ISSN 2424-6050 (Online) ISSN 1392-1274 (Print). TEISĖ 2018 107
DOI: https://doi.org/10.15388/Teise.2018.107.11824

THE VIRTUAL TROJAN HORSE IN MODERN CONFLICTS

Alaa Al-Aridi
Master degree in law from Vilnius University
Currently a PhD candidate, Public Law Department at Vilnius University
Sauletekio ave. 9, LT- LT-10222 Vilnius, Lithuania
Email: <alaa_g_aridi@hotmail.co.uk>

Straipsnyje nagrinėjamas tarptautinės teisės taikymas kibernetiniams veiksmams. Daugiausia dėmesio skiriama kibernetinėms atakoms, kurias reguliuoja jus ad bellum, *teisės šaka, nustatanti jėgos panaudojimą kibernetiniame lauke; analizuojamas Jungtinių Tautų pagrindinių teisių chartijos 2 straipsnio 4 dalies taikymas, taip pat teisė į savigyną, nustatyta šios chartijos 51 straipsnyje. Be to, aptariami tarptautinės humanitarinės teisės principai* (jus in bello), *taikomi kibernetinėms operacijoms ginkluotų konfliktų metu.*

The article will examine the applicability of international laws to cyber affairs by focusing on cyber-attacks that fall under the jus ad bellum the law relating resort to the use of force in the cyber field; and analyzing the applicability of article 2/4 of the UN charter as well the right to self-defense articulated in article 51 of the UN charter; on the other hand will analyze how the legal parameters of IHL (jus in bello) apply to cyber operations in armed conflicts.

Introduction

Following up the shift in warfare from conventional to modern ones, new technologies have been highly invested in conflicts such as cyber-attacks, accompanied by the change of conflict actors that is no more limited to dual state conflicts but as well an explicit involvement of non-state armed groups, terrorist groups, proxy fighters sponsored or solely motivated. The majority of political and military conflicts have cyber dimensions with variety of cyber strategies and tactics, both states and non-state actors enjoy fruitful investment in cyber tactics resulting to the manipulation of critical infrastructure in many cases. Several examples of cyber or virtual operations/attacks have been waged since 1990s, such as the Black Hand group that held attacks against the NATO's internet infrastructure at 1999 as a response to the military operations in Serbia[1], the Pakistani Hackerz Club that targeted the pro-Israeli lobby AIPAC at USA as a response to the conflict in Palestine[2]. Furthermore, in April 2001 USA has been targeted by China[3], then the cyber-attack that targeted Estonia in 2007[4] and resulted a

[1] Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer. *Bosnian Serb News Agency SRNA*, March 28, 1999 (BBC Monitoring Service, March 30, 1999).

[2] Israel Lobby Group Hacked. *BBC News*, 3 November 2000, <http://news.bbc.co.uk/2/hi/middle_east/1005850.stm>.

[3] WAGSTAFF, J. The Internet could be the Site of the Next China-U.S. Standoff. *The Wall Street Journal*, April 30, 2001.

[4] Such Attacks requires request from more than a million computer based in over 100 countries hijacked and linked through the use of Botnets that flooded governmental and private websites and caused servers to crash in Estonia. ROSCINI, M. World Wide Warfare – Jus ad bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations law*, 2010, Vol. 14 , p. 94.

highly diplomatic interest due to the possible reinterpretation of article 5 of the NATO[5], STUXNET that targeted the Iranian nuclear centrifuges, and recently in May 2017 Ransomware cyber-attack that affected thousands of civilians infrastructure in more than hundred nations[6]. In a globally interconnected network any attack might be a threat to a state or the international security if it reaches a level of intensity. And despite all the danger cyber-attacks impose to the international peace and security yet clear international legal analysis is still lacking.

Cyber warfare and Cyber-attack lacks clarity in the terms they are used for, a cyber-attack might lead to an armed conflict and might not. According to Tallinn manual, Cyber operations are the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace[7], defining such attacks as: "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[8]. Cyberwarfare has been defined in a broad way by some scholars ,for example Joseph Nye in 2015 includes in his definition all forms of electronic crimes and sabotage through DoS (denial of service) attacks[9] , however a narrow definition and more restrictive should be considered such as the Tallinn Manual in the definition mentioned before, but such definition should focus on the attacks that target critical infrastructure and that it must be made by state actors or proxies that are with no doubts sponsored and financed by a state. On the other hand, Michael Schmitt views on cyber operations and the Tallinn manual was one of the first scholars investigating cyber operations and came out with the Schmitt criteria[10] by which for cyber-attacks to qualify as armed force that it must fit into the traditional consequences and based frame provides a fruitful basis for analyzing jus ad bellum in the context of cyber-attacks , however considering the physical damage criteria, attacks targeting critical national infrastructure that aim deliberately to destroy or damage objects of strategic values of another state must be dealt with in expansionist way to be considered as armed force even with no physical damage.

The objective of this article is to examine the applicability of international laws to cyber affairs by focusing on cyber-attacks that fall under the jus ad bellum; the law relating resort to the use of force in the cyber field by analyzing article 2/4 and article 51 of the UN charter, as what would be considered a use of force or armed attack triggering article 51 of self-defense in cyber realm, that involves at the same time the principles of necessity and proportionality, then identifying the challenges of applying these laws to cyber-attacks such as state responsibility; and on the other hand will analyze how the legal parameters of IHL (jus in bello) apply to cyber operations in armed conflicts, by analyzing the role of IHL in governing cyber-attacks in armed conflicts, the role of non-state actors and how would the principles of LOAC be respected in cyber operations? The article will conclude if new laws need to be drafted or extension of their analogy in this area is enough? especially that although international law applies to cyber space but some of the main features of cyber operations can create a problem in practice such as attribution, state responsibility and the intensity threshold of an armed attack in cyber paradigm. Pointing that, will exclude the cyber-crimes such as espionage or IP theft, as well as

---

[5] GEERS, K. Cyberspace and the Changing Nature of Warfare. *Cooperative Cyber Defense Center of Excellence*, <www.scmagazine.com>.

