RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Anticipatory on the use of cyber-attacks: an analytical legal study in the light of international humanitarian law

By

Mohammed Oudah Mohsin
Email: Moudah992@gmail.com
Public Law Department – College of Law/Al- Nahrain University/Baghdad/Iraq

Ali Yusif Abdulnabi AL- Shukri
2 Iraqi Presidency/Baghdad/Iraq.
Email: alialshukrilaw@yahoo.com

Saja Mohammed Abas AL- Esmeel
Public Law Department – College of Law/Al- Nahrain University/Baghdad/Iraq
Email: saja@law.nahrainuniv.edu.iq

Abstract

One of the most assured issues in the scope of International Humanitarian Law is the avoidance of the use of means and methods of warfare that directly and indirectly affects civilians, as well as taking the feasible precautions to avoid these effects, especially if there are certain facts, confirm that the use of a certain weapon or combat method will lead to a serious breach of the rules of International Humanitarian Law. This can be illustrated by conducting an approach between the concepts of anticipating ahead and whether cyber-attacks are a means of combat whose potential effects can be determined before use or not? In comparison with the rest of the weapons whose potential effects can be determined in the physical filed and not in the virtual filed (the digital).

Introduction

In this essay, we will try to review the legal rules governing the expected effects of cyber-attacks, in other words, can the effects be controlled by anticipating? and can digital technology be trusted to reduce out of control? especially as cyber-attacks pose a new challenge that requires the creation of a new legal mechanism for anticipating them. in other word, the current rules governing the Cyber-attacks and what they should to be, so as to fix the challenges before the International Humanitarian Law (Lex ferenda).

Essay Hypothesis

The rules of International Humanitarian Law may apply to some cyber-attacks. Thus, the principle of anticipating will be risen as to the provisions of these rules. However, they may not be applicable in all cases. Anticipating in the use of cyber-attacks varies from case to another.

Essay Plan

The essay will discuss main issues in two parts:

Part One: Limits of anticipatory in the Use of Cyber Attacks.
Part Two: A Legal Approach between anticipatory and Cyber Attacks

Part One: Limits of anticipatory in the Use of Cyber Attacks

In the beginning, it must be said that, through a review of the rules of International

Humanitarian Law, we did not find an explicit definition of the term "anticipatory".

Accordingly, the concept of "anticipatory"can be traced back to the relevant customary rules, including those governing the use of the feasible precautions mentioned in rule (15), as well as the practice of States, like Belgium's Law of War Manual, which define it as "Everything possible must be done to avoid incidental damage to civilian objects and loss of civilian life (Henckaerts, Doswald –Beck, 2006, p15)

Therefore, we attempt to define the anticipatory as "the mental perception associated with a decisive logical prediction of the magnitude of the effects that will result from the use of a means or method of combat which is based on material and legal facts before the moment of implementation at a very short time".

As for Cyber-attacks known as a "cyber-attack aimed at controlling electronic sites or electronic-protected infrastructure to disrupt, destroy or damage them (Kissel, 2013, p 57) in this regard It does not focus on information gathering (Lewis, 2010, p 56)but on a military side (Al-Fatlawi, 2018, p 13) against energy systems, transportation, and all electronic services (Lynn, 2012, p 518)

01 .Predetermined degrees of anticipatory of the cyber-attack and its conditions

In reading the International Humanitarian Law, it is clear that anticipatory get grades and conditions:

A- Grades of anticipatory of cyber attack

At this point we will try to discuss situations that can be determined by anticipating:

A-1-A: Pre-Probability anticipatory

By which we mean every anticipatory effect of the cyber-attack occurs when there are (probability) indications of its existence, Articles (35), (55) & (57) of Additional Protocol I of 1977. Therefore, the word (may be expected) indicates that the probability projection is sufficient to avoid attack (Abdel-Sadiq, 2007) the text of each article was limited to the mere possibility of incidental damage.

A-1-B: Possible Anticipatory

We mean the anticipatory expectation that - and not imperatively - can be caused by the cyber-attack, Article (15) of Additional Protocol II of 1977 ". Therefore, the phrase (may be expected) and " if such attack" indicate that the cyber-attack here is reasonably expected to cause material damage or destruction to the attacking target"(Schmitt, 2013, p 92).

