NEW CHALLENGES FOR INTERNATIONAL LAW

Article

DOI: 10.17803/2713-0533.2026.1.35.100-135

Controls for the Use of Cyber Weapons in the Light of International Humanitarian Law: What are the International Efforts to Legally Regulate Cyber Weapons?

Tareq Al-Billeh, Shahd Morad

Applied Science Private University, Amman, Jordan

Corresponding Author —Tareq Al-Billeh

Abstract: The article analyzes the controls on the use of cyber weapons in the light of international humanitarian law. This is to show the extent to which the rules of international humanitarian law can be applied to cyber weapons. Cyberspace, in particular, is considered one of the modern fields that man has sought to develop and exploit in a way that achieves interests. Therefore, the concept of cyber weapons, the means and attacks that take place in it, and the scope of international recognition of these weapons will be clarified. The study also shows the appropriateness of the rules of international humanitarian law to be applied to these weapons. In conclusion, the authors formulate a set of results and recommendations. The most important of which is that the use of cyber weapons led to the creation and imposition of the concept of unconventional warfare that enables the conflicting parties, whether States or other parties, to launch attacks on other parties and inflict se-

vere damage on all economic and social aspects. Finally, countries must seek to find new strategies that are compatible with the special nature that distinguishes cyberspace from physical reality and with the security challenges that arise with the continuous development of technology. The international legal rules regulating wars and conflicts must be reviewed in a manner consistent with the continuous technical and technological development. The international criminal justice system must also be activated, and cyber weapons must be included in agreements related to the control of the use of weapons.

Keywords: cyberspace; electronic weapons; cyber attacks; international conflicts; international efforts

Cite as: Al-Billeh, T. and Morad, Sh., (2026). Controls for the Use of Cyber Weapons in the Light of International Humanitarian Law: What are the International Efforts to Legally Regulate Cyber Weapons? *Kutafin Law Review*, 13(1), pp. 100–135, doi: 10.17803/2713-0533.2026.1.35.100-135

Contents

I. Introduction

Cyber weapons include a series of attacks targeting the information systems of countries. These attacks are committed through cyberspace with the aim of sabotaging data or tampering with associated facilities (Al-Burhami and Ali, 2022, p. 423). Therefore, countries have begun to adopt the option of attacks that are committed through cyberspace in the framework of the wars that break out between them and other countries. It is preferred to resort to it by countries in many international armed conflicts, given that these weapons are considered less costly to countries than conventional weapons, in addition to the secrecy and ambiguity of these weapons, in order to achieve the desired goals that are inflicting serious damage on the opponent (Abdul Wahed, 2021, p. 39).

Countries, international organizations and major companies have become increasingly focusing on cyberspace to achieve their goals and interests. Websites and online programs, especially those related to the infrastructure of countries, have become a means, a tool, and a goal that they seek to own and exploit to meet their own needs (Zaruqa, 2019, p. 1020).

The problem of the study lies in the fact that there is an urgent need for controls over the use of cyber weapons in the light of international humanitarian law, after the weapons used in wars became electronic instead of conventional weapons. However, until international controls are issued for the use of cyber weapons, we must deal with the texts of international conventions and covenants and the resolutions of the United Nations (UN) represented by the General Assembly and the Security Council relevant to the subject of this study. There is an urgent need for the international community to intervene in order to call for codifying some rules and controls for the use of cyber weapons in the light of international humanitarian law.

Therefore, through this study, we will try to answer the main questions that represent the problem of the study, namely: What is meant by cyber weapons? What are the international efforts to legally regulate cyber weapons? To what extent is it possible to apply the rules of international humanitarian law to cyber weapons? Have clear rules been codified to regulate the use of cyber weapons?

The study aims to explain what cyber weapons are, identify the available means and capabilities to confront them, demonstrate international efforts to organize international conventions and charters for cyber attacks and their weapons, clarify the criteria for determining legitimate military targets during cyber attacks in international humanitarian law, and demonstrate the applicability of the rules and principles of international humanitarian law to attacks in which cyber weapons are used, especially since the use of cyber weapons to launch military operations has turned the laws of armed conflict upside down.

The intended targets of any attack using cyber weapons are likely to be civilian rather than military and will affect the civilian population rather than the military forces. The study also aims to review applied cases of cyber attacks in which cyber weapons were used and occurred in and outside the context of the armed conflict.

The issue of controls over the use of cyber weapons in the light of international humanitarian law is one of the modern and important issues that has a significant impact in practice. In this study, we will examine this topic in an in-depth and extensive manner. We will pay our attention to all aspects of the subject both theoretical and practical.

