International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 11, Issue 3, 2020

Dialectical Rules of Engagement in Cyber War

Abdulkareem Kadhim Ajeel[a], Kareema Lateef Abdullah[b], [a,b]College of Media /Dept.of Press/University of Thi-Qar/Iraq, Email: [a*]abdkazm@gmail.com

The study deals with the rules of engagement in cyber war, which have not yet crystallised, unlike the traditional wars. The most important thing is how to distinguish between combatants and civilians from participating in cyber war and what the limits of this distinction are, so when the hacker becomes a fighter. As a result of the great world scientific development in electronics, there is a series of important inquiries to determine strategies for military response, and how to deal with the enemy. These inquiries decide whether a country is subjected to cyber-attack or to a normal attempt of piracy, whether it is made for amusement purposes or it is a theft of accounts by some amateurs and hooligans. Also, it determines the limits of the national sovereignty of the state in cyber war, and whether the attack on websites of civilian bodies belonging to the state (government), is an electronic attack that should be responded immediately or not, and what the limits of international responsibility for cyber-attacks and others are.

Key words: *Rules of Engagement, cyber war, cyber deterrence, cyber combatant, international responsibility.*

Introduction

The great developments in technology and communication have significantly changed the nature of international relations and the form of international conflict. Cyberspace is no longer an exclusive domain of states; it is open to all, especially for non-state actors, including terrorist groups, who use this space as a platform to carry out cyber- attacks to achieve their goals. However, no legal response has yet been issued by the United Nations and its principal organ, the Security Council, or the International Court of Justice on the seriousness of cyber-attacks, which have become a daily reality that threatens international peace and security (Priyanka, 2015).

Modern technological innovations, especially in the field of cyberspace, change the traditional conception of war, and change the traditional forms of power, and introduce new concepts that never exist before, and reformulate old ones, and appear as a new type of power which is the electronic power (cyber power), working alongside with the traditional forms of it, whether hard or soft. Cyber power becomes one of the most important tools to achieve the foreign policy of States, and also the domestic policies. It is also intended that the ability of the actors (States and non-States) to use the means of modern technology and communications to achieve certain objectives through computer networks and the Internet. These objectives include theft of data, destruction, modification, closure or re-tuning of electronic systems, and they also may be civilians or militaries, private or public (Ehab).

The US government recognises the danger of cyber threats, particularly against critical infrastructure, and the Ministry of Defense officially describes cyberspace as a field of war. Also more than 140 countries have or are developing electronic weapons, and more than thirty countries are working to establish electronic military units. According to some estimates, this interest is not limited to states, but also includes non-state actors, including cybercriminals, hackers from different levels of evolution. Terrorist organisations are interested in this area and are working to develop their capabilities and resources; they are ready to use them to support heinous goals (Iasiello, 2013).

There are multiple applications and patterns of cyber war. Cyberspace is been used as a battlefield for different levels, such as the low intensity pattern, the cyber-attacks between China, the United States and Russia or between South and North Korea or Iran and the United States can be such a model. While the other type is the medium-intensity pattern, where cyberspace conflict becomes an arena parallel to a conventional war this may be a prelude to military action. Examples of this pattern include the attacks during the 2006 war between Hezbollah and Israel, and cyber-attacks of the Georgian-Russian war in August 2008. The last type, the most dangerous, is called the pattern of heated cyber war and high-intensity conflict. Although the world has not experienced a single cyber war without conventional military action, there are signs of a shift in the future. This pattern of conflict is characterised by the control of the technological dimension of the conduct of military operations where cyber weapons are used only against enemy facilities, such as using drones or robots in remotely administered wars. Tools of war are being developed in the field of defence, cyber-attack and acquisition of cyber force. An example of such attacks is the cyber-breach was done by Israel in cooperation with the United States, against Iran's nuclear facilities, later known as the Stuxnet virus in October 2010.

Through different patterns and levels of cyber engagement, it is shown that the armed conflicts of this century are more diverse than in the previous two centuries. Military strategies and tactics are evolve more directly to the entire population of a country or region

because the conflict has become larger than ever before. The problem of distinguishing between combatants and civilians or protecting civilians from hostile cyber operations and deterring them intellectually remains unresolved. The Geneva Conventions and even the Charter of the United Nations are closely related to cyber measures and their field, but the attributes of this interdependence are vague and unclear because cyberspace is new in comparison to these instruments, which we will seek to highlight in this paper.

