International Journal of Law
ISSN: 2455-2194
Impact Factor: RJIF 5.12
www.lawjournals.org
Volume 4; Issue 6; November 2018; Page No. 83-88

The challenges of cyber-warfare in the application of international humanitarian law (IHL): A critical examination of IHL rules in addressing those challenges

Addisu Genet
Assistant Lecturer, College of Law and Governance Study, Dilla University, Ethiopia

Abstract
The centuries old, conventional jargons and doctrines in the domain of warfare are replaced with a new concept and techniques. The rapid advancement of means and methods of warfare in the area of non-kinetic warfare such as cyber-warfare, coupled with IHL rules are designed to apply to means and methods of warfare basically; involving the use of kinetic force in the physical world, makes an awkward fit for the hostilities that consists of the manipulation of data in cyberspace, despite enormous civilians suffering. Two arguments revolve concerning the challenges currently facing to regulate cyber warfare. While some argues the existing law is not adequate to govern the employment of cyber warfare. The other side maintains that the violation is being committing against the existing laws and calls for strengthening the compliance mechanism. This article has the aim of assessing the adequacy of the existing laws and customs of war in regulating cyber-warfare. This article reveals the challenge arising through cyber warfare in the contemporary armed conflict through legal and extra-legal factors. Finally it emphasis's for the sincere exploitation of the existing legal framework until cyber specific treaty is reached.

Keywords: cyber-warfare, compliance system, adequacy, non-kinetic warfare

1. Introduction

Cyber-operation, which involves development and dispatch of the computer code from one or more computers to target computers, can be aimed at either infiltrated a computer system to collect, export, destroy, encrypt data, tripper alter or otherwise manipulate processes [1]. Cyber operation may be directed either to the computer system or directly against the people. In the former, civilians' installations such as banking system, railroad, water treatment and distribution system, gas and oil pipelines, air traffic control are susceptible to cyber-attack, while the latter attacks only civilian population.

Although, there is no provision in IHL that explicitly outlaws cyber warfare or computer network attacks, either carried out independently or during times of war, it appears to be uncontested that IHL norms on the means and methods of warfare apply to a cyber-warfare. This essay aims to explore the adequacy of existing law of war to regulate cyber-warfare. Firstly, it assesses the scope of the existing law. Secondly, it triggers the cyber-warfare events and challenges to the application of IHL. Thirdly, the possible panaceas are advanced, followed by conclusion lastly.

2. Delimiting scopes of application of IHL to cyber-warfare

It is axiomatic that IHL applies only to situations of Armed Conflict (AC). Legally there are two types of conflict: International Armed Conflict (IAC): and Non-International armed-conflict (NIAC). IAC exists whenever there is a resort to armed force between two or more states through their representatives or acts acknowledged by them while NIAC is a conflict that takes place in the territory of a State where there is protracted AC between governmental authorities and organized armed groups or between such groups. If cyber-attack is committed as part of ongoing AC in both typologies of war, we face no serious problem to apply IHL rules. To begin with IAC, one should examine the inclusion of cyber-attack within the meaning of force as stipulated under art 2(4) of the UN Charter. By doing so, it is possible to determine the applicability of IHL [2].

There are two lines of arguments herewith. One deals with exclusion of cyber-attack from the realms of prohibitions under art 2(4) of the Charter. The reverses views for its inclusion thereby allowing the victim state the right of self-defense under art 51 of the Charter. The author believes the second line of argument is legally and logically acceptable. Firstly as envisaged from the preamble, the very purpose of the charter is to maintain peace and security. Therefore, once the employment of cyber-attack is threatened the interest of states, it does not hold water to preclude such attack from the realm of force. This is reiterated in art 31 of the Vienna Convention on the laws of treaty (VCLT) that dictates good-faith interpretation of a treaty in accordance with object and purpose of the treaty in question to execute ambiguous provisions in international treaty like art 2(4) in the case of cyber-operation. Secondly, it is relatively uncontroversial that cyber operations fall under the prohibition of article 2(4) of

[1] Cordula Droege (2012), Get off my cloud: Cyber-warfare, IHL, and the protection of civilians, International Review of the Red Cross, Volume 94, Number 886, P. 533, 538.

[2] However, it should not be interpreted as to the existence of confusion in relation to Jus ad bellum and Jus in bellom.

the UN Charter once their effects are comparable to those resulting from kinetic, chemical, biological or nuclear weaponry [3]. The international court of justice has also renders, the prohibition applies "to any use of force regardless of the weapons employed [4]. Hence, cyber-operation having the required threshold of AC triggers the applications of IHL.