[6] Cyber-attack: Europol says it was unprecedented in scale (13 May 2017). *BBC News*. <http://www.bbc.com/news/world-europe-39907965>.

[7] SCHMITT, M. Tallinn Manual on the International Law applicable to Cyber Warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013, p. 258.

[8] SCHMITT, M. Tallinn Manual <...>, Rule 30.

[9] NYE, Joseph S. International Norms in cyberspace. *Project syndicate*, 11 May 2015.

[10] SCHMITT, M. Cyber operations and the Jus ad bellum revised. *Villanova Law Review*, 2011, Vol. 56, pp. 576 et seq.

cyber-terrorism, but the main focus will be only on jus ad bellum and jus in bello. This article as well will explore existing literature on the legality of cyber-attacks, such as Tallinn Manual by exposing and exploring key issues related to adequacy of the legal framework envisaged by it, in addition to publications of scholars and experts in this area.

The principles of international law from positivism perspective stems from international conventions, customary law and general principles of law as mentioned before. Therefore an analysis of relevant legal rules and role of state practices in relation to these rules will be implemented. Main focus on the challenges cyber-attacks impose to the legality of use of force and self-defense in the framework of UN charter alongside with ICJ judgments that illustrates the state responsibility and attribution in cyber realm.

The article will be analyzing this emerging area of law by being involved in studying primary sources and recognized sources of international law such as treaties, customary international law, general principles of law , judicial decisions and legal doctrine[11] especially the UN charter, Geneva conventions I- IV and its protocols I and II that govern armed conflicts both international and non-international, in addition soft law and secondary literature in the theoretical dimensions of the research project by qualitative means as cyberwarfare is not subject to specific regulation. Case law in ICJ plays an important role in providing comprehensive approach to the use of force and self-defense in particular Nicaragua v. USA, Uganda v. DRC cases. This paper will use the legal dogmatic method to analyze the established sources of international law to respond to the complex challenges of such forms, especially when dealing with the uncertainties of the applicability of jus ad bellum and IHL to cyber operations in armed conflicts.

Jus ad Bellum and Cyber operations

The primary treaty of jus ad bellum is the United Nations Charter, which forbids all parties from the use of force in international relations in accordance to article 2(4) of the UN Charter stating that any state-sponsored cyber operations qualifying as a use of force against another state would fall under general prohibition of this article. While cyber operation that didn't reach to the limit of use of force are as well prohibited by customary principle of non-intervention and represents lawful countermeasures in response to internationally wrongful acts. Injured states by cyber operations amounting to level of an armed attack permit it to use its right to self-defense through means prohibited generally by the charter (the resort to force). Moreover, cyber operations that threaten international peace and security or any acts of aggression allow the Security Council to take feasible measures. Theoretically might be clear but in practice such operations can be confusing to law based on the unique features of cyber-attacks.

One of the implications is state responsibility that covers the legal consequences of a state's violation of international law which is considered a body of customary international law is when states are responsible for their internationally wrongful acts to other states they have injured. Law obliges a targeting state to immediately cease the offending conduct, or comply with required duty and make full reparation[12]. Moreover, a state to which the cyber operation of non-state actors is attributable is legally required to do all possible means to stop them[13]. Otherwise, counteracts from the victim state will be taken, and will be considered legal as long as they comply with the various measures set forth for countermeasures in the law of state responsibility[14].

---

[11] Article 38 (1), statute of the International Court of Justice (ICJ).

[12] Draft articles on Responsibility of States for Internationally Wrongful Acts, Year Book of International Law Commission, Volume II, Part II , United Nations Geneva 2001, Chapter II Article 34, p.95

[13] SCHMITT, M.; VIHUL, L. Proxy wars in Cyberspace: The Evolving International Law of Attribution. *Fletcher Security Review*, Vol I, Issue II, Spring 2014, p. 58.

[14] Draft articles on Responsibility of States for Internationally Wrongful Acts, Ibid, Article 49–54 , p. 129–139.

The question that arises from that is: to what extent cyber operation can qualify as force within the meaning of this prohibition? Especially with the absence of a treaty definition and any clear interpretation to the concept of "Force". The term force in this article doesn't limit use of force to kinetic, chemical, biological or nuclear weaponry, According to the ICJ in its advisory opinion concerning the legality of the threat or use of nuclear weapons 1996, the prohibition applies to any use of force regardless of the weapons employed[15]. This would certainly include cyber operations that cause death or injury to person or damage, destruction of infrastructure. For example, cyber operations target computer systems causing a meltdown in a nuclear power station, or opening the floodgates of a dam above a densely populated area, or disabling a busy airport's air traffic control during bad weather conditions, each with potentially horrendous consequences in terms of death, injury and destruction[16]. This elaborates that there won't be any specified list of cyber-attacks to be considered as armed attacks and that will be left to the case itself by the On the spot state practices, interpretation of the courts, as well the circumstances accompanied by the motivation behind the use of force. Moreover, attacks made by conventional or cyber means must be treated equally, as the means of wars been developed and states using that advantage to destabilize orders. But the means of response will be an issue to the case itself, by self-defense or other means of response. As a result, the paper hints that this gap between article 51 and article 2 (4) requires that the state to which has been the victim of use of force that does not constitute an armed attack, is limited to non-forcible countermeasures or non-forceful actions unless the security council has given authorization to do so[17], however state practices proved otherwise and this will be elaborated later in this paper.