The importance of the study lies in addressing the increase in cyber attacks in recent times and the difficulty of determining who issued these attacks and the lack of a legal basis regulating them. The study addresses a recent topic that is still in the process of evolving and sheds light on the concept and exceptional nature of these attacks. In addition, the study analyzes the rules and principles of international humanitarian law to examine their applicability to cyber attacks, and to evaluate this applicability to applied cases of cyber attacks that actually took place on the ground.

In this study, the comparative approach will be followed for the diversity of the General Assembly and Security Council resolutions, in addition to the international conventions and covenants that differed in dealing with sections and topics included under this topic, explaining the differences between them, and knowing the strengths and weaknesses of the various directions and the extent of their adoption. This will be done by reviewing what cyber weapons and cyber attacks are and analyzing the rules and principles of international humanitarian law in order to assess their applicability to cyber weapons and cyber attacks.

This study also requires an analytical approach to analyze all texts of international conventions and covenants and the UN General Assembly and the Security Council resolutions that are relevant to the subject of this study. This is in order to identify its contents, implications and goals, and to criticize and comment on it.

The critical approach will also be followed, to highlight the opinions and trends of jurisprudence in the issues that have been taken, and the critical side of the researcher for each side that has been taken by the jurisprudential approach. The study required the use of several research approaches due to its complex nature between international conventions and covenants, United Nations resolutions, and jurisprudential opinions and trends.

II. What are Cyber Weapons?

The wide electronic revolution in the field of cyberspace weapons led to the emergence of modern weapons. The weapons used in wars are no longer the traditional weapons, but rather they are committed

with completely different weapons in terms of form and content (Amar, 2019, p. 137).

Therefore, cyberspace wars have emerged, which have rules of engagement that differ in content from conventional wars. Cyber weapons do not aim at destroying the military equipment of hostile countries, nor to seizing and occupying the territory of other countries, but rather to inflict severe damage on the infrastructure of hostile countries at the lowest possible material costs (Farhat, 2019, p. 92).

II.1. What is Meant by Cyber Weapons?

Cyber weapons constitute one of the most important forms of conflict in the information age. These weapons are characterized by the fact that they work to destroy hostile parties, such as espionage. Its repercussions are very serious by destroying the important websites of the State by introducing viruses to harm those sites (Shloush, 2018, p. 189).

The information revolution in the world has led to the creation of an environment for cyberspace with the existence of what can be called cyber power through the development of cyberspace weapons that have a great impact on the whole world. Cyberspace has become the site of conflict between States, rather than a territory being the site of conflict. This provided cyber weapons with an active role at the international and local levels (Ghoneim, 2019, p. 260).

II.1.1. Definition of Cyber Weapons

What is meant by cyberspace is "a group of computer networks in the world, and everything that these networks are linked to and controlled by. It is not limited to the Internet, but rather includes many different computer networks. Therefore, cyberspace constitutes the computer networks that manage the activity of States, their institutions, facilities, and everything related to the military and civil sectors" (Farhat, 2019, p. 93).

It must be noted that the use of intelligence in the military industries led to the development of combat systems of an automatic nature independent of human intervention. Its capabilities often exceed the

limited capabilities of humans in terms of its use in managing various battles, detecting external threats, using various weapons, collecting and analyzing information in a way that serves the military position of countries (Abdul Hamid, 2020, p. 3128; Al-Billeh et al., 2024a, p. 851).

In this context, there is no unified international agreement on a specific designation for cyber weapons. This issue is still the subject of wide discussion among countries, due to the high technology enjoyed by these weapons, which differ from conventional weapons in terms of their technical nature. Therefore, it has been called several names such as lethal autonomous weapons, automatic weapon systems, unmanned and autonomous military systems, autonomous killer robots, and lethal robotic weapons. However, the common factor between these definitions is that it is a weapon system that can choose the targets that are monitored and attack them independently (Abdali, 2008, p. 286). Perhaps it is useful to emphasize that the International Committee of the Red Cross has used the term "automatic weapon system" as a term that includes all types of autonomous weapons, whether those weapons are on land, at sea, or in air (Abdel-Sabour, 2017, p. 6).

On the other hand, the US Department of Defense has defined cyberspace as a wide range of man-made technical weapons and that its military operations mix issues of geography, sovereignty, law, and civil rights in ways that transcend traditional legal boundaries. They must be approached in a different way (Abdel Hamid and Atef, 2015, p. 62).