Therefore, the probable anticipatory in the use of cyber-attacks is that the degree of belief of its occurrence is similar to that of the belief of non-occurrence, whereas the possible anticipatory is that the degree of belief of its occurrence is greater than the belief that it will not occur.

In a similar sense, if there is an expectation supported by certain data, the use of a weapon or method of combat, resulting in injury to civilians or civilian objects in excess of the purpose of destroying a military objective, is illegal (Milan Martic, p 95).

A-1-C: Predetermined Anticipatory

We mean the certain anticipatory, as stated in the San Remo Manual on International Law Applicable to Armed Conflicts at Sea(46 (d)) throughout the phrase "if it may be

expected" this expectation in using cyber-attack is certain not just indications that it is likely to be realized

B- Legal conditions for anticipating the use of cyber attacks

There are prerequisites for anticipating cyber-attacks

A-1-A: carefully studied

Anticipatory should be carefully studied so as to provide a definitive prediction of the effects of a cyber-attack, the article (48) of Additional Protocol I of 1977 refer to this issue by this phrase (shall at all times distinguish), According to the above, the military plans prepared for the cyberattack should be studied with great care, because their effects are wider and less manageable if they occur(Abdul-Sadiq, 2017, p 8).

A-1-B: Synchronous with military certainty

Anticipatory of the use of cyber-attack shall coincide with military certainty of the legitimacy of the effects of the attack (Beirut, 2006, p. 32.).

A-1-C: The element of continuity

The boundary between the (certainty) of anticipating a cyber-attack and its entry into probability is the continuation of the same prediction. It is not true that the anticipatory that occurred when planning the cyber-attack (certainty) is predetermined at the beginning of the implementation (probability), Violations may occur in the period between planning and implementation.

02 .differentiating anticipatory from circumstantial developments of cyber-attack

There may be a sudden circumstance prior to launching a cyber-attack in a critical moment. Then, there is a difference between anticipating and situational developments:

(A) The time factors

Anticipatory begins during the planning of a cyber-attack; it may extend to execution, while circumstantial developments emerge when implementation is initiated.

B - Military Options

Anticipatory in the use of cyber-attack can be remedied and the attack is not carried out because anticipating does not appear suddenly, but with planning, while the situational developments appear in a critical point in which it is not possible to abandon the attack and remedy it. Therefore, it has a real impact or imminent occurrence inevitably.

C - Legal effects

The emergence of circumstantial developments permanently breaks the legal relationship between anticipatory and the effects of the cyber-attack, because the effects of the cyber-attack are caused by novel developments and not by anticipating, and this is an important issue.

In this regard, the Tallinn Manual has organized this subject in some detail by focusing on self-defence, and whether resorting to it may lead to an aggressive decision without regard to prior expectations and the effects that accompany such decisions, on the grounds that failure to pay attention to anticipatory, Is due to an urgent military necessity (Schmitt, 2013, p. 215).

Part Two: A legal approach between anticipating and cyber attacks

Article (36) of Additional Protocol I of 1977 is the first international step to contribute

to the review of weapons developed (McClelland, 2003) Therefore, attention should be given to the possibility of applying precautionary rules to developments.

In this regard we will discuss critical issues as below:

01: The relationship of anticipatory with possible precautions on the use of hostile cyberspace

Anticipatory occurs at a time-out when planning at a later time stage of the potential precautions mentioned in article (56: para 3) as well as article (57) of Additional Protocol I of 1977, by obliged the conflict parties to take (the precautionary measures).

However, feasible precautions are included as an element in anticipatory, including (the effect of time-cybersecurity - protection measures - alternative options - measurement of necessity when planning a cyber-attack) (Beirut, 2013, p. 402). Therefore, controlling anticipations and taking all feasible precautions is a criterion for measuring the legitimacy of the use of cyber-attacks (International Criminal Court, 1998). Rather, it is in consistent with the spirit of International Humanitarian Law, that anticipatory is predetermined to take all feasible precautions before a cyber-attack, indicating that the planners of the attack needed sufficient information (W, 2012, p. 20). because this type of warfare is based on the control of the technological dimension in the management of military operations. Thus, illegal effects may not be caused directly by the cyber-attack, but as a side-result of it, the application of Article (57) of Additional Protocol I of 1977 should be observed.