Coming back to the characterization of cyber-attack as NIAC, the issue demands for specific analysis. It is certain that, weakly associated cyber-operation and cyber-operations conducted by individuals cannot qualify as NIAC because they are insufficiently 'organized. That means, singular and merely sporadic cyber incidents capable of being controlled by domestic law enforcement do not qualify armed conflict. At this juncture hacker or other similar groups, that are organized entirely online cannot constitute armed groups within the meaning of IHL. Because, the members of virtual organizations may never meet nor even, know each other's actual identity. Such online organization will not have the required disciplinary rule and internal administration required to be an armed group.

Besides, crime is not an act of war, nor is espionage although the consequences of cyber espionage currently are constantly on the verge of escalating into full-scale war [5]. Security threats emanating from cyberspace such as "cyber-crime", "cyber piracy", "cyber policing" etc. does not fulfill the threshold of armed conflict. Terrorists are not "lawful combatants" as defined by international law. Nevertheless, whether terrorist attack qualifies as armed conflict would depend on the nature and duration of the attack. A single attack could be considered a criminal act rather than an act of war; multiple attacks by the same group as part of a sustained campaign could justify the use of military force [6].

As far as the object under attack is concerned in both typologies of war, should IHL be applicable only to direct cyber-attack against the people or should it include attack against computer system need to be investigated. Here, we can argue in two ways. One enlarging the meaning of armed conflict to include attack against computer system would unjustly extend the scope of IHL. Oppositely, it can be propagated for the characterizations of cyber-attack against the computer system as armed conflict. This article argues favoring the second line of argument owing from the following reasons. First, IHL stands to minimizing human suffering and protecting persons affected by war, at any rate its scope is not depends on the type of object under attack.

Cyber-operation would certainly constitute an attack within the meaning of Art 49(1) of additional protocol I (API) which reflects customary international law. In this regard there is still disagreement concerning whether "destruction" as consequent elements of the attack should be complied or else the result of the attack like dysfunctional is sufficient. Both sides weigh but I found certain lacunas in both of them in that the 1st one narrowly interprets the notion of attack so that attacks like incapacitation of a state's air defense system would not qualify as an attack by the mere fact of having no specific destruction, death or injury. The second argument will also unnecessarily overstate every sort of attack. So I opine aggravating the two level of understanding to their extreme will miss the nature and purpose of IHL. Nevertheless, it should be known cyber-attacks unlikely to result in death, injury or destruction could still amount to an "armed attack" if they aim to incapacitate, *inter alia*, "critical infrastructures [7]. After intense discussion, the majority of experts of the Tallinn Manual [8] agreed that beside physical damage, loss of functionality of an object might also constitute damage. At this juncture, it should be known that IHL concept of attack does not apply to non-physical means of psychological or economic warfare such as the dissemination of propaganda or the establishment of embargo [9] cyber-operation that interferes with civilian communication system too, like jumping of radio communication or television broadcasting, which have not traditionally been considered an attack in IHL, and other acts equivalent to such form of "warfare" does not amount to an attack within the meaning of Art 49(1) and art 52 of API.

Related to the issue raised above the point regarding civilians participating in the hostility amounting direct participation in the case of cyber-warfare needs to be settled. Although, ICRC clarifies cyber operations directly causing military harm to the adversary in a situation of armed conflict amounts to direct participation in hostilities [10] the types of *harm* and its *extent* of attack justifying direct participation have not yet clarified. With the mode of argument I raised above, attack should not be limited to destruction, death and injury but also any harm directly and adversely affecting military operations or military capacity of the adversary should be included too.

3. Adequacy of existing IHL norm to regulate cyber warfare

Contemporarily, two lines of arguments are revolving around laws applicable to cyber-warfare. The first one adheres the existing IHL are sufficient to regulate cyber-warfare and one should focus on the enforcement of the existing norms. On the other hand, the second one advocating for adopting of new

[3] Michael Schmitt (1999), Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, vol. 37, p. 916.

[4] ICJ (1996), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, p. 39 and Ian Brownlie (1963), International Law and the Use of Force by States, Oxford University Press, p. 362, 431.

[5] Dunn Cavelty, Myriam (2012), The Militarization of Cyberspace: Why Less May Be Better, IEEE-Explore, 4th International Conference on Cyber Conflict (CYCON), P. 1-13.

[6] Ibid.

