ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 7, Issue 3, pp: (487-490), Month: July - September 2019, Available at: www.researchpublish.com

CYBER CONFLICT: NEW TREND TO ARM CONFLICT

IBRAHIM SHEHU

FACULTY OF LAW

USMANU DANFODIYO UNIVERSITY, SOKOTO

Abstract: **Cyber conflict remained a challenge to the global community. Information technology has created a situation where countries in the world have engaged one another in cyber war. The same platform equally serves as a medium for conflict resolution which dispensed the traditional means of face to face conflict resolution. This paper intend to unravel some of the existing framework of cyber conflict by connecting it with the existing humanitarian laws of jus in bellum and jus ad bellum. The paper further identified some of the major challenges created by cyber conflict and recommend on the possible ways of addressing it.**

1. INTRODUCTION

The internet is inherently neither a weapon of war nor a weapon of peace. The ideals and values of some of its key innovators were central around human needs, aspirations, international, global and cosmopolitan values. The internet is now a global site where conflict is conducted, it is also massively but presently under utilized but yet powerful tool for conflict resolution. However, the internet through the ease of access and the interactivity and creativity enabled by the world wide web is a global space not only for information sharing and email communication but also for new media, social networking sites, user centered and collaboration resources such as wikis and blogs, e-commerce, global accessible e-learning, e-academics and fourth part dispute resolution.[1]

The internet is an ideal place to practice communication and conflict resolution skills. Just as the absence of visual and auditory clues, the anonymity, invisibility delayed reactions and neutralizing of status face us to say whatever negative thing we want, they can also free us to try new and more positive communication styles and to take all this time we need to do that.[2] Online platforms are increasingly implemented in conflict resolution program.[3] Over the past decade there has been growing number of internet users and other communication technologies for conflict management and peace buildings. This paper is aimed at examine the role of internet in conflict resolution.[4]

2. DEFINITION OF CYBER CONFLICT

Conflict in cyber space refers to actions taken by parties to a conflict to gain advantage over their adversaries in cyberspace by using various technological tools and people based techniques.[5] It is further defined as the confrontation between two or more states in the information space aimed at damaging information systems processes and resources and undermining political, economic and social systems, mass brainwashing to destabilize society and state as well as forcing

[1] Oliver R., Contemporary Conflict Resolution, e-book https:/books.google.com/books?1sbn=0745649734 assessed on 7th/9/2016

[2] Kali M., Conflict in cyberspace: How to resolve conflict online www.rider.edu/suler/psycyber.html assessed on 7/9/2016

[3] Sandy S, Digital Conflict resolution: Using Internet based platform to improve intergroup relations

[4] Laura R., can the internet solve conflict?

[5] Herbert L., Cyber conflict and international humanitarian Law, international Review of Red Cross. Volume 94 Numb 886 2012.

the state to take decisions in the interest of an opposing party. Cyber conflict can also be seen as information operations conducted in situations of armed conflict and excludes information operations occurring during peace time.[6]

Therefore, the use of the term cyber conflict should be restructured to armed conflicts within the meaning of international humanitarian law. Indeed, security threats emanating from cyberspace which do not reach the threshold of armed conflict can be described as cybercrime, cyber operations cyber policing or where appropriate as cyber terrorism.[7]

3. THE LEGAL FRAMEWORK FOR CYBER CONFLICT

The legal framework for conflict applies to both state and non state actors but the decision as to where to apply it depends in large part on whether an action is deemed to have involved the use of force. Note that cyber conflict today almost exclusively involves crime and espionage.[8]

It is important to note that two separate bodies of law apply to cyber conflict Jus ad Bellum, the laws governing a decision to resort to the use of force and jus in Bellum, the laws governing the conduct of hostilities, the former guide a nation' s decision as to whether an incident justifies engaging in armed conflict or trigger the provision of the UN Charter on a nations right to use force in self defense.[9] The provision of the UN Charter provide the legal framework for the Jus ad Bellum.