The Concept of Rules of Engagement

Rules of engagement in military science mean "those rules by which the armed forces shall obey, when force is used in the course of military operations in international, regional or national scene, whether in peacekeeping missions or in armed conflicts, therefore, when using force, the state should look at the multiple dimensions of military, operational, strategic, legal and political of the rules of engagement" (Article 35 of the First Additional). The NATO defines them as: Instructions issued by an authorised military authority that establishes the conditions and limits in which the use of force is allowed to initiate or to continue the engagement. Also, the rules of engagement are not tactical instructions to guide them, but they draw the framework for engagement, such as organising weapons or countering a hostile attack. So, the rules of engagement must be amended to provide an adequate response to any emergency (Public Service, 2012).

In conventional wars, rules of engagement are generally concerned with how to respond to the threat, the size of the force used and under what circumstances to choose the appropriate weapons to deal with the enemy, the amount of power, and the size of decision-making given to the persons responsible of the security to initiate or ceasefire. For example, what decision a military officer in charge of protecting a security headquarters can make if a suspicious man is approaching him, and how far it is the warning or direct shot at the target and others (Abbas, 2010).

The rules of engagement also mean military directives which, by describing the circumstances under which different air, land and naval forces will enter, continue to engage and fight with opposition forces, formally, where the rules of engagement refer to orders issued by a competent military authority that determine when, where and how, military force can be adopted against hostile forces. The rules of engagement are part of a general recognition that specific measures and standards are necessary to chart the behaviour and effectiveness of civilized war (Ashley Roach, 2018).

The idea of military engagement is organised with a long list of internal rules and bilateral or international treaties and agreements. The most relevant international conventions are the Geneva Conventions which regulate the treatment of prisoners of war and civilians.

Nevertheless, the rules of engagement can be considered as a modern concept necessitated by the possibility of nuclear war, progressing in communications, increasing threat or using the force in international relations for peace, security and peacekeeping (Kalshoven and Zegveld, 2011).

As for the rules of engagement in the cyber war, we point out that it has not yet clearly crystallized. In this context, there are important questions to be answered to determine the rules of engagement and how to deal with the enemy or to determine the strategies of military response. These questions decide and determine whether a country is under cyber-attack, or under normal piracy attempts, and its purpose is to entertain and steal accounts by some amateurs, fiddlers and the limits of national sovereignty of the state in cyber war, and whether the attack on the websites of civilian bodies belong to one of the state institutions considered it is a cyber-attack that should be responded to immediately (Said, 2016). Military theorist Carl Clausewitz believes that war is the use of force to restrain the enemy from doing what he wants. He adds that war is a political measure and a continuation of politics by other means. In this sense, cyber war defers to the actions made by a state that attempts to infiltrate the computers and networks of another state with the aim of causing serious damage or disruption (Yahya, 2017).

A cyber-attack is also known as an electronic operation that is reasonably believed to cause injury or fatalities, damage or destruction to objects (Michael, 2013). Thus, the nature of the elements and environment of conventional and cyber wars are very different one from the other. The reason for this difference has a great impact in defining and drawing rules of engagement. In this context, the following question arises: are the legal rules governing conventional wars and armed conflicts applicable to cyber warfare or cyber activity? There is no definite answer. However, most experts, including those of the Tallinn Guide experts, point out the need for a link between cyber activity and armed conflict to apply traditional legal norms; but they differ regarding the nature of that relationship (Schmitt).

Distinction between Electronic Actors

The most important challenge of cyber engagement is how to distinguish between electronic actors that is, between the so-called cyber-combatants and other users. This is one of the thorniest issues on which international law has not been agreed upon and are essential for the application of legal rules relating to international humanitarian law to cyber war and several questions arise in this regard, especially when the pirate / hacker becomes a warrior (Said, 2012).

The Additional Protocol I and II in 1949 to 1977 in the Geneva Convention take into account the change in means of war to a better combatants and civilians protector in both types of armed conflict. The two Additional Protocols provide for the specific situation of civilians directly participating in hostilities in both types of armed conflict (API Art. 1.45 and 3.51) (APII Art. 3.13). They affirm that these persons retain their civil status and do not lose the protection afforded to civilians by the international humanitarian law, except during the period of direct participation in hostilities (Geneva).