Difficulty of attribution is a main challenge for nations in reducing the overall insecurity coming from cyber space and addressing identifiable actors, which leads to legal difficulties when it comes to the respond by the victim state to such acts. Same is the misattribution or what is so called false flag, which can be used as a propaganda or deceptive tactic. In international law, acts will be attributed to a state if they are performed by persons or entities acting on behalf of a state or under its command, while others who are not acting this way cannot be regarded as state agents, yet can be described as non-state actors. International law dictates that a state may not "allow knowingly its territory to be used for acts contrary to the rights of other states," and this applies to cyber infrastructure[18]. According to the individual attribution to a state, it must be determined based on the international law of state responsibility which is regulated by the draft articles on responsibility of states for internationally wrongful acts 2001. In this matter some state agents carrying such attacks can be not only government agents "de jury" that constitutes attribution to a state, but can as well be private contractors "de Facto agent"[19] such as non-state groups[20]. Nothing in article 2(4) prohibits directly non-state actors from the use of cyber operations which may be relevant according to IHL and international criminal law. However, any support and sponsoring of state to group's activities that amount indirectly to a use of force is considered a violation to article 2(4) and the principle of non-intervention. Therefore, the attribution of a non-state actor to a state will make it responsible internationally based on such assistance. This was noticed by ICJ in the Nicaragua case, in which it ultimately concluded that the

---

[15] International Court of Justice ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, p 39; see also BROWNLIE, I. *International Law and the Use of Force by States*. Clarendon Press Oxford, 1963, pp. 362-431.

[16] MELZER, N. Cyber Warfare and International Law. UNIDIR Resources 2011, p. 7.

[17] *Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. National Research Council, The National Academic Press, Washington D.C. 2010, p. 163.

[18] SCHMITT, M. Tallinn Manual <...>, Rule 5 and its commentary.

[19] MELZER, N. Cyber Warfare <...>, p. 10.

[20] MILANOVIC, M. State Responsibility for Genocide. *European Journal of International Law*, 2006, p. 576–577.

relations between the U.S and the contra rebels did not qualify as de facto agency, but that the U.S conduct under review constituted "indirect use of force"[21]. In this context, the attribution of non-state actors to a state is conducted when such actors are acting under the supervision or control of a state[22]. All in all, two main standards can be analyzed with the state sponsorship of aggression under article 8 of the International Law Commission Drafts Articles on the responsibility of states for internationally wrongful acts[23], first is the effective control that applies directly to non-state actors by which according to the ICJ in Nicaragua case the only instance in which states sponsors of cyber-attacks would be if their effective control by its state is beyond any doubt[24]. Second is more restrictive and mentioned by the ICJ in Tadic Case which is the overall control standard that goes beyond the mere financing of such forces but also involving in participation for planning and supervision of military operations[25], but it was not approved by the majority of the states as the Effective control standard. The ICJ in Nicaragua case intimated the requirement of clear evidence in the case of attribution of a non-state group's act to a state[26]. As such clarity is not equated and absolute, certainty or elimination of all possible alternatives is not required[27].

In the cyber context, countermeasures often represent an effective means of self-support by allowing the injured state to take urgent action that would otherwise be unavailable to it, such as "hacking back," in order to compel the responsible state to cease its internationally wrongful cyber operations. But according to article 41 of UN Charter, not any threat or use of force prohibited by article 2(4) automatically constitutes an armed attack justifying self-defense action according to the article 51[28]. This explanation was confirmed by customary international law in ICJ stating that it was necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms[29], as well reassured by the case of Oil Platform by the ICJ[30]. It is though hard to distinguish between use of force and armed attack which creates a gap in between article 2(4) and article 51 of the UN Charter, especially that all armed attacks are use of force, but not all uses of force amount to an armed attack[31].Such gap was asserted by the ICJ in Nicaragua case as mentioned before. Even if such gap exist yet the bar is set relatively low by which limited actions don't fall outside article 51, and state practice reassured that in several cases where self-defense been conducted against actions that didn't qualify as an armed attack[32].According to the ICJ in the armed activities

---

[21] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). *International Court of Justice (ICJ), Reports 1986*, p. 115, 205, 247.

[22] Articles on State Responsibility, *Ibid*, Chapter II. paras. 2–3.

[23] Draft articles on Responsibility of States for Internationally Wrongful Acts, *Ibid*, p.47.

[24] SHACKELFORD, S. *State Responsibility for Cyber Attacks: Competing Standards for a growing problem*. University of Cambridge, 2010, p. 204-205.

[25] Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A. *International Criminal Tribunal for the former Yugoslavia (ICTY)*, 15 July 1999, p. 62 , para 145.

[26] The International Court of Justice recognized this basis in the Tehran Hostages case. There, the Court found that Iran bore responsibility for holding US hostages between 1979 and 1981 because "the approval given to [the seizure] by the *Ayatollah Khomeini* and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State.", see Nicaragua v. United States of America, ICJ. 1986, para. 109.

[27] SCHMITT, M.; VIHUL, L. Proxy wars <...>, p. 66.

[28] RANDELZHOFER, A. "Article 51 UN Charter", in Bruno Simma (ed.), The Charter of the United Nations: A Commentary, vol. I, 2002, p. 790 .

[29] Nicaragua v. United States of America <...>, p. 191.

[30] Case Concerning Oil Platforms , Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), 6 November 2003, p. 51.

[31] DINSTEIN, Y. Computer Network Attacks and Self-Defens. *International Law Studies*, U.S. Naval War College 2002, p. 163.

[32] Hfarn Steiner, Cyber Operations, Legal Rules and State Practice. Stockholm University, Spring 2017, p. 33.

case: DRC vs Uganda (use of force and non-state actors), Uganda didn't not demonstrate that it had been subjected to armed attack by the DRC and attribution of ADF to the DRC had no satisfactory proof which conversely gave the right of self-defense against Uganda[33]. Moreover, ICJ considered that article 51 didn't permit states to use force to protect perceived security interests beyond the parameters explicitly provided, where other means available is recourse to the Security Council[34], as well Uganda didn't report to USC that it had regarded as requiring it to act in self-defense in respect to article 51 of the UN charter. Important to note that, the traditional customary law governing self-defense by a state derives from an early diplomatic incident between the USA and the UK over the killing of a number of US citizens engaged in transporting men and materials from American territory to support rebels in what was then the British colony of Canada.[35]