It must be emphasized that there is no specific definition of weapon. The term is sufficiently common in usage and treatment under international law. A weapon is "something designed with the primary purpose of killing, maiming, injuring, damaging or destroying." This appropriate definition of conventional weapons can also be used as a definition of cyber weapons to ensure compliance with international law, particularly in the absence of clear guidelines in cyber operations. It might make sense to align definitions related to cyber operations with definitions used in conventional military operations (Al-Mubaideen, 2020, p. 72).

As a result, a cyber attack must be defined as an electronic operation using a cyber weapon. In the same regard, an electronic attack can

be defined as "a process in which electronic means are used for the purpose of killing, maiming, injuring or destroying" (Al-Busaili, 1990, p. 86). This would clarify when the laws of war apply to cyber operations and open up discussion about issues surrounding them that fall short of the use of force, which constitute the vast majority of cyber operations that take place today and are done without coherent rules to control behavior (Al-Billeh, 2022b, p. 7; Schmitt, 2017, p. 245).

Although there are advantages to defining a cyber weapon, there are also potential drawbacks to this definition. A stricter limitation of electronic weapons would obviate the need for most legal reviews prior to operational planning (Belqziz, 1989, p. 17). Although legal review is required before any electronic technology can be used in a process to address potential violations of international law, conducting post-legal review wastes time and resources in developing that technology. This can be addressed by consciously reviewing the methods of electronic warfare and the legality of distributing harmful cyber capabilities and stopping uncontrolled random distribution and deeming it illegal (AlSadiq, 2016, p. 28; Al-Billeh et al., 2024b, p. 339).

Therefore, it must be taken into account that the in-depth analysis of the definition of cyber weapons is intriguing, given that the Internet is the only area of military operations in which the State can directly cause significant material damage to the opponent or enemy without the use of weapons. Operational legal review will continue to address concerns of international law whether those concerns arise from the means used, the method adopted, or the proportionality of the means and the goal. It is the intention and effect of the process that will govern its legitimacy. Cyberspace is unique enough to justify this finding to some extent (Abdul-Ghaffar, 2016, p. 32).

II.1.2. Legal Nature of Cyber Weapons

At the outset of the discussion about the legal nature of cyberspace weapons and the possibility of applying the rules of international humanitarian law to them, we must determine the jurisprudential and legal adaptation of this issue in terms of the legality of cyber weapons in the light of international law. Contemporary rules of interna-

tional humanitarian law do not prohibit the use of electronic weapons (Al-Fatlawi, 2016, p. 613; Al Makhmari et al., 2024, p. 94).

Moreover, the use of cyber weapons is considered an illegal act: "States are prohibited in their international relationship from threatening to use cyber weapons against each other or political exploitation of any State or any act inconsistent with the purposes of the United Nations" (Abdul Rahman, 2020, p. 19). Perhaps it is useful to emphasize that the traditional legal texts are no longer compatible with the weapons of cyberspace. This requires the intervention of the international bodies to enact modern laws to confront such weapons, preserving the principle of criminal legality, while strengthening international cooperation to combat them (Hilali, 1997; p. 23).

Therefore, it must be taken into account that cyber security has become an important strategic weapon for countries, especially the superpowers. Electronic weapons have become a new method and part of modern tactics for attacks and wars between countries. Whoever has an electronic weapon strategy will create a balance of terror for him or use it as a deterrent weapon to achieve peace (Al-Burhami and Ali, 2022, p. 428).

From this point of view, the Statute of the International Criminal Court indicated that: "No weapon, missiles, materials or methods of warfare that by their nature cause unnecessary harm or suffering in violation of the international law of armed conflict should be used." To conclude from the foregoing, it is noted that this text was general, aiming not to use any potential advanced electronic weapons manufactured in the future, in terms of modern technology, in the manufacture of weapons of war. To clarify this, it can be said that electronic weapons based on advanced modern technology fall into the category of prevention, prohibition and criminalization according to the rules of the International Criminal Court System (AlSadiq, 2016, p. 38; Alkhseilat et al., 2024, p. 725).

Therefore, it was necessary to examine the extent of the legality of using electronic weapons in the field of international relations. When these electronic attacks are considered a legitimate right in the case of defense, or an illegal violation in the case of a threat or damage to international peace and security, in addition to the role of international

and regional organizations and States in confronting such electronic attacks without prejudice to the basic rights and freedoms stipulated in international covenants and the constitutions of local states (Al-Sadiq, 2006, p. 22; Al-Billeh, 2022b, p. 13).