The Tallinn Guide (The Tallinn Manual) International Expert Group generally agrees on the three cumulative criteria for classifying an action as direct participation. Firstly; the act (or series of closely related acts) intended or actual effect of adversely affecting the operations or the military capabilities of the adversary, or death, bodily harm, physical destruction of persons or objects protected from direct attack (threshold of damage). Secondly; the direct causal link between the act in question and the intentional or inflicted damage (causation). Finally, the acts directly related to military actions (combat relationship). It should be noted that although the majority agrees with these standards, some differences of opinion on its precise application to certain procedures are identified (Text of RULE 35).

Nevertheless, the phrase "direct participation in hostilities" raises many controversies in the context of screening between the combatant and the civilian. There is no precise definition of the concept of direct participation in hostilities in international humanitarian law. The precedents concerning the exercise of states as well as the provisions of international criminal jurisdiction, do not provide any definition. This silence leaves the field of doubt open to specialists and to the judges of the international criminal courts.

The concept of "direct participation in hostilities" is based on two main elements, (Nils, 2009) being direct participation and hostilities. The first element refers to individual contribution to these processes, while the second element refers to; the collective resort of a party to the conflict to means and methods that may harm the other party, depending on the quality and the degree of individual contribution to hostilities, it can be characterised as a direct or indirect contribution. The direct participation of individuals in hostilities takes the form of spontaneous, intermittent or unregulated participation, and it may also be part of a permanent function for government forces or organized armed groups affiliated with a party to the conflict. Knowing which of the two photographs is taken by individuals is crucial to determining their status as civilians or not civilians, and the determination of the status of the individual participant does not affect the hostilities in terms of the link between this participation and the legitimacy of strikes against the participants directly. In this regard, determining the individual status of the individual involved is of value in the event of capture. If he is part of the military's, he is classified as a prisoner of war, but if he is a civilian, he

incurs to criminal prosecution, except for a collective grant against a possible invasion (Rawabji, 2016).

In general, civilians who take a direct part in hostilities retain their status as civilians, despite the fact that they are directly participating in hostilities. However, they temporarily deny the protection that covers civilians - for the duration of their direct participation (Protocol 1, Article 3.51, Protocol 2, Article 3.31) (https://ar.guide-humanitarian-law.org/content/article/5/mdnywwn/).

Those conducting hostilities already face the difficult task of distinguishing between civilians who are and are not engaged in a specific hostile act (direct participation in hostilities), and distinguishing both of these from members of organised armed groups (continuous combat function) and State armed forces. In operational reality, it would be impossible to determine with a sufficient degree of reliability whether civilians not currently preparing or executing a hostile act have previously done so on a persistently recurrent basis and whether they have the continued intent to do so again. Basing continuous loss of protection on such speculative criteria would inevitably result in erroneous or arbitrary attacks against civilians, thus undermining their protection which is at the heart of International humanitarian law. Consequently, in accordance with the object and purpose of International humanitarian law, the concept of direct participation in hostilities must be interpreted as restricted to specific hostile acts (Nils).

In this context, when one of the parties to the conflict foresees that there is an objective possibility of harm of a military nature resulting from an act of direct participation in hostilities, the requirement to reach the threshold of damage is considered satisfied regardless of the quantitative risk and loss. (Yves and Christophe, 1986) Military injury is not limited to death or injury to martials. It causes destruction with their notables, but also to any consequences that could adversely affect the actions and military capability of a party. For example, the unarmed acts of sabotage that would impede the advancement of enemy forces could be considered, and the acts that adversely affect enemy military operations, cyber and electronic hacking by civilians hackers against enemy forces falls within this concept. However, expanding in this context the negative effects of direct participation in hostilities is a characteristic of asymmetric armed conflicts (Nils).

The strongest party in unequal armed conflicts always tends to expand the concept of direct participation of civilians in military actions, beyond the physical action and the trial of hostile intentions of the civilian population. This constitutes a risk to the distinction which is established by international humanitarian law between the temporary loss of protection associated with the damage caused by these civilians to the enemy during in their participation of hostilities. During this period of participation exclusively, the permanent loss

of protection that is based on a specific function of these civilians falls within the criterion of continuing the combat function, the strongest party deals with civilians on the basis that they permanently lose their protection without providing clear and strong evidence (Omar).