02 .The role of anticipatory in cyber-attacks in accordance with the principle of "primary considerations of humanity"

Cyber-hostile activity may be targeted at self-resolution weapons such as drones or early detection devices. However, the anticipatory is associated with the use of cyber-activity on a well-established legal principle (for the primary considerations of humanity).

The use of cyber-activity such as against civil aviation contravenes the rules governing international behavior and the primary considerations of humanity. This is the same as that contained resolution of ICAO in the 15 September 1983.

Cyber-attacks may consider a preliminary weapon for hostile operations, may directly or indirectly cause the collective or partial destruction of military targets, disrupt or destroy like communications at airports, and are considered a means of combat (Al-Fatlawi, 2018, p. 21).

Conclusion

The term "anticipatory" should be review by the International legal experts in order to adopt the distinction of "anticipatory" in cyber-attacks specifically the notion of "Circumstantial developments" of cyber-attack precisely.

We believe that "anticipatory" is a "personal element" since it relates to the issue of planning a cyber-attack other than "Circumstantial developments", which is an "objective" element. The emergence of "circumstantial developments" will lead to the lack of the legal existence of anticipatory, while the element of (surprise) is the distinction between them. According to the level of legal protection, the degree of anticipatory ranges from on the use of cyber-attacks under International Humanitarian Law. Equally, Cyber-attacks blur the boundaries between war and peace and make International Humanitarian Law subject of wide controversial with international human rights law. Because they can be launched even in

peacetime and not only in the time of armed conflict. Therefore, this has to be reconsidered as to some of the Additional Protocols of 1977 in consistent with developments in the technology of lethal warfare, specifically in cyber-attacks.

References

1. Boothby, W, (2012): The Law of Targeting. Oxford University Press.
2. James A. Lewis (2010): Sovereignty and the role of Government in Cyberspace" Center for Strategic and International Studies Journal, Spring Summer, Vol. XVI, Issue II.
3. Michel N. Schmitt (2010): Tallinn Manual on the International Law Applicable to Cyber Warfare "Cambridge University press first publishes.
4. Richard Kissel (2013): Glossary of Key Information Security Terms" National Institute of Standards and technology, U.S Department of Commerce "Revision, 2.
5. Ahmed Obais Al-Fatlawi (2018): Cyber Attacks, Legal Study on the Challenges of Contemporary Organization, Zain Publications, Beirut.
6. Herbert Lynn (2012): Cyber Conflict and International Humanitarian Law, Selections from the International Journal of the Red Cross, vol. 94 (886).
7. Adel Abdel Sadik (2007): Is Electronic Terrorism a New Form of International Conflict? Al-Ahram Strategic File, No. 156.
8. Ian Anthony (2006): Reflections on the Continuation of Arms Limitation and Change, Stockholm Institute for International Peace Research, Annual Book 2006, Published by the Center for Arab Unity Studies.
9. Antonio Cassese (2015): International Criminal Law, Human Rights Publications, Beirut.
10. Salah al-Din Amer (2003): distinction between combatants and non-combatants, an article published by a group of specialists and experts, (International Humanitarian Law - a guide for application at the national level), Dar Al Mustaqbal Al Arabi, Cairo.
11. Justin McClelland (2003): Arms Review in accordance with Article 36 of Additional Protocol I, International Review of the Red Cross, No. 850
12. Nezha Al-Madhmed(2013): Legal Regulation of Landmines in International Law, Scientific Book House.
13. Adel Abdel – Sadeq (2017): Patterns of Cyber War and its Implications for Global Security, Journal of International Politics, Cairo.
14. Protocol Additional to the Geneva Conventions of 12 August 1949, Protocol
15. Protocol Additional to the Geneva Conventions of 12 August 1949, II.
16. Rome Statute of the International Criminal Court.
17. San Remo Manual on International Law Applicable to Armed Conflicts at Sea.