Therefore, Jus in Bello is based in large part on the provisions of the Geneva Conventions and their customary counterparts. However, all member states shall refrain in their international relations from threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistence with the purposes of the United Nations.[10]

The use of force contained in Article 2(4) establishes the benchmark standard for determining a violation of international law in the world of Kinetic conflict. Therefore, once the use of force occurs, permissible responses are determined by the law of state responsibility. An interpretation of Article 2(4) could include cyber intrusions depending on the severity of their impact. Cyber attacks, in addiction, the use of force framework has little value in developing responses to terrorist. By the terms of the Charter, non state actors cannot violate Article 2 (4) and responses to uses of force are limited to activities carried out by or otherwise the responsibilities of states.[11]

Meanwhile, the UN Charter further states that nothing in the present Charter shall impair the inherent right of individual or collective self defense if an armed attack occurs against a member of the United Nations until the security council has taken measure necessary to maintain international peace and security.[12]

Note that, the law of self defense remains unsettled. The text of Article 51 " armed attack is not as amenable as use of force to a flexible interpretation nor did the Charter drafters consider the possibility that every harmful consequence could follow from a non kinetic cyber attack. The legal bases for self defense may also be extended to anticipatory self defense in the cyber context.[13]

Furthermore, to trigger the right of self defense, national authorities would need to decide if a cyber exploit constituted an armed attack. Therefore cyber exploit that was a violation of sovereignty is by itself not sufficient. An exploit that did not directly cause substantial death or physical distinction would most likely not qualify as an armed attack. The applicability of these provisions of the UN Charter will remain somewhat ambiguous. However, while it is possible to clarify when and under what circumstances a disruptive exploit in cyberspace could be considered an armed attack.[14]

[6] Kerstin et. Al., Confronting cyber conflict. Forum sidarmament. United Nations Institute for Disarmament Research, Geneva, 2011

[7] ibid

[8] James A.L., A note on the Laws of war in Cyberspace

[9] Ibid.

[10] Article 2(4) United Nations Charter.

[11] William C.B., Developing Norms for Cyber Conflict forthcoming in research Handbook on remote warfare ed (Edward Elgar, 2016)

[12] Article 5 (1) United Nations

[13] Williams Opcit.

[14] James Opcit

It is worthy to note that there are 3 principles from the law of war that establish a framework for judging the legality of using different form of cyber attack during armed conflict.

This principle of distinction which requires attack to be limited to legitimate military objectives and that civilian objects shall not be the object of attack. However, the principle of proportionality which requires that the use of force in self defense must be limited to that which is necessary to meet an imminent or actual armed attack and must be proportionate to the threat that is faced and the principle of discriminate attack prohibits attack that cannot reasonably be limited to a specific military objection and which are indiscriminate or haphazard in their inclusion of civilian targets.[15]

However, the above legal principle would seem to prohibit attacks on purely civilian infrastructure when the resultant disruption would not produce meaningful military advantage. To be consistent with the laws of war the use of cyber attacks during conflict would face the same constraints as attacks using kinetic weapons.[16]

In Nigeria, there is no particular regulation on resolving cyber conflict. The only law available is the recent law passed on cyber crime Known as Cyber Crime Act 2015 by the former administration of president Goodluck Jonathan in 2015.

Meanwhile, the dynamic growth of reliance on the internet to support our infrastructure have caused the United States to modify its longstanding views on the predicates for treating e cyber intrusion as an armed attack or use of force. It suggested that Cyber attackers that have especially harmful effects will be treated as armed attacks while lower level intrusion would enable cyber counter measures in self defense.