Within the previous legal definition, a problem arises about the participation of civilians in cyber or even conventional war through their participation in the war using modern communication techniques to cause obstruction or harm to the enemy. Is this participation direct or indirect? This includes, for example, what becomes known as popular mobilisation of cyber or (popular e-delegation), and others. For example, during Operation Cast Lead on Gaza (2008-2009). Advocates of the Palestinian caused attack some Israeli websites in the traditional way (DDOS) and succeed in disturbing the atmosphere of the Israeli Internet for several days. On the other hand, the Israelis adopt a new method of cyber-attack based on the popular electronic mandate of unit 8200 in the IDF to enable the latter to use their devices as a centrally managed cyber-attack and employ it as a single massive electronic object that is harmed when it is attacked. This method is based on a simple principle which is that the internet penetrates under most of the popular sectors in the country around the world and the estimated number of users is in the millions if the united efforts of supporters and the public who want to participate in the cyber war and directed in one way, by obtaining a voluntary authorisation to employ their devices and subscribe to the internet by uploading a friendly virus to their devices managed by the central console. The power of the system grows dramatically, with thousands of devices representing enormous computing power and thousands of ports on the Internet representing (bandwidth) contribute to the concentration of that cyber force and put it at the disposal of a single command, contribute to the concentration of that cyber force and put it at the disposal of a single command (Badran).

Within the above description, it is evident that the international instruments did not provide a precise description of the distinction between military and civilian, especially in light of the rapid development in the nature of weapons, the mechanisms and tools of war. Although the text of the "Tallinn Guide" tried to deal with this issue, we still find it unclear about the nature of this important participation of civilians and the impact of the rules of engagement during the cyber war.

The problem remains as to whether an action can be classified as a “direct” rather than an “indirect” participation in military operations. Although some standards are established, others remain very flexible rules that would include any war effort within the concept of direct participation in hostilities. Thus, depriving large parts of civilians of the protection afforded to them by direct attacks, we believe that the most important criterion for discrimination is by understanding the direct causal relationship which means: The intended harm must be achieved in one causal step. So the notion of direct participation in military operations excludes individual conduct, which is sufficient to build the capacity of a party to

cause or maintain damage to its adversary. In other cases, it causes damage only indirectly. For example, there are acts such as imposing a pattern of economic sanctions on a party to an armed conflict, depriving him of his financial assets, or provide his opponent with goods and services. It will have a potentially significant impact, but there is also an indirect effect on that party's military capability or operations (Nils).

Therefore, the simple participation of civilians cannot be considered as having a significant impact on cyber operations by direct participation in hostilities, unless its effect is direct and achieved in one causal step. Otherwise, these actions fall into indirect participation, (such as the above example, which can be measured), during which a civilian does not lose the protection.

International Responsibility for Cyber Attack

Due to the lack of formal legal adaptation, particularly from the United Nations, and to the causes of Siberian war, several jurisprudential studies emerge to address the issue of cyber-attacks, and the Tallinn Guide is the most prominent. Tallinn experts decide that the distinction between cyber breakthroughs and other activities, like espionage or psychological war, and cyber-attacks, are violent acts that may cause harms for purposes that aim at either individuals or installations. The magnitude of the damage intended herein is serious damage, i.e. serious damage to installations or individuals, and the attack on a facility may cause serious damage, such as disruption or destruction of dam systems that cause flooding. The limited harms of Siberian attacks whether installations or individuals are so little compared with us other harms. Therefore, the intended "harm" should not be limited to acts of violence or kinetic force attacks, as established in the law of armed conflict, in the violent effects of non-motor weapons such as biological and chemical weapons and, of course, cyber-attacks. The harmful effects of the latter, whether military or civilian, or causing civilian casualties or injury, are according to Tallinn experts, an "armed attack." (Michael, 2013) Some go further, as every external operation aims at massively blocking the Internet is a military act (Moro, 2010).

In this description, the provision of equipment and training by a state for the purpose of cyber-attacks against another State is considered an unlawful use of force, as it contradicts the purposes of the United Nations, particularly Article 2, paragraph 4. Although the article is flexible, its content could be expanded to include cyber-attacks or capacity-building to threaten international peace and security.