The public case Stuxnet is one of the examples that could equate to a kind of use of force that would entitle the state to use force in self-defense. An operation carried out against the Iranian nuclear centrifuges that led to property destruction, such attack caused loss of view (LOV) and loss of control (LOC) showing false data about centrifuges. This incident was first cyber weapons used by one state against a national critical infrastructure, Reportedly Iranian did respond not in armed force but in cyber realm. If such attack occurred in USA it would be considered an armed attack, as the US position is that any use of force triggers self-defense, while in the rest of the world there is gap between the use of force in article 2/4 and the armed attack that triggers self-defense. In this matter, in the US pentagon's attempt to reconcile what constitutes an act of war with international legal standards, it explained that a cyberattack that meets the threshold of an act of war would include a "significant loss of life, injury, destruction of critical infrastructure, or serious economic impact"[36]. In this regards, the prohibition of use of force under artcile2/4 must evolve to cover malicious use of cyber instruments causing destructive effects on state's critical infrastructure and an expansionist view can be adopted to consider cyber-attacks even with no physical outcomes that targets such infrastructures to be considered armed attacks.

However, article 51 of the UN Charter reflects the customary right of self-defense[37], which recognizes the customary international law. The UN Charter doesn't explicitly define what article 51 covers and especially in the context of armed attack and its inherent right, as this article is an exception to article 2(4) that prohibits the use of force. Therefore, a state can use force without violating article 2(4) when it is victim of an armed attack which doesn't require any authorization from Security Council and limited to states. In this matter Tallinn Manual in rule 5 stated that cyber infrastructure control is a standard that must be taken into account in the attribution issue. States are prohibited from allowing the usage of its cyber infrastructure on its territory; land, sea or airspace; as adversely or unlawfully affects other states[38]. Such responsibility is a violation of international law according to rule 6 of the manual which is of customary nature and reflected in the international law commission articles on state responsibility.

The ICJ in Nicaragua case stated that the definition of an armed attack must be interpreted with guidance from the Definition of Aggression as a basis for determining what may constitute the threat or use of force and armed attacks[39], and in order for the use of force in self-defense to be considered

---

[33] Case concerning Armed Activities on the Territory of the Congo , DRC v. Uganda, ICJ 2005, para 304.

[34] *Ibid*, para 109.

[35] CLAPHAM, A. Brierly's Law of Nations, Oxford University Press, Oxford, 2008, 7th edition, pp. 468–469.

[36] ADAMS, M. J.; REISS, M. How should International Law treat Cyberattacks like WannaCry? *LawFare blog*, 22 December 2017.

[37] SCHMITT, M. Tallinn Manual <...>, Rule 13, p. 54.

[38] *Ibid*, Rule 5.

[39] United Nations General Assembly Resolution 3314 (XXIX) Definition of Aggression, United Nations, Geneva 1974, Article 3 para. A-G.

legal, the state acting in self-defense must have been the victim of an armed attack, declared itself to have been so attacked[40], and requested the assistance of the states which comes to its aid[41]. According to the Tallinn Manual, the international group of experts did agree upon some indications which can be used when separating lesser grave forms of use of force from the gravest forms. However, the incidents where use of force lead to the death of human beings or destruction or damage to property would in scale and effect constitute an armed attack[42], that was reconfirmed by Y. Dinstein through his conclusion that illegal use of force will amount to an armed attack whenever it causes the death of human beings or results in serious destruction of property[43].

Moreover, the reaction as a self-defense against cyber-attacks must meet the requirements of necessity in which the use of force is the last resort after failure of available means[44] and such act that must occur within a timely manner should be essential for the protection of the state's security and interest[45]. Second requirement is proportionality, that requires balancing the response against its objective of ending the attack[46], and this principle may permit the use of traditional force against the cyber-attack, for example bombing the attacking computer that launched the cyber operation[47]. Finally, the victim state must prove attribution to the state which they launch their counter attacks against. In other words, any cyber-attack attributed to a state held by de jury or de facto actors triggers a state responsibility that requires countermeasures as self-defense or even further steps by the Security Council as a threat to peace and security (Chapter VII) UN Charter, according to principle of non-intervention which is derived from a fundamental principle of international law, that is sovereignty[48] .

However, as new technology creating a challenge to international law, it is important to spot the light with the development of norms on the long term that can come out by states' practices and what the law requires and that will qualify as a law through customary practices. In this matter the norm might be developing in a way that cyber incidents should be responded to by cyber means (Stuxnet Iranians responded by cyber means, Sony incidents in which USA hacked back in Korea, DNC hack by which USA responded in cyber means against Russia). Even though laws allow states to respond by kinetic means, however state practice is shifting towards cyber responses for strategic or political agendas.

Jus in Bello and Cyber operations

Jus in Bello or the Law of Armed Conflicts (LOAC) is the law that applies in armed hostilities, such law is concerned in the protection of non-combatants as well the behavior of states and combatants in an armed conflict or occupation[49], so it no longer concern the legitimacy of use of force or jus ad bellum.

Although, international humanitarian law (IHL) doesn't explicitly mention cyber operations in its rules, yet doesn't mean that such operations are not subject to IHL, and that is discussed in

---

[40] *Ibid*, para 196.

[41] *Ibid*, para 195–199 and 232–233.

[42] SCHMITT, M., Tallinn Manual <...>, p. 54–55.

[43] DINSTEIN, Y. Computer Network <...>, p. 100.

[44] ROSCINI M., World Wide Warfare- Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14 , Netherlands 2010 , p. 119.

[45] Nicaragua v. United States of America <...>, p. 194.

[46] BARNETT, S. Applying Jus Ad bellum in Cyberspace. University of Toronto, 2016, p. 7.

[47] DINNISS, H. Cyber Warfare and the Laws of War. Cambridge University Press, 2012, p. 104.

[48] SCHMITT, M. Tallinn Manual <...>, Rule 1.