[7] UNGA Resolution No. 58/199 of 30 January (2004),US Presidential Decision Directive 63, Critical Infrastructure Protection, 22 May (1998), Australian government, Cyber Security Strategy,(2009), p. 20; defined critical
infrastructures broadly and includes essential public facilities, attacking them cause consequences directly affecting national security, including that of the individual, society and state within the sphere of sovereignty of another state.

[8] The most comprehensive of these efforts is the Tallinn Manual on the International Law Applicable to Cyber Warfare, (June 2011)which was drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence.

[9] Michael Bothel, Karl Josef partsch and Waldemar A. solf (1982),New rules for victims of armed conflict: commentary to the two 1977 protocols additional to the Geneva Convention of 1949, P. 289.

[10] ICRC (2005), Third Expert Meeting on the Notion of Direct Participation in Hostilities, Summary Report, P. 14.

legal framework [11]. The article is of the opinion that both of the two argument veils lacunas. In the first place, IHL rules crafted basically taking in to account Kinetic warfare are less suitable to apply for non-kinetic warfare. In doing so the enforcement of IHL grand norm; minimizing human suffering and protecting victim of the conflict is becoming a serious problem in the case of cyber-warfare. On the other hand, while adopting cyber-specific treaty under the prevailing atmosphere is not a simple task letting cyber warfare to remain unregulated under the guise of waiting new law is not acceptable.

An increasing number of state and international organizations have publicly asserted for application of IHL to cyber-operation. ICJ recalled that the established principles and rules of IHL applicable in armed conflict apply "to all forms of warfare and all kinds of weapon" those of the future [12]. Despite these facts, a number of cyber-attacks both by states and non-state actors were allowed to go without being handled by IHL despite their devastating results. For instance, when Russia launched a massive DDoS (distributed denial of service) attack against Estonia in 2007, Georgia in 2008 and recently against Ukraine in 2014, the three victim countries lost much of their ability to defend themselves and its citizens as well as to appeal to the outside world. Moreover, the attack has resulted the loss of property, infrastructure, and human life [13]. The author believes the gap in applying IHL to cyber-warfare is attributed to both legal and practical lacunas [14].

3.1 Legal Factors

1. Although most hackers are civilians, who remain protected by IHL against direct attack, the situation is different if hackers take a direct part in the hostility by way of a cyber-attack in support of one side in armed conflict. At that moment, they would be obligated not only to be a legitimate object of attack but also have the duty to comply the law and customs of war. Nevertheless, administering the principle of distinction under the prevailing law to the question of cyber-operation poses the following challenges.
   - Difficulty of characterizing hackers as a "combatant" by using the criterion of the law of war. For instance, wearing uniform and carrying arm openly; the prevailing requisite to be a combatant could be difficult to establish. This in turn undermines civilian protection.
   - Difficulty in *"Levee en masse*" to obtain Prisoners of War status because it is uneasy to establish the requirements of carrying arm openly and territory owing from the nature of cyber-warfare. The requirements of organization and affiliation required for combatant status could also be difficult to establish [15].
   - Beside this, the principle of distinction and proportionality may encounter problems to apply it against infrastructures having dual purpose. For example, 98% of American military communication goes through a civilian infrastructure [16]. Although literal understanding of the existing law seems to make them military objectives [17]. It is hardly possible to handle the attack committed against dual purpose cyber instruments in the case of cyber warfare under the existing legal frameworks. In particular, the following issues are challenging currently.
   - Whether the destruction of data is protectable, if so, the extent of protection.
   - The principles of proportionality dictating the attacking side to drive a definite military advantage in the attack. And the fact that attacks offering a definite military advantage under cyber-operation is difficult to determine based on the existing IHL. So it needs to have clear and precise parameters.
   - To what extent attacking dual installations would be justified owing to the difficulty of making a complete proportionality calculation.
   - The fact that constructive attack of civilian objects through data stream like blockage of communication is not prohibited.
2. Although it is easy to operate cyber-attack outside of a national border by state and non-state actors, the principle of neutrality is designed to international armed conflict despite the continuing violation of this principle in the conduct of non-international armed conflict.
3. The increasing rate of cyber espionage, cyber criminality and cyber terrorism, and the fact that the existing law of war is short of regulating them.
4. Confusion regarding threshold required to constitute cyber-attack as armed conflict. Especially, in case when the hostile act is committed solely via cyber operation.
5. The notion of attack contained in art 49(1) of API and customary international law rule mainly crafted for kinetic warfare and less suitable for non-kinetic warfare.
6. In addition, issues involving sovereignty, "force" or "over flight" the use of cyber-attacks by terrorists are relatively ambiguous under the current legal framework.