The right to self-defence is one of the most important rights enshrined in international law, as it is addressed in the UN Charter in Article 51, and in the context of cyber warfare, there is also such a right, in accordance with the same controls applicable to defence in general which

are proportionate to the reaction to attack to inform the Security Council, to assess the extent of necessity, and the ability to determine the absolute attack. This is what states must take into account in the implementation of any cyber-attack. In addition to adhering to the relevant rules of international humanitarian law also when launching cyber warfare, one of the most important pillars of this law is to observe the principle of humanity, which requires the respect of human dignity and protection in all cases. Also, military necessity must be assessed, as this electronic weapon must be used only to the extent necessary to achieve the purpose of the attack (Munira, 2016).

In this context, we can talk about the legitimacy of military intervention as a defence against the cyber-attack. By applying the principle of proportionality, it will be difficult to use military force and move the armies of the state because of the cyber-attack. Here, the question arises: What if this cyber-attack touches military installations or hacks electronic devices to control strategic weapons? Is it possible to resort to military defence in this case? However, the response to the use of military force requires adherence to the rules of force used by the rules of international law. One of the most important controls is to establish the rate of aggression of the state accused of the attack, as it is difficult to provide convincing evidence that identifies the source of the cyber-attack. Anonymous users make it hard to prove absolute attacks. If they do so, it can take a long time and could lead to the wrong source. For example, an attacker could hack into an innocent person's device and make those attacks appear to have come from that person. Therefore, must check and assign a categorical point to the perpetrator of the attack (Yahya).

Among the issues that also arise in cyber war is the difficulty of distinguishing between civilian and military targets. In cyberspace, civilian agencies may interfere with the military, such as the use of Internet and communications equipment to deliver logistical supplies to civilians, Global Positioning (GPS), which is linked to satellites by civilians and military. In this context, one must be aware of the accidental damage resulting from the targeting of hostile military points, which may indirectly lead to civilian damage such as cutting off power supplies and water. The issue of cyber security raises many issues within the framework of international law (Munira, 2016).

First, are cyber-attacks classified as acts of aggression that threaten the international peace and security, which the United Nations, represent by its members on the Security Council, and our which guarantees to preserve and protect? In accordance with Article 39 of the Charter of the United Nations, which states that "the Security Council shall decide whether there has been a threat to or breach of peace or an act of aggression". Therefore, only the Security Council has the discretion which determines whether the threat and damage of such attacks constitutes an aggression that threatens international peace and security, and on this

basis will decide to intervene and take the necessary measures to put an end to the event of an electronic war.

Secondly, within the framework of establishing controls for electronic use and curbing these attacks and cyber breaches, it is necessary to move internationally to conclude international conventions and treaties. For instance, a guide named "Tallinn". Russia proposes an international treaty to prevent countries from processing viruses that could be released at any moment to attack other countries' organs.

Thirdly, the identification of the aggressor and its location are very problematic in cyber war. That is, the ignorance of identity in cyberspace is a rule rather than an exception. This results in difficulty in determining the responsibility and attribution of the attack to a particular party or entity, since international law restricts the responsibilities of a party or individual. Thus, great difficulties arise where the relationship between cyber-breaches and a military conflict remains difficult to prove, and determines whether there is international responsibility in the absence attacker identity (Ben and Haidira, 2017).

So when does the accused state bear international responsibility? To answer this question, it should be noted that it is so difficult to prove the proportion of a cyber-attack of a particular country, even if the victim State is tracing it. It requires time and effort, and in most cases the source is unknown, assuming that the affected state is able to prove that a particular state cyber-attacks against it. In this case, the elements of liability are carried out and the resulting damage is assessed so that the accused State can bear the resulting consequences on the establishment of international responsibility, namely compensation if the accused part is to infiltrate and launch such attacks, individuals or groups (not a State). According to the indirect responsibility, the state is responsible of its people, in condition that it has not done enough effort to control them, and it should enact laws that criminalise such acts, set limits on electronic use, and impose penalties for perpetrators of cyber-attacks. If not, the state will be held responsible for the actions of the perpetrators of these crimes (Munira).

Although there is no explicit regulation to distinguish direct from indirect civilian participation in military operations, any military operation carried out in the event of armed conflict must comply with the rules of international humanitarian law and customary rules of engagement that govern the scope of military operations. The type and degree of force permitted to be used against legitimate military objectives, are based on two main principles (military and humanitarian necessity), which form the basis and essence of the overarching framework of all rules of international humanitarian law, defining the format in which force should be interpreted. Considerations of necessity cannot derogate from, or overwhelm, special provisions of international humanitarian law (Nils).