In 2015, the U.S Department of defense publicly announced the major cyber milestones, first the department of defense must be prepared to defend the United States and its interest against cyber attacks. June same year the department of defense release its long awaited law of war manual which include a chapter on cyber operations.[17]

4. CHALLENGES OF CYBER CONFLICT

The absence of adequate laws and policies on cyber conflict have created a major challenge towards resolving cyber conflict. Therefore parties to arm conflict exploit some of the lacuna created as a result of absence of the law to further advance with their heinous act. The provision of the Jus ad Bellum and jus in Bellum did not provide a solution to the new trend of cyber conflict. Even though, developed countries like the United State have taken good steps to arrest the menace of cyber conflict. However, developing nations are yet to wake up from slumber and therefore did not make an in road in addressing the issue of Cyber conflict.

High level of poverty and lack of computer literacy especially in Africa and other developing countries has affected the issue of conflict resolution on the internet and hence become a challenge towards online conflict resolution.

It is worthy to note that lack of infrastructure facilities i.e power, internet facility etc. Especially in developing countries have created a big challenge to conflict resolution on the internet. Therefore, in areas of armed conflict like the Central African Republic, Southern Sudan and Even the case of Boko Haram can be seen as a clear example of this.

There are a number of reasons to explain why conflict may be heightened online. One is the absence of visual and auditory cases. When we talk to someone in person, we see their facial expression, their body language and hear their tone of voice, for example, someone could shout and put their finger at you or they could speak gently and with kindness but in online communication, we have no visual or auditory clues to help us to decipher the intent means and tone of the message, all we have are the words and a computer screen.[18]

It is further observed that computer mediated communication often makes it difficult to clearly identify interaction partners ,people might pretend to be someone else and in turn, users find it difficult to trust one another online.[19]

The issue of confidentiality concern is also another major challenge, whereas traditional mediation does not create a physical record, online mediation create an electronic record and thus could potentially enable a party to print out and

[15] ibid
[16] ibid
[17] William Op.Cit
[18] Kali Op.Cit
[19] Digital Conflict resolution, using internet based platforms to improve intergroup relations.

distribute e-mail communication easily and without the knowledge of the other party and thus may hinder the development of open and honest exchanges in cyber mediation.[20]

Moreover, cyber mediation loses the dynamic of traditional mediation because it takes place at a distance and in front of computer screen rather than with face to face communication, the substitution of e-mail for dialogue for example makes it difficult to give any weight to emotion in mediation.[21]

5. CONCLUSION

It is clear that conflict in cyber space can occur. However, as far as the law is concerned, the phenomenon of cyber outlet does not exist in legal vacuum but as subject to well established rules and principles. Even though certain difficulties and a number of questions were raised with regards to this. Therefore, existing laws for armed conflict can be applied to cyber conflict but that there are areas of ambiguity involving the violation of third party sovereignty, the international community lack consensus regarding the generally accepted principles of law applicable to cyber conflict. Countries remain divided regarding the sufficiency of those provisions to regulate sovereign conduct in cyber space.

REFERENCES

[1] Herbert L., Cyber conflict and international humanitarian Law, international Review of Red Cross. Volume 94 Numb 886 2012.

[2] James A.L., A note on the Laws of war in Cyberspace

[3] Joseph, W. Goodman, the pros and cons of online dispute Resolution: An assessment of cyber mediation websites.

[4] Kali M., Conflict in cyberspace: How to resolve conflict online www.rider.edu/suler/psycyber.html assessed on 7/9/2016

[5] Kerstin et. Al., Confronting cyber conflict. Forum sidarmament. United Nations Institute for Disarmament Research, Geneva, 2011

[6] Laura R., can the internet solve conflict?

[7] Oliver R., Contemporary Conflict Resolution, e-book https:/books.google.com/books?1sbn=0745649734 assessed on 7th/9/2016

[8] Sandy S, Digital Conflict resolution: Using Internet based platform to improve intergroup relations

[9] William C.B., Developing Norms for Cyber Conflict forthcoming in research Handbook on remote warfare ed (Edward Elgar, 2016)

[20] Joseph, W. Goodman, the pros and cons of online dispute Resolution: An assessment of cyber mediation websites.

[21] Ibid.