3.2 Extra-legal factors

1. Due to its veil of secrecy technical and practical matters including key information's regarding the technology available, the attack conducted, the identity of the actor, the policies and guidelines regarding the employment of cyber-warfare are also most of the time unknown [18]. This

[11] James A. Lewis (2010), A note on the laws of war in cyberspace, p. 1.

[12] Supra note 4, ICJ reports 226. The participant in 2004 Stockholm experts conference also agreed that, "IHL applies to computer network attack (CAN) in an ongoing IAC." See also art 36 of AP I of the 1949 Geneva Convention (1977).

[13] Available at. http://securityaffairs.co/wordpress/18294/security/fireeye-nation- state-driven-cyber-attacks.html.

[14] This enlistment is a mere attempt, not the conclusive one.

[15] Nils Melzer (2011), Cyber warfare and International Law, Center for Business and Human Rights.

[16] Eric Talbot Jensen (2010), Cyber warfare and precautions against the effects of attacks, in Texas Law Review, Vol. 88, p. 1534.

[17] Art 52 (1) AP I and customary international humanitarian law rule 8 defining as: military objective are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstance ruling at the time, offers a definite military advantage. No doubt those infrastructures effectively contribute to the military action and attacking them would offer a definite military advantage. See also Tallinn Manual, supra note 8.

[18] Eitan diamond (2014), Applying IHL to Cyber-Warfare, Memorandum No. 138, Tel Aviv: Institute for National Security Studies.

entails the difficulty in identifying the party responsible to the attack, characterization and extent of the liability. This problem is much easier, however, in case of cyber-attack committed in tandem with an ongoing armed conflict.

2. Distinguishing between exploitation and attack. It relies on the idea that exploitation is legal and attack is not.

Finally, it goes without saying that although lacunas on the part of the law to address cyber specific norms and the nature of cyber-attack has lied difficulty to govern cyber warfare, the most drastic challenge is widespread violation of already existing laws. So in tandem with the above factors violation of the existing laws is the prominent reason for the current widespread cyber-attacks contrary to the law and customs of war. According to the ICRC "lack of satisfactory enforcement, adequate awareness and willingness among the parties to the conflict to interpret the existing IHL in good faith and respect" are the underlying reason for the existing causalities [19].

4. The way forward

This section discusses a way forward to rectify the aforementioned challenges based on two departures. So, the author recommends exploitation of the existing legal framework and the adoption of new laws to rectify the challenge facing in the operation of cyber warfare.

4.1 Positively interpretation of the existing IHL

The principles of interpretation of international treaties contained in the Vienna Convention on the Law of Treaty 1969 (VCLT) which is considered to be CIL dictates interpretation of treaties in accordance with object and purpose of the treaty [20]. Further, art 26 of the same dictates good faith performance of a treaty obligation. The replica of this statement has also provided by ICJ stating, treaties should be interpreted and applied within the framework of the legal system prevailing at time of the interpretation, rather than at the time of the drafting or adoption of the text. Accordingly, the application of current IHL should not be defeated by the mere fact of being not cyber-specific. Instead, any interpretations should be in light of the underlying objective of IHL; minimizing human suffering and protecting person affected by conflict.