[49] The threshold applicable to international and non-international armed conflicts can be noticed by common article 2 and 3 of the Geneva Conventions.

article 36 of the additional protocol I 1977, but still one of the problems IHL face in cyber realm is the anonymity of the actors in contemporary conflicts especially that IHL was created to govern conventional warfare, but in the same manner the group of experts at Tallinn Manual agreed that IHL is able to govern cyber warfare[50]. For e.g. some isolated acts such as STUXNET attack launched by several states against the Islamic Republic of Iran targeting the uranium facilities has not been conducted in an ongoing armed conflict ,however if attribution was clear then an international armed conflict (IAC) would have occurred[51]. In this matter, IHL didn't define clearly the IAC, where such conflict is derived from the common article 2 of the Geneva conventions 1949. The convention and its additional protocol I apply to IACs, such armed conflict requires opposition of high contracting parties (Member States), in other meaning a conflict between the legal armed forces of two different states, even if one party of the conflict doesn't recognize the government of the adverse party or no formal declaration of war noticed[52], and it makes no difference how long the conflict lasts or how much slaughter takes place[53].Moreover, according to the ICRC, neither the duration nor the intensity plays a role in blocking the applicability of IHL to such conflicts[54].It is important to bear in mind that armed conflicts can arise when a state use unilateral forces against another state even if the latter doesn't or cannot respond with military means[55]. In the same manner IAC can arise with any attack by a state against territory, infrastructure or persons in the other state triggering by that the applicability of IHL if it was considered an armed attack, though to date it have not witnessed that. In cyber-attacks, the applicability of IHL cannot be limited to acts committed by members of the state armed forces but must be extended to the conduct of any other person acting as a state agent, whether de jure or de facto, on behalf of a belligerent. Accordingly, state-sponsored cyber operations would give rise to an IAC if they are designed to harm another state not only by directly causing death, injury or destruction, but also by directly and adversely affecting its military operations or military capacity[56]

On the other hand, Internal Armed conflicts or Non-International Armed Conflicts (NIAC) is mainly the use of force within the boundary of one state, with the involvement of one or more armed groups and the government forces, or between those armed groups. According to Bert Roling, the laws of war derive their authority during a war from the threat of reprisals, prosecution and punishment after the war[57]. With regards to the applicability of IHL treaty to NIAC, two main legal sources govern such armed conflict, Common Article 3 of the Geneva conventions and article 1 of the additional protocol II. The common article 3 of the Geneva Conventions 1949, defined NIAC as an armed conflict occurring in one of the high contracting parties. NIAC must reach level of confrontation that requires two criteria according to the ICTY in the Tadic case: First, the hostilities must reach a minimum level of intensity[58], and secondly non-governmental groups involved in the conflict must be considered as „parties to the conflict", meaning that they possess organized armed forces[59].

---

[50] SCHMITT, M., The Law of Cyber Warfare: Quo Vadis? *Stanford Law and Policy Review*, 2014, p. 2–3.

[51] SCHMITT, M. Classification of Cyber conflict. *Journal of Conflict and Security Law*, Vol. 17, Oxford university Press 2012, p. 252.

[52] Geneva Conventions (I, IV) 1949, Application of the convention, Ch. 1, Common Article 2.

[53] PICTET, J. Commentary to the third Geneva Convention, ICRC, Geneva 1960, p. 23.

[54] PICTET, J. ICRC commentary to Article 2 of the First Geneva Convention, Geneva 1952, p. 23 , See also SANDOZ, Y. the ICRC Commentary to Article 1 of Additional Protocol I , Geneva 1987.

[55] ICRC, 32nd International Conference of the Red Cross and Red Crescent, Ibid. p. 8

56 MELZER, N. Cyber Warfare <...>, p. 23–24.

[57] ROLING, Bert. Criminal Responsibilities for Violations of the Law of War , Belgian Review of International Law, 1976, p. 10.

[58] The Prosecutor v. Fatmir Limaj, Judgment, IT-03- 66-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 30 November 2005, para. 135–170.

[59] *Ibid*., para. 94–134.

In the cyber paradigm Rule 23(2) of the Tallinn Manual stated that the application of IHL doesn't depend on specific means and covers the cyber operation even with the absence of kinetic methods triggering a NIAC[75], but that will depend on the threshold of violence and degree of the organization of armed groups. In this matter as discussed before, the violence to be qualified as an non-international armed conflict must be protracted, which means that the qualifying violence need not be continuous in nature, and that what the ICTY in Limaj case confirmed[60]. Important to keep in mind that such groups must be with an organized structure, but in the virtually organized groups command and the members are not easily recognized, the majority of the group of experts in Tallinn Manual stated that the failure of members of the group to physically meet, doesn't alone preclude it from having the requisite degree of organization. In this regards, the informal grouping of individuals working as collectively virtual attackers not in coordination, the majority of experts agreed that the mere fact that individuals are acting toward a collective goal doesn't satisfy the organization criterion[61]. This opens the gate to the importance of the attribution and state relation to those groups, so in my opinion such issue is left to opinio juris and state practice.

Attribution in cyberspace in the context of IHL looms with respect to whether a state support creates an armed conflict, serves a transformative or initiating function with respect to the conflict itself[62]. Moreover, it requires identifiable states as parties to the conflict and this is the issue of attribution. In other words, support of a non-state armed group might trigger an IAC, or internationalize an ongoing NIAC[63].In this matter, all the infrastructure of the supporting state as well its citizens that are participating directly in hostilities will be legitimate targets from the other state[64], that was supported by rule 38 of the Tallinn manual concerning the civilian objects and military objectives[65]. So if the state's sponsored de jure or de facto actors targeted another state, then the state will be responsible depending on the relation of the state with the organized or unorganized armed group, which is different from the law of state responsibility and the effective control standard. The Tallinn Manual takes a similar legal view in rule 7: 'The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation'.

In this Matter, and according to the *TADIC* case, ICTY stated that:" the mere financing and equipping of such forces was insufficient, whereas participation in the planning and supervision of military operations qualified[66]. As well, the ICC in its judgement at the *LUBANGA* case found that: "a role in organizing, coordinating, or planning the military actions of a non-state armed group in another state, internationalizes and NIAC[67]". Therefore, the main requirement of attribution in cyberspace in accordance to IAC or NIAC is the over-all control standard. And in all cases, as IHL applies to an ongoing armed conflict, any cyber during this conflict will be governed by the IHL rules.