II.2. Extent of International Recognition of Cyber Weapons

The increasing and wide spread of technical knowledge and its distribution without technological hindrance has led to the proliferation and development of cyber weapons of strategic weight. This matter constituted a threat that outweighs many of the national efforts that have been made and are still being made to try to secure cyberspace and make it available to all (Abdul Sadiq, 2017, p. 33).

Perhaps it is useful to emphasize that cyberspace differs from the space in which we live. It confirms the inability to be absolutely equal between traditional and electronic space. This leads, as a result, to differing jurisprudential opinions regarding the scope and possibility of subjecting cyber weapons to the provisions of international humanitarian law (Khalifa, 2014, p. 22). Some of the jurisprudence went to say that the rules of international humanitarian law apply to cyberspace and that they are sufficient to regulate the use of electronic weapons. They do not backup the supporters of the trend that there is a legal vacuum in cyberspace (Ni'ma, 2018, p. 27).

At the outset of the discussion on subjecting cyber weapons to international humanitarian law, the legal advisor of the International Committee of the Red Cross affirmed that international humanitarian law applies to cyber weapons and cyber conflicts. Its norms are considered applicable to deal with the new developments caused by cyberspace (Abdel-Sabour, 2017, p. 6; Al-Khawajah et al., 2023, p. 32).

The fourth paragraph of Art. 2 of the Charter of the United Nations (1945) affirmed the prohibition of resorting to or threatening of force by state parties in a manner inconsistent with their purposes. This means that the weapons used in cyberspace are considered weapons in the intended sense and have a devastating effect on the physical world. The use of force and weapons against a country constitutes the national right of the attacked State to defend itself. This confirms the need to

implement and respect it without the need to include new legal rules (Ni'ma, 2018, p. 16).

The use of weapons in cyberspace by a country against another country constitutes an act of aggression without counting or limiting the type of weapons to a specific scope. This was confirmed by the text of Art. 51 of the Charter of the United Nations, which authorized the right of defense and the use of force to respond without specifying the type of weapons.

In sum, what the proponents of this opinion inferred is that both conventional and electronic warfare are similar because the effects of each are devastating and reflected on the physical world. Also, Art. 51 did not specify or restrict the type of weapons, which confirms that all disputes that occur are covered by the rules of international humanitarian law. European and American jurisprudence tended not to consider cyberspace among the areas subject to the provisions of international humanitarian law. This leads as a result to making all acts practiced in it permissible so that individuals may practice hostile activities and actions without being subjected to any rules or self-restraint.

This jurisprudence supports the argument that access to the virtual world is through keyboards, computers, and passwords. This means that they cannot be limited to the scope of a specific country. It follows that they are not subject to international humanitarian law, given that this law itself was unable to determine the rule of airspace (Abdul Hamid, 2020, p. 3129).

From this point of view, the idea of the setters of this trend is based on refusing to deal legally with the Internet and cyberspace on the grounds that it is a new world that is not compatible with the traditional physical reality. This leads as a result to the non-applicability of legal rules in international humanitarian law and international conventions to cyberspace weapons. It did not include legal rules suitable for virtual reality. In addition, the application of the rules of international humanitarian law seems unrealistic, given that the means and weapons of cyberspace are not considered sufficiently clear and understood in terms of their use and implications (Abdul Sadiq, 2017, p. 33). It is noted from the foregoing that the users of electronic weapons do not have a fixed place or a place that shows that the attack or the use

of weapons was carried out by them, especially in the event that anonymous and encrypted communication technology was used to hide their identity (Abdul Salam and Al-Atabi, 2018, p. 60).

This means that the proponents of this trend refused to apply the provisions of international law and international humanitarian law to weapons and conflicts in cyberspace, because the actions resulting from them are not considered conflicts or weapons in the true sense and are not subject to the rules of war. They also emphasized that the application of the rules of international humanitarian law requires regular armies, battlefields, confrontation, and actual weapons, unlike the case in cyberspace (William, 2011, p. 38; Haataja, 2022, p. 236).

III. Applications of Cyber Weapons in the Light of International Humanitarian Law

The possibility of applying the principles and rules of international humanitarian law regarding the use of cyber weapons, their application in relation to cyber attacks differs from that in conventional attacks by determining who bears responsibility for illegal acts, especially with regard to individual criminal responsibility. Therefore, it was necessary to set rules consistent with the nature of attacks in which cyber weapons are used during international armed conflicts (Saud, 2018, p. 82).