i) Sincere exploitation of existing way-outs

1. Core IHL rules and principles governing the conduct of hostility are broad and can be flexibly interpreted to accommodate far-reaching developments on the means and methods of war such as cyber warfare. To this effect, the "Martens Clause" as well as ICTY asserts that the veil of elementary consideration of humanity shall not be derogated under the guise of lack of specific agreements.
2. Regarding dual infrastructures, though contemporary understanding as well as art 52 API & rule 8 CIL seems to make them legitimate object of attack, I opine the problem created in this regard can be felt or at least minimized via employing the principles of proportionality (not to cause excessive collateral damage disproportionate to military advantage), principle of necessity (humanitarian and military considerations), and principles of precaution (taking all feasible precautions to rescue civilians infrastructures). Moreover, the belligerent should first appreciate the cyber weapon they used are not indiscriminately attacking one.
3. It should be stressed that technological weapons are discriminatory and proportional. Certainly, collateral damages under this assumption, is not essentially evil. It will happen, but it is possible to reduce it significantly, because the technology to do so is at hand. Cyber offers an enhanced ability to be "hyper distinguishing." Hence, belligerents should be encouraged to employ target specific cyber systems.
4. The meaning of armed hostility should be interpreted in a lenient manner. In this regard, Article 2 common to all the four Geneva Conventions invites us to widely interpret the meaning of war. Commentaries to the Geneva Conventions and their subsequent Additional Protocols have posited that" armed conflict" can be viewed in a fairly expansive way. In tandem with the above constructive interpretation:-
   - Measures that are essential to protect civilians including segregating military objective from civilian infrastructure and network, segregating computer system on which essential civilians' infrastructure depend from the internet, backing up important civilian data, using anti-virus and advance arrangement to foreseeable kinds of cyber-attack should be adopted by the contracting states [21].
   - Developing an Internet anonymity system is also recommended: doing so requires stakeholders typically ICRC to work with international institutions like the International Telecommunications Union, the European Network and Information Security Agency working to establish clearer policies on cyber use, fighting cyber-attacks and developing a global information infrastructure.
   - The ICRC should adopt guidelines regarding the characterization and acts comprising of cyber-warfare until binding treaty made on the score.
   - The contracting states should also make researches to important civilian cyberspaces regarding the possibility of cyber-attack. They should also make civilian infrastructures less susceptible to cyber-attack.
   - Establish awareness creating forums such as educating military personals, states and any stakeholders to ensure the obligation arising from IHL.

ii) Technical and operational challenge not a reason denouncing the Application of IHL

1. I opine most challenges raised based on cyber warfare such as determining the author of particular cyber-attack and from which location it comes from, the destructive potential and the like are practical and technical problems

[19] International institute of humanitarian law (2013), respecting international humanitarian law: challenge and response. 36th round table on current issue of international humanitarian law, sanremo, 5-7 September 2013.

[20] Art 31 (1) of the Vienna Convention dictates the interpretation of a treaty in light of its object purpose and good faith.

[21] Prosecutor vs. Martic (1996), Review of Indictment pursuant to rule 61, No.IT-11-R 61, Para 13.

or else arising from poor interpretation of the law that should be resolved by technical or practical layouts only but not by means of law. As difficulty to locate the scenes and suspect of the crime doesn't make the criminal law inapplicable. In nutshell, it should be recognized that the law is designed to solve legal problems not technical one.

2. In kinetic warfare, a sniper does not disclose its identity or source but such problem does not avoid the application of IHL to the attack. Hence, there is no reason to act differently to cyber warfare because of its difficulty to prove source. Instead, we should focus on proving it through sophisticated evidentiary means like forensic investigation. Regarding burden of proof in the Oil Platforms case [22], it effectively apprehended that the state/party invoking the right of self-defense shall prove thereof.
3. Thus, it is important and would be in line with the solid aim of IHL and the goal pursued by ICRC to analyze and apply the existing IHL in a temperate manner than easily capitulating ourselves to modern and technologically most complex means and methods of warfare. Accordingly, it requires working for strengthening the compliance system of the existing laws mainly through dissemination and revitalizing of the existing mechanism [23].

4.2 Revisiting the void-filling of existing legal frameworks

Although there might be a fear that the general international atmosphere at present is not conducive to the introduction of new law, I view for gradual adoption of them with the following minimum features:

- Redefining the notion of attack in the cyber context
- The fit of infrastructure having dual purposes and civilians who do not understand the fact that their computer is running a cyber-operation.
- Standard guideline to characterize and how states can permissibly use computers to carry out attacks either independently or part and parcel of a traditional AC and attribute cyber warfare.
- Law prohibiting constructive attack of civilian infrastructures.
- Law protecting essential civilian's data stream.
- Special protection to cyber-specific installations like medical infrastructures, works, installations containing dangerous forces, objects dedicated to the survival of the civilian population.
- Rules governing cyber espionage that currently is escalating into full-scale war.
- Revisiting the principle of neutrality to make it more compatible to NIAC.
- Adopting cyber compatible requirements regarding *levee en masse* and combatant status. Example, the requirements of carrying arms openly should be replaced by criteria like unremitting participation.
- Establishing a central cyber monitoring body under the UN system. This is because although there are regional bodies like NATO, Council of Europe, and Shanghai Cooperation they lack inclusivity.

[22] ICJ (3003), Oil platforms, (Islamic republic of Iran v. USA), summary of judgment.