However, a cyber-attack from a small group of hackers organized and under command against the governmental military forces for example, will trigger a NIAC as long as it fits with the requirements.

---

[60] *Ibid*., para.168,171/3.

[61] SCHMITT, M. Tallinn Manual <...>, p. 90, para 15.

[62] SCHMITT, M.; VIHUL, L. Proxy wars <...>, p.70.

[63] *Ibid.*, p. 71.

[64] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, United Nation Treaty Series, June 8, 1977, arts. 51, 52.; see also. HENCKAERTS, J-M.; DOSWALD-BECK, L. *Customary International Humanitarian Law*: Cambridge University Press, New York, 2005, Rules 1-6-7.

[65] SCHMITT, M. Tallinn Manual <...>, Rule 38, p. 125–133.

[66] Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, (ICTY), July 15, 1999, para. 145.

[67] Prosecutor v. Lubanga, Decision on Confirmation of Charges, International Criminal Court (ICC) January 29, 2007, para. 211.

But yet it might not if the intensity is not high or not protracted which could be considered a criminal threat dealt with by the law enforcement. While the ICRC's contribution to the 2004 Stockholm Conference stated, "Whether cyber network attack alone will ever be seen as amounting to an armed conflict will probably be determined in a definite manner only through future state practice"[68]. In all cases, IHL applies to NIACs but what are the cyber operations that amount to an armed conflict? It is the question of threshold which showed that Tallinn Manual was able somehow to explain the limit of threshold.

There is no reason why cyber operations cannot have the same violent consequences as kinetic operations, for instance if they were used to open the floodgates of dams or to cause aircraft or train to collide. In such circumstances, and if such violence is not merely sporadic, it may meet the threshold for a non-international armed conflict according to such intensity of hostile[69]. The ICJ in its advisory opinion about the legality of threat or use of nuclear weapons, invoked the martens clause in the preamble to the Hague convention IV of 1907, which stated that: "Even in cases not explicitly covered by specific agreements, Civilians and combatants remain under the protection and authority of principles of international law derived from the established custom principles of humanity and from the dictates of public conscience."[70]. Such statement is found as well in article 1 of the additional protocol I of 1977. Therefore, IHL extends to the sphere of cyber operations in armed conflicts. Moreover, Article 36 of the additional Protocol I to the Geneva Conventions provides that: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

The term attack refers to a particular type of military operation during an armed conflict to which particular IHL norms apply; therefore it must not be confused with jus ad bellum notion[71]. Hereby, it is important to keep in mind that IHL requires several principles in its role of protecting civilians, and those principles are derived from the military necessity as a legal notion used in IHL to consider a cyber-attack lawful but the article considers that necessity in Jus in bello when it comes to cyber paradigm doesn't create any novel challenge. As well distinction by obliging parties of armed conflict to distinguish at all times and under all circumstances between combatants and military objectives on the one hand and civilian objects on the other hand by only targeting the former, Such right is lost in case civilians took part of hostilities or been acting in continuous combat function that makes them lawful targets in a combat[72]. This principle was first set forth in the St. Petersburg declaration, stating that: "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy", rule 31 of Tallinn Manual applies this rule as well in accordance to article 48 of the add. protocol I[73]. According to the Kassem case in 1969, Israel's military court at Ramallah case recognized the immunity of civilians from direct attack as one of the basic rules of IHL[74].

---

[68] DORMANN, K. The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint, ICRC 2001, see also. BOYSTOM, K. International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law. Swedish National Defense College, Stockholm 2004, p. 142.

[69] DROEGE, C. Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. ICRC Geneva, 2012, p. 552.

[70] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, paras. 74–87.

[71] SCHMITT, M. "Attack" as a Term of Art in International Law: The Cyber Operations Context, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2012 p. 285–286.

[72] Additional Protocol to the Geneva Conventions of 12 August 1949 And Relating to the Protection of Victims of International Armed Conflicts (Protocol I), United Nation Treaty Series 1979, Articles 48, 51–53, 57.

[73] SCHMITT, M. Tallinn Manual <...>, p. 110.

[74] ICRC, Customary IHL, Israel "Practice relating to Rule 106". Conditions for Prisoner of War Status, Section A, Chapter III.

In this matter, article 51(4) of additional protocol I classifies indiscriminate attacks that are prohibited, and belligerents should always be capable of discriminating between combatants and civilians as well their objects, thus such principle is very complex in cyberspace, even if attacks targeted military only but the consequences of such attacks will nevertheless spread over unintended objects, civilian ones or those who are not engaged in hostilities. For e.g. uncontrolled viruses, that might spread to civilian property causing collision between aircrafts, release of radiation or toxins from nuclear or chemical plants. Only those cyber operations and attacks are subject to the principles of distinction, proportionality, and precaution[75]. Cyber operations might constitute attack in the meaning of IHL not only by causing death, injury or physical destruction or damage, but also any interference with the functioning of an object by disrupting the underlying computer system. According to Tallinn manual, the circumstances under which the internet in its entirety could be attacked are so highly unlikely as to render the possibility purely theoretical at the present time. Instead, the international group of experts agreed that, as a legal and practical matter, virtually any attack against the Internet would have to be limited to certain discrete segments thereof[76]. Most important in the distinction requirement is the military objectives that in my opinion needed to be narrowed to reduce the complexity of distinction vis a vis cyber sphere. While the principle of proportionality is articulated in article 51(5)(b) of the AP I that prohibits the attack that cause incidental loss of civilian life, injury to civilians, damage to civilian objects or combination which would be excessive in relation to the concrete and direct military advantage anticipated[77]. It is right to argue that foreseeable damages even if they need time to occur, must be taken into account in this principle[78], even though it is more complex to be examined as in kinetic conventional attacks, but yet it should not be excluded as it involves important principle in IHL. In addition, attacks that comes from neutral states causes confusion to the injured state especially that the state from which the attacks were launched may not be responsible, unable or unwilling to block the attacks from its territory, this brings us back to the attribution and state responsibility discussed in previous chapter. Such issue can be solved by stronger national cyber security strategies to control cyber activities within the borders of states with the involvement of other legal frameworks that fill in this gap, but unfortunately law is not the only answer but that also require economic and technological abilities that are not available in less developed countries.