III.1. Extent of Subjection of Cyber Weapons to the Provisions of International Humanitarian Law

Technological developments in weapons have led to the emergence of new means and methods of warfare, such as cyber weapons. This has raised legal challenges, so it is important for any State, when developing a new weapon or method of weapon use, to assess that those weapons comply with international humanitarian law. The application of pre-existing legal rules to technology using new electronic weapons may raise questions about the adequacy of the rules of international humanitarian law in light of the characteristics of those weapons (Abdul Wahed, 2021, p. 26; Dwan et al., 2022, p. 49).

III.1.1. Subjection of Cyber Weapons to the Provisions of International Humanitarian Law

International law has recognized many principles related to the use of various forces in international relations. However, it meant by force the hard power that includes the use of conventional weapons in all its forms during international and internal conflicts. However, in light of the technological development and the communication revolution that prompted us to search for the possibility of reconciling the will of the legislator with what was imposed by evolution (Czosseck and Podins, 2012, p. 17).

Perhaps it is useful to emphasize that the principles related to international law in most armed conflicts, whether of an international or non-international nature, are characterized by a general customary and peremptory nature. It is distinguished by the fact that it applies to all warring parties, whether they are a party to the international agreements that contain the principles or not (Abdul-Ghaffar, 2016, p. 21).

Therefore, there are many principles that guide the parties, including the principle of the right of belligerents to use the methods and means of warfare that are not prohibited, and the related prohibition of the use of weapons that cause "superfluous injury or unnecessary suffering."[1] The other principle is the distinction between combatants, civilians, military objectives, civilian installations, and installations of a dangerous or dangerous nature (Abdul Rahman, 2003, p. 27; Al-Burhami, 2022, p. 423).

Based on the above, the general rule in international humanitarian law is based on Art. 35(1) of the First Additional Protocol of 1977 to the four Geneva Conventions of 1949[2]. It states that: "The right of the Parties to the conflict to choose methods and means of warfare is not unlimited." The methods mean the methods of fighting, while the means are the weapons and equipment placed at the disposal of the combatants of the parties to the conflict.

[1] Art. 35(2) of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

[2] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

From this point of view, international humanitarian law dealt with weapons and their use according to three levels represented in the general principle. This principle is based on defining the general principles as the comprehensive framework for controlling the gaps that any agreement overlooks, present or in the future. This is embodied in the Martens clause contained in the Preamble to the Hague Conventions (1907). Article 1 stipulates that civilians and combatants in cases not provided for in this protocol or any other international agreement shall remain under the protection and authority of the principles of international law, as established by custom, humanitarian principles and the dictates of public conscience.

This matter is understood from it that the warring parties are governed by this text and cannot invoke the absence of a text prohibiting the use of a particular weapon. That is, in the sense that it is not entitled to use any of the weapons whose use leads to overstepping the general principles of humanity (Al-Busaili, 1990, p. 36).

Accordingly, weapons are prohibited by nature and may not be used if their use results in indiscriminate effects, massive damage, and unjustified pain. Likewise, its use leads to damage to the environment on a large scale and for a long time (Abdali, 2008, p. 288). The agreements related to the law stipulated the prohibition of weapons. These weapons were described in two parts, the first: prohibited weapons, which are prohibited from being used and mentioned clearly, as they are called by international treaties and agreements, the most important of which are chemical and biological weapons and anti-personnel and bacteriological mines. The other part is: the weapons whose use was restricted, meaning that their use was permitted on a specific scale and according to certain conditions. It was mentioned exclusively and its provisions were organized in the texts and rules of the relevant agreements and treaties (Al-Daami, 2019, p. 36).

Accordingly, the sources of international humanitarian law include a set of principles, customs and rules of a customary nature that are binding on all. As a result, weapons which are permitted to be used, but which are not expressly prohibited in any convention, treaty or declaration are subject to the general principles (Al-Dabbagh, 1997, p. 66).

In the scope of cyberspace, the weapons and attacks that take place within it raise many problems. Among the most important of them: the extent to which weapons and attacks are subject to general principles because they do not include violence in the traditional sense? The answer to this question requires first defining attacks according to what was stated in Art. 49 of the First Additional Protocol, which defined them as: "Acts of violence against the adversary, whether in offence or in defence." It is understood from this matter that general principles and international humanitarian law apply to weapons and attacks committed in cyberspace due to their security repercussions. International humanitarian law is applied if attacks aim to kill and destroy. It must be noted that it is carried out differently from traditional attacks. That is, it takes place according to different methods and through a different medium that greatly affects communication systems and entails many political, economic and social repercussions.