For example, the an unarmed civilian who sits in a restaurant and uses a radio or a mobile phone to transmit tactical information about the intended target to be attacked by the air force is likely to be considered as directly involved in hostilities, but if the restaurant is located within an area that the counterpart actually controls, the military threat posed by this civilian may be nullified by arresting him or by any other non-lethal means without endangering the occupying forces or residents in the neighbourhoods (Ibid).

Conclusion

According to what is mentioned above, it is clear to us how important it is and the necessity for the cooperation of various international and regional bodies to establish a comprehensive and binding international organisation that regulates this type of war, and the work of a treaty to prevent cyber arms. We must be fully aware of this threat to states and their citizens, and within this perception of the coming cyber war, many future questions arise within the framework of the United Nations. It is difficult to identify with the development of cyber weapons. Another future question arises regarding the ability of the United Nations adopting an electronic security measures as a form of collective security or even punitive in the absence of implementation of international resolutions.

References

Abbas, B. (2010). Cyber war engagement in the information world. Center for Cyber Government Studies (Beirut). P. 33.

Ashley Roach, J. (2018). 'Rules of Engagement', 36(1), 46–55.

Ben, S. B. and Haidira, M. (2017). Cyber attacks and countering them in the light of international law. Journal of Human Rights and Public Freedoms, published by the Laboratory of Human Rights and Public Freedoms at the University of Abdelhamid Ben Badis - Mostaganem, Issue 4, June 2017, p. 203.

Ehab, K. The possibilities of deterrence in cyberspace conflicts, trends trends magazine. issued by the Future Center for Advanced Research and Studies, No. 13, p. 48.

Iasiello, E. (2013). Is cyber deterrence an illusory course of action. Journal of Strategic Security 7, no. 1: 54. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

Kalshoven, F. & Zegveld, L. (2011). Constraints on the waging of war: An introduction to international humanitarian law. Cambridge University Press.

Michael, N. S. (2013). SCHMITT, Michael N. (Ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013., ed. by Michael N Schmitt, Cambridge (Cambridge University Press).92.

Michael, N. S. (2013). Tallinn mnnual on the international law applicable to cyber warfare (Michael N. Schmitt ed.), 106-107.

Moro, I. (2010). Systems Security and Information Networks, World Culture Magazine, published by the National Council for Culture, Arts and Literature, Kuwait, Year 28, Issue 158, January-February, p. 30.

Munira Fahad Al-Hamdan (ibid).

Munira, F. A.-H. (2016). International law position on cyber war, al-riyadh newspaper, Issue 17389, February 2, 2016. Available at: <<http://www.alriyadh.com/1124892>>.

Munira, F.A.-H. (2016). Towards rules of engagement in cyberspace, riyadh magazine, available at: <<http://www.alriyadh.com/1500661>>.

Nils, M. (2009). Interpretive guidance on the notion of in hostilities participation direct under international humanitarian law (Geneva, Switzerland: International Committee of the Red Cross ICRC), 43.

Priyanka, R. D. (2015). Use of force" and "armed attack" thresholds in cyber conflict: The looming definitional gaps and the growing need for formal U.N. Response. Texas International Law Journal, Vol. 50, Issue 2, pp. 380-396.

Public Service, (2012). 'Rules of engagement vis-à-vis international humanitarian law', 11 (1), 1–11.

Rawabji, O. (2016). 'The problematic determination of the concept of a legitimate fighter in unequal armed conflict'. Journal of knowledge published by the University of Bouira, No. 21 d. P. 182.

Said, D. (2012). 'What is cyber warfare in the light of the rules of international law. Annals of the University of Algiers 1, No. 29a. P. 124.

Said, D. (2016). The nature of electronic warfare in the light of the rules of international law. Annales de l'université d'Alger 29(2): 122-136.

Yahya, M. A.-Z. (2017). The Strategic and Legal Dimensions of Cyber War, Journal of Research and Studies, No. 23 Year 14 Winter 2017,235.

Yves, S. & Christophe, S. (1986). Commentaire des protocoles additionnels du 8 juin 1977 aux Conventions de Genève du 12 août 1949, 633.