounds: Direct Participation in Cyber Warfare' (2013) 9(1) I/S: A Journal of Law and Policy for the Information Society

Fatma Taşdemir, Uluslararası Nitelikte Olmayan Silahlı Çatışmalar Hukuku, (Adalet Yayınevi 2009)

Gary D. Solis, The Law of Armed Conflict: International Humanitarian Law in War, (Cambridge University Press 2010)

Herfried Münkler, The New Wars, (Polity Press 2005)

ICTY, The Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995

Ido Kilovaty, 'ICRC, NATO And The US-Direct Participation in Hacktivities- Targeting Private Contractors and Civilians Cyberspace Under International Humanitarian Law', (2016) 15(1) Duke Law & Technology Review,

Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Humanitarian Law Vol I: Rules, (Cambridge University Press 2009)

John D. Sutter, "Anonymous declares 'cyberwar' on Israel", CNN, 20 November 2012, http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html, accessed 2.10.2017

John Markoff, 'Before the Gunfire, Cyberattacks', The New York Times, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html, accessed 8.9.2017

Jose Paglieri, 'The Inside Story of the Biggest Hack in History' CNN Tech, http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html, accessed 20.11.2017

Karl Zemanek, 'Armed Attack', (2017) Max Planck Encyclopedia of Public International Law, online edition, Ed.Rüdiger Wolfrum, Oxford University Press

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. (July 9)

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J (July 8)

Legality of Use of Force (Yugo. v. Belg.), 1999 I.C.J. (June 2)

Logan Liles, 'The Civilian Cyber Battlefield: Non-State Cyber Operators' Status under the Law of Armed Conflict' (2014) 39, North Carolina Journal of International Law and Commercial Regulation

Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30(2) Berkeley Journal of International Law

Michael N. Schmitt, ' 'Attack' as a Term of Art in International Law: Cyber Operations Context', (2012) 4th International Conference on Cyber Conflict, NATO CCD COE

Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis', (2014) 25 Stanford Law & Policy Review

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. (June 27)

Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, (ICRC 2009)

Peter W. Singer, Allan Friedman, *Siber Güvenlik ve Siber Savaş*. Translated by Ali Atav. (Buzdağı 2015)

Priyanka R. Dev, 'Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response' (2015) 50(2) Texas International Law Journal

Rebecca Bryant, 'What Kind of Space is Cyberspace' (2001) 5 Minerva: An Internet Journal of Philosophy

Sean Watts, 'Combatant Status and Computer Network Attack' (2010) 50(2) Virginia Journal of International Law

Stanimir A. Alexandrov, Self-Defense Against the Use of Force in International Law, (Kluwer Law International 1996)

Stephen Herzog, 'Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4(2) Journal of Strategic Security

Tallinn Manual on the International Law Applicable to Cyber Warfare, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf, accessed 4. 11. 2017

Terence Check, 'Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict, NATO-Centric Approach', (2015) 63 Cleveland State Law Review

United Nations Charter (1945), https://treaties.un.org/doc/publication/ctc/uncharter.pdf, accessed 23.11.2017

US Army Cyber Command, http://www.arcyber.army.mil/, accessed 3.10.2017

Yoram Dinstein, War, Aggression And Self-Defence, (Grotius Publications Limited 1988)

Zakaria Dabone, 'International Law: Armed Group in a State-centric System' (2011) 93(882) International Review of the Red Cross