Conclusion

This paper concludes that international law is capable of regulating the cyber operations theoretically but broadly as legal status of cyber-attacks and appropriate responses are not clear. There is no official definition of cyber warfare in international law and not explicit by any major international treaty. Moreover, no rulings dealing directly with cyber warfare however existing laws are extended to cyber domain. Scholars' definitions vary and some of them are with broad terms, therefore a clear legal definition of cyber-attacks with a narrower and restrictive approach is a must. As some experts proposed amendments to the treaty provisions applied to cyber warfare, however such nor amendments are not easily achieved internationally neither a new international accord dealing specifically with cyber-attacks. But best proposal meanwhile would be updating or amending existing law to use new definitions that includes cyber-attacks between nation states based on the principle of International law. First step can be with bilateral or regional treaties.

---

[75] SCHMITT, Michael. Cyber Operations and The *Jus in Bello*: Key Issues. *Naval War College International Law Studies*, Vol. 87, 2011, p. 91.

[76] SCHMITT, M. Tallinn Manual <...>, Commentary on Rule 39, para 5.

[77] *Study on Customary International Humanitarian Law*, ICRC, note 87, Rule 14.

[78] SCHMITT, M. Tallinn Manual <...>, Commentary on Rule 51, para. 6.

The paper examined state responsibility in cyber operations and challenges that arise in practice due to the unique characteristic of cyber operations and the role of actors especially when it comes to non-state armed groups that can afford states a degree of anonymity and detachment from the non-state operations that serve useful political and legal ends. The paper showed that attribution is not easy task to confirm the state responsibility to such acts as well the right to trigger self-defense when attribution is not clear, but concluded that an effective control by state in cyber operations conducted by groups is beyond doubt of attribution. All in all, an articulation of binding and narrow domestic and international rules that would draw the line between lawful and unlawful actions would facilitate the punishment of cyber aggressors and this protects international peace and security for being violated by an expansive reading of self-defense that triggers armed conflicts.

Moreover, cyber-attacks can qualify to an armed attack that allows the victim state to take countermeasures under article 51 of the UN charter law in the incidents where the cyber-attack either causes human fatalities or large scale damage or destruction to property, but the paper disagrees encourages a more restrictive approach to attacks that target critical infrastructure and to be considered as armed force even if no physical damage occurred as long as it aims deliberately to cause such damage, Stuxnet as an example. In this regard, The Tallinn Manual played an important role by providing basis for analyzing jus ad bellum in the context of cyber operations, but couldn't fully clarify the evidentiary standard which will always create a difficulty for states in the practical guidance regarding this legal issue, moreover such document remains with no authoritative power on the legal rules on cyber-attacks but rather remains private opinions of its authors.

This paper examined as well the applicability of law of armed conflict (IHL) to cyber operations in armed conflicts and concluded that although cyber-attacks are not regulated by any of the IHL treaties, yet their development and employment in armed conflict do not occur in legal vacuum. As well analyzed the main requirement of attribution in cyberspace in accordance to IAC or NIAC which is the over-all control standard therefore any cyber operations during this conflict will be governed by the IHL rules. The paper focused on the principles of distinction that should be interpreted in narrow way regarding military objectives to tackle its complexity in cyber warfare and that state practice will provide nuance to the application of LOAC to clarify the definition on the use of it in armed conflicts, and that will be a case by case study.

This leads to a conclusion that existing laws are capable in regulating cyber-attacks but extension of the analogy of those laws is needed to cover all its unique features especially with the rapid development of technologies and its growing involvement in contemporary conflicts. In addition, the article stresses that currently the term cyberwar lacks practical evidence, as to date we have not witnessed a war that has been fought purely in cyberspace or through cyber means but only operations that can be used as means of conflict, however state practices is drawing a development of norms on the long term that can come out by states' practices in a way that cyber incidents should be responded to by cyber means due to concerns of targeted states to escalate towards dramatic situations basing its responses on the advantage of cyber operations characteristics , that will qualify as a law through customary practices especially as none of the cyber-operations has reached the von Clausewitz's dicta about actions should be Violent, instrumental and political to qualify as war but that doesn't mean it won't witnessed in the near future. Moreover, detailed studies on the importance of development of strategies by UN and international organizations to deal with malicious use of cyberspace, and the role of UN Security Council mechanism to combat any threats intended via cyberspace to the international security and peace.

BIBLIOGRAPHY

Treaties and Agreements

1. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
2. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
3. The Geneva Conventions of August 12, 1949, International Committee of the Red Cross, Geneva.
4. United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI.