III.1.1.1. Appropriateness of the Basic Principles of International Humanitarian Law that Govern Cyberspace Weapons

Force is one of the means permitted by international law to be used as one of the means used to resolve international disputes. Force is one of the manifestations upon which the State relies to highlight its sovereignty. As a result, international law is based on the organization of force in wars. However, the use of force between States in conflicts led to many dire consequences that harmed humanity. This prompted the international community to limit their use and consider them internationally illegal (Al-Dulaeen, 2014, p. 37).

In this context, by relying on the provisions of the Charter of the United Nations, its Member States should seek to resolve their disputes by peaceful means. They shall refrain from using or threatening to use force against the integrity of other States on the political or economic scale in a manner that is contrary to the purposes of the United Nations. It is not permissible to resort to force except in the case of legitimate defense according to specific controls (Al-Fatlawi, 2016, p. 612).

Therefore, jurisprudence went in two directions in interpreting the term "force." The first is based on the interpretation of force in the narrow domain. This matter excludes cyber weapons from the text of Art. 2(4) of the Charter of the United Nations, and that their use does not fall within the scope of the ban. This is based on what was stated in the Preamble of the UN Charter, which stipulated that "armed force shall not be used, save in the common interest." In addition, Art. 44 stipulates: "If the Security Council decided to use force, then it would have accepted a request from a member not represented in it to provide armed force." In other words, the term "force" does not include weapons used in cyberspace. The other direction of jurisprudence went to the fact that force includes all forms and types, whether armed or economic. Article 2(4) of the UN Charter clarified the prohibited forms of force that are directed against territorial integrity or political independence or are inconsistent with the purposes of the United Nations. As we mentioned in the previous chapter of the study, force includes the use of weapons in cyberspace (Shata, 1986, p. 67).

Thus, it turns out that the consequences of attacks and weapons used in cyberspace are similar to the results of conventional attacks. However, the difference between them is in the means and strategies used in implementation. In other words, attacks and weapons in the virtual and realistic ranges result in material losses (Al-Mubaideen, 2020, p. 16).

This requires that attacks in cyberspace are based on waging psychological warfare, competition for information, and continuous work to develop and invent cyberspace weapons. This underscores the resulting diversity in the means of warfare and conflict in the hypothetical domain. Diversity was not limited to the means, but also included the actors in this war. Terrorist groups or companies working in information technology, as well as individuals and governments, may participate in the conflict. This leads as a result to the creation of the so-called open war that continues to develop methods and weapons of war (Al-Sadiq, 2006, p. 96).

From another angle, international humanitarian law is applied in cases of the outbreak of armed conflicts. In its application, it is based on activating two types of rules. The first type works to limit the ability

of the parties to use the means and methods of war, and the second presupposes that there are rules to be applied to protect people and property in times of armed conflict (Al-Shammari and Ismail, 2020, p. 277).

Thus, the use of force is not free and without observance of restrictions and controls. Failure to specify the nature of military activity does not mean freedom to use force. International humanitarian law has imposed rules on military activity that prohibit the use of certain types of weapons because of the unwarranted harm they cause. One of the basic rules of international humanitarian law recognized that in the event of an armed conflict, the parties have the right to choose the means and methods of fighting. However, this choice is specific and not absolute. It must be done in accordance with the rules of the law (Al-Sheikh, 2019, p. 248).

III.1.1.2. Conditions must be Met for the Application of International Humanitarian Law to Cyberspace Weapons

It should be noted that although most countries sought to develop legislation to combat the non-peaceful use of cyberspace, they still failed to provide effective protection because the legal framework in each country is not applicable in other countries (Al-Shuaibi and Al-Naqeeb, 2022, p. 538). As a result, in order to be able to apply international law to cyberspace weapons, a set of limitations must be available. These limitations are represented in the fact that electronic weapons and attacks that take place in cyberspace are a means of warfare, even if they do not result in the same damages and injuries resulting from conventional attacks (Al-Tai, 2018, p. 18).

In addition, the harmonization of weapons with the spirit of international law requires States to accept interpretations related to armed conflict and attack in a manner commensurate with the development in attack mechanisms and tools. Otherwise, it will make it difficult to apply international humanitarian law to cyber weapons (Amar, 2019, p. 136).

Electronic weapons target many protected facilities and places. Thus, the act resulting from it can be considered an attack in a way that leads to an expansion of the scope of war goals so that we can apply international humanitarian law to it (Ashour, 2018, p. 33). Cyber

weapons are also based on testing the concept of war in its traditional sense. This is a result of the disagreement over the concept of attack, even if space weapons include it (Bougrara, 2018, p. 101). Moreover, the application of international humanitarian law is limited. This is as a result of the use of cyberspace by civilians without creating specific limits separating their use of it from the use of States. This means that there are no limits to the extent of civilian participation in hostilities committed in cyberspace. This will lead to the weakening of international humanitarian law (Shloush, 2018, p. 187).

Undoubtedly, in order for international humanitarian law to be used in respect of cyber weapons, several indicators must apply to the consequences of these attacks, as follows:

— severity of the attack, in the event that civilians were subjected to an electronic attack in a way that exposed them to death or severe damage to their property. In this case, it is considered a military action if the damage is minimal or similar to the use of force in its traditional form (Mukhtar, 2015, p. 23);

— immediacy, in the sense that the effects of the attack will occur within minutes or seconds through vision, as is the case in a conventional attack. As for taking work for a period of weeks or months, it does not fall within the concept of force (Berri, 2019, p. 36);

— initiation, that is, the event is a result and not a cause that is, the availability of a relationship between cause and effect (Al-Sheikh, 2019, p. 249);

— subjecting the action to measurement and observation, in the sense of being able to measure the size and amount of material losses resulting from the use of weapons (Al-Dabbagh, 1997, p. 37);

— penetration, that is, if the act of using weapons is accompanied by an illegal violation of international borders, whether this is done on institutions or installations (Al-Dulaeen, 2014, p. 17);

— ability to impose the legitimacy of work, in the sense that States can assume legitimacy and their ability to monopolize legal use (Abdel Hamid and Atef, 2015, p. 37);

— responsibility, for the State to be responsible for the consequences of using weapons in cyberspace on the grounds that it is a military action and to bear its legal obligations (Belqziz, 1989, p. 33).

III.1.2. Non-Subjection of Cyber Weapons to the International Humanitarian Law

International law envisages many possibilities that include the course, results and effects of conflicts between States. This prompts us to discuss the possibility of including cyber weapons into the international legal discourse, as they are in dispute. Cyberspace and the use of its weapons do not represent an attack in the traditional sense known in international law, but their use at the same time leads to injuries to persons or targets that are protected by international law (Hilmi, 1999, p. 33).

Simultaneously, the use of weapons in cyberspace results in many attacks that affect countries and individuals in one way or another. The scope of impact differs from attacks in their traditional sense. This constituted a temptation for the conflicting parties to push them to resort to and use cyberspace weapons on the grounds that they contribute to the receding of the effects of aggression. The nature of cyberspace and the restrictions imposed on countries in relation to the nature of the international communication and information network subject them to safety and protection standards in a way that may conflict with the management of their internal affairs. This was confirmed in the decision of the International Court of Justice regarding Nicaragua (Wardana et al., 2022, p. 453).

The application of international law collectively as a legal system, especially international humanitarian law, faces many problems; given that cyberspace is a networked world that transcends international borders and national sovereignty. This made the subject of defining the concepts of peace and security in this scope undefined. Since the damage resulting from the use of weapons is not tangible and material, neither *jus in bello* nor the law of Geneva, which aims to protect civilians, can be applied to this attack. Therefore, the issue of determining legal responsibility for these attacks is considered one of the issues that cause problems (Abdul Salam and Al-Atabi, 2018, p. 62).

In addition, the non-applicability of international humanitarian law is due to the difficulty of identifying the attack in cyberspace re-

sulting from the use of its weapons, so it is difficult to distinguish the parties if the attacks were just a reaction, or if the cyber attack was carried out by more than one country. This requires concerted international efforts and cooperation to work towards a global agreement that contributes to providing protection against cyberspace weapons. This is achieved by working to activate existing international agreements or concluding new agreements (Farhat, 2019, p. 90).

Thus, it turns out that it is difficult to apply the provisions of international humanitarian law to cyber weapons in light of the lack of acceptance of the multiple existing interpretations to explain the concept of conflict and force. Also, narrowing the concept of war aims leads to the inability to apply international humanitarian law to weapons used in cyberspace, especially since they were not considered traditional means of war (Samesim, 2010, p. 39).

As a result, many international efforts have been made to limit the use of non-conventional weapons, especially those intended for use against mankind. This necessitated the conclusion of many agreements and the establishment of organizations. By applying the same principle to cyber weapons that are directed and used to harm the global information infrastructure, civil interests and the global economy, it is necessary to seek to limit the use of these weapons (Perlroth, 2021, p. 16).

In this context, the principle of the operation of these weapons is based on harming the security of space in a way that affects the capabilities and production of countries. Its danger increases in the absence of a legal and regulatory framework that defines and controls the basis for the use of weapons in cyberspace (Zaruqa, 2019, p. 1019). On the other hand, stopping the proliferation of cyber weapons and declaring that some areas are free of them depends on the will of States. These countries must take the initiative to create public and comprehensive spaces in the field of cyberspace that are free of electronic weapons based on awareness of the dangers that result from the wrong use of them, especially by non-state parties such as terrorist groups and electronic companies (Al-Daami, 2019, p. 67).

III.2. Available International Means and Capabilities to Confront the Weapons of Cyberspace

The specific system of rules of war in international law has evolved in conjunction with the development of tools and methods used in combat and armament. The increased reliance on information and communication technology in international relations and military operations led to the emergence of a new type of war and armament called electronic weapons, which took cyberspace as a special field for engagement and conflict. This matter necessarily requires providing and organizing the legal provisions related to it and framing it in a way that condemns the parties involved and establishes international responsibility for that (Al-Burhami, 2022, p. 423). From this standpoint, in order to study the international means and capabilities available to confront cyber weapons, we will study the international technical systems and international agreements related to limiting the use of cyber weapons (William, 2011, p. 16).

III.2.1. International Technical Systems to Limit the Use of Cyber Weapons

The pace of countries resorting to cyberspace has increased, considering that it is one of the areas in which conflicts between parties arise and lead to harm to enemies and adversaries. This is done by targeting communication and information networks and their associated systems, facilities, and interests of military and civilian scope (Saeed, 2013, p. 22).

It must be noted that defense systems in cyberspace are based on technical programs that are based on providing and developing programs continuously and quickly to comply with the legislative aspect of the same defense systems. This is in order for the State to secure its cyberspace from any electronic attacks that may harm its interests (Ashour, 2018, p. 38).

III.2.1.1. The Specificity of Cyberspace Weapons and their Impact on the Application of the Principles of International Humanitarian Law in the Event of Armed Conflict

The attacks carried out through cyber weapons raise many basic legal issues in terms of their legality. Especially the law of war does not include any legal text referring to cyber weapons. They are considered non-moving attacks, meaning that they are not military in themselves. As for international humanitarian law, it applies to it because its main goal is to protect civilians from the scourges of war (Abdul Wahed, 2021, p. 20).

The application of international humanitarian law must examine its ability to regulate methods and means of the new war. It is also necessary to state the illegality of using cyber weapons in the case of legitimate defense and armed conflicts in accordance with the international legal framework based on the following basic principles.

— Restricting the rights of belligerents to use weapons of war. This principle requires placing restrictions on belligerents during armed conflict to avoid any harm to civilians and facilities. Based on the provisions of the Geneva Convention of 1949, protection was granted to persons in the event of war without reference to electronic attacks and without limiting them to the use of specific weapons. According to Art. 36 of the First Additional Protocol, it is clear that any military activity that is not regulated in a precise manner does not mean that it can be used without controls and rules, and this applies to cyberspace weapons. Cyberspace weapons are directed at the opponent with the aim of causing damage to the other party. Therefore, it is considered one of the means and methods of war.

— Prohibition of unexplained pain. This principle is based on the fact that the connection between the civilian natures of cyberspace can be exposed to the damage that results from the use of cyberspace weapons that harm the economic, social and political aspects. This means that attacks and electronic weapons used in cyberspace result in excessive and unjustified pain, especially if the attacks are directed at critical infrastructure (Ghoneim, 2019, p. 262).

— Distinguishing between combatants and non-combatants, civilian and military installations. Military objectives are the legitimate objectives of war in international law. By applying this to electronic weapons, it is noted that there is an overlap between the civilian and military uses because they are linked through a single network. This confirms the difficulty of identifying military targets as targets for war, as there are no prisoners or wounded, but there are facilities and systems (Isa et al., 2022).

— Neutrality in international law. The use of cyber weapons is a violation of the principle of neutrality. The international nature of cyberspace makes any party vulnerable to attacks. Launching attacks and directing weapons is done through countries that are not involved in the conflict, so they become involved in the conflict. This constitutes a flagrant violation of the rules of international humanitarian law and the Geneva Conventions. Although countries refrain from transferring cyber weapons through their communication networks because they cause severe harm to civilians and facilities, their transfer may take place without their realizing.[3]

— Precautions during the attack and the duty of commanders in the field. The use of cyberspace is characterized by the possibility of adopting hostile activities during the attack. This requires taking all precautionary measures to avoid loss of life and material damage. However, due to the intertwining between communication and information networks, it is difficult to take the necessary precautions (Wardana et al., 2022, p. 453; Roscini, 2014, p. 137).

III.2.1.2. Scope of the Use of Weapons in Armed Conflict

International humanitarian law does not