[23] Kremte, H. A (2017). Minimizing human suffering and protecting person affected by conflict: A critical appraisal of the compliance system of international humanitarian law. Beijing law review, 8, 440-450. Available at https://doi.org/10.4236/blr.2017.84024

5. Conclusion

Saving extensive arguments on its adequacy currently, there is utmost consensus that existing IHL rules and norm applies to the employment of cyber-operation in warfare. However, it poses legal and practical challenge in an attempt to ensure its use in complies with the existing IHL norms. It appears that cyber-warfare in contemporary armed conflict causes devastating and terrible enormous human suffering and destruction of civilian and military infrastructures even more badly than kinetic warfare's. This repercussion being caught in the midst of hostilities would be far lesser if the existing IHL were properly implemented by the parties to conflicts. Hence, while as far as possible revisiting of the existing IHL to fill the legal lacunas is advisable, till that we should give emphasize to strengthening the compliance system with the existing dogmas of war.

6. References

1. Bothel Michael, partsch Karl Josef and Waldemar A. solf, New rules for victims of armed conflict: commentary to the two 1977 protocols additional to the Geneva Convention of 1949, 1982.
2. Cavelty Dunn, Myriam, The Militarization of Cyberspace: Why Less May Be Better, IEEE Explore, 4th International Conference on Cyber Conflict (CYCON), 2012.
3. Diamond Eitan, Applying IHL to Cyber Warfare, Memorandum No. 138, Tel Aviv: Institute for National Security Studies, 2014.
4. Droege Cordula, Get off my cloud: Cyber Warfare, International Humanitarian Law, and the protection of civilians, International Review of the Red Cross. 2012; 94:886.
5. Eric Talbot Jensen. Cyber warfare and precautions against the effects of attacks, in Texas Law Review, 2010, 88.
6. Henok Ashagrey. Minimizing Human Suffering and Protecting Persons Affected by Conflict: Critical Appraisal of the Compliance System of IHL, a paper presented for East African Humanitarian Law Essay Competition (unpublished), 2016.
7. Ian Brownlie, International Law and the Use of Force by States, Oxford University Press, 1963.
8. ICRC, International humanitarian law and the challenges of contemporary conflicts, Document prepared for the 30th International Conference of the Red Cross and Red Crescent, (Geneva, Switzerland, 2007, 26-30.
9. ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report prepared for the 28th International Conference of the Red Cross and Red Crescent, Geneva, 2003.
10. ICRC. Commentary on Additional Protocol of 8 to the Geneva Convention of, (Geneva: Martins Nijhoff publisher, 1977-1987.
11. ICRC. Improving Compliance with International Humanitarian Law, Background Paper prepared for Informal High-Level Expert Meeting on Current

Challenges to International Humanitarian Law, (Cambridge, 2004, 25-27.
12. ICRC. Third Expert Meeting on the Notion of Direct Participation in Hostilities, Summary Report, 2005.
13. International Institute of Humanitarian Law, Respecting International Humanitarian Law: Challenges and Responses, 36th Round Table on Current Issues of International Humanitarian Law Sanremo, 2013.
14. James A. Lewis, A note on the laws of war in cyberspace, Center for Strategic and International Studies, 2010.
15. Melzer Nils, Cyber warfare and International Law, Center for Business and Human Rights, 2011.
16. Michael Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1999, 37.
17. Misganaw Belete, The use of explosive weapons in densely populated areas: an assessment of its legality under the rule of IHL, a paper presented for East African Humanitarian Law Essay Competition (unpublished), 2015.
18. W. smith, Thomas, The New Law of War: Legitimizing Hi-tech and Infrastructural Violence, International Studies Quarterly. 2002; 46:3.
19. Tallinn Manual on the International Law Applicable To Cyber Warfare, 2011.
20. US Presidential Decision Directive 63, Critical Infrastructure Protection, 1998.
21. Additional protocol I to the Genera conventions of, 1949-1977.
22. Additional protocol II to the Genera conversions of, 1949-1977.
23. UN. Vienna Convention on the Law of Treaties, Treaty Series 1155-1969.
24. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 1949.
25. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949.
26. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 1949.
27. Geneva Convention Relative to the Treatment of Prisoners of War, 1949.
28. http://www.genevacall.g
29. http://www.icrc.org
30. https://www.csis.org/ane
31. http://www.ccdcoe.org/249.html
32. http://unidir.org/files/publicatiof
33. http://www.inss.org.il/publicatte/
34. ICJ, Oil platforms, (Islamic republic of Iran v. USA), summary of judgment, 2003.
35. International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996.
36. Prosecutor VS. Martic, Review of Indictment pursuant to rule 61, No.IT-11-R61, 1996.
37. International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, ICJ Reports, 1986.