Academia Books and Articles

5. BARNETT, S. *Applying Jus Ad bellum in Cyberspace*. University of Toronto, 2016.
6. BOYSTOM, K. *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*. Swedish National Defense College, Stockholm, 2004.
7. BROWNLIE, I. *International Law and the Use of Force by States*. Clarendon Press Oxford, 1963.
8. CLAPHAM, A. *Brierly's Law of Nations*. Oxford University Press, Oxford, 2008.
9. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, National Research Council. The National Academic Press, Washington D.C, 2010.
10. DINNISS, H. Cyber Warfare and the Laws of War. Cambridge University Press, 2012.
11. DINSTEIN, Y. Computer Network Attacks and Self-Defense. *International Law Studies*, U.S. Naval War College, 2002.
12. DORMANN, K. *The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint*. International Committee of the Red Cross, 2001.
13. DROEGE, C. *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*. ICRC Geneva, 2012.
14. GEERS, K. *Cyberspace and the Changing Nature of Warfare*. Cooperative Cyber Defense Center of Excellence, August 2008. <www.scmagazine.com>.
15. GRANGE, M. *Cyber Warfare and the Law of Armed Conflict*. University of Wellington, Victoria, 2014.
16. HENCKAERTS, J-M.; DOSWALD-BECK, L. *Customary International Humanitarian Law*. Cambridge University Press, New York, 2005.
17. ICRC, Customary IHL, Israel "Practice relating to Rule 106". Conditions for Prisoner of War Status, Section A, Chapter III.
18. MELZER. N. *Cyber Warfare and International Law*. UNIDIR Resources, 2011.
19. MILANOVIC, M. State Responsibility for Genocide. *European Journal of International Law*, 2006.
20. PICTET, J. *Commentary to the third Geneva Convention*. ICRC, Geneva, 1960.
21. PICTET, J. *ICRC commentary to Article 2 of the First Geneva Convention*. Geneva, 1952.
22. RANDELZHOFER, A. "Article 51 UN Charter", in Bruno Simma (ed.), *The Charter of the United Nations: A Commentary*, Vol. I, 2002.
23. ROLING, Bert. Criminal Responsibilities for Violations of the Law of War. *Belgian Review of International Law*, 1976.
24. ROSCINI, M. World Wide Warfare- Jus ad bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law*, Volume 14, Netherlands, 2010.
25. SANDOZ, Y. the ICRC Commentary to Article 1 of Additional Protocol I. Geneva, 1987.
26. SCHMITT, M. & VIHUL, L. Proxy wars in Cyberspace: The Evolving International Law of Attribution. *Fletcher Security Review*, 2014.
27. SCHMITT, M. Classification of Cyber conflict. *Journal of Conflict and Security Law*, Vol. 17 , Oxford University Press 2012.
28. SCHMITT, M. "Attack" as a Term of Art in International Law: The Cyber Operations Context, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn 2012.

29. SCHMITT, M. The Law of Cyber Warfare: Quo Vadis? *Stanford Law and Policy Review*, 2014.

30. SCHMITT, M. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press 2013.

31. SCHMITT, Michael. Cyber Operations and The Jus in Bello: Key Issues. *Naval War College International Law Studies*, Vol. 87, 2011.

32. SHACKELFORD, S. *State Responsibility for Cyber Attacks: Competing Standards for a growing problem.* University of Cambridge, 2010.

33. Tallinn Manual. NATO Cooperative Cyber Defense Centre of Excellence CCDCOE, Cambridge University Press, 2013.

34. WAGSTAFF, J. The Internet could be the Site of the Next China-U.S. Standoff. *The Wall Street Journal*, April 30, 2001.

International Cases and Decisions

35. ICJ, Case Concerning Oil Platforms, *Islamic Republic of Iran v. United States of America*, 6 November, 2003.

36. ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996.

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

38. Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.

39. *Prosecutor v. Fatmir Limaj*, Judgment, IT-03- 66-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 30 November 2005.

40. *Prosecutor v. Lubanga*, Decision on Confirmation of Charges, International Criminal Court (ICC) January 29, 2007.

United Nation Documentation and Resolutions

41. Draft articles on Responsibility of States for Internationally Wrongful Acts, Year Book of International Law Commission, Volume II, Part II, United Nations Geneva 2001.

42. United Nations General Assembly Resolution 3314 (XXIX) Definition of Aggression, United Nations, Geneva 1974.

Online Journals

43. BBC News, Cyber-attack: Europol says it was unprecedented in scale, 13 May 2017. <http://www.bbc.com/news/world-europe-39907965>.

44. BBC News, Israel Lobby Group Hacked, 3 November 2000. <http://news.bbc.co.uk/2/hi/middle_east/1005850.stm>.

45. Bosnian Serb News Agency SRNA Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer, March 28, 1999.

VIRTUALUS TROJOS ARKLYS ŠIUOLAIKINIUOSE KONFLIKTUOSE

Alaa Al-Aridi

S a n t r a u k a

Internetas yra nuostabi žinių, laisvės ir komunikacijos erdvė, kartu nematomas pasaulis su daugybe matomų padarinių. „Shadow Networks“ generalinis direktorius Ericas Winsborrowas yra pasakęs: „karai nėra kariaujami ginklais ar šoviniais, šiandienos šnipai yra kibernetiniai šnipai.“ Straipsnyje nagrinėjamas tarptautinės humanitarinės teisės principų taikymas kibernetiniams veiksmams, daugiausia kibernetinėms atakoms, kuriuos reguliuoja *jus ad bellum* (teisės šaka, nustatanti jėgos panaudojimą kibernetiniame lauke), ir analizuojamas Jungtinių Tautų pagrindinių teisių chartijos 2 str. 4 d. taikymas, taip pat teisė į savigyną, nustatyta šios chartijos 51 straipsnyje. Taip pat tiriama, kaip teisiniai tarptautinės

humanitarinės teisės principai (*jus in bello*) taikomi kibernetinėms operacijoms ginkluotųjų konfliktų metu. Konstatuojama, kad tarptautinė teisė taikoma kibernetinėms atakoms, tiek *jus in bello*, tiek *jus ad bellum,* tačiau išskirtiniai kibernetinių tinklų atakų bruožai sukuria iššūkių daugelyje sričių, pvz., valstybių atsakomybė, operacijų intensyvumas, į kuriuos reikia atsižvelgti ginkluoto užpuolimo atveju. Taip pat atkreiptinas dėmesys į tai, kad tarptautinei humanitarinei teisei šie konfliktai nėra gerai pažįstami ir aiškiai sureguliuoti, nes ši teisės šaka buvo sukurta reguliuoti konvencinius konfliktus, o kibernetinių atakų ypatybės iš esmės kelia iššūkį esminiams tarptautinės humanitarinės teisės principams.

Įteikta 2017 m. lapkričio 27 d.
Priimta publikuoti 2018 m. balandžio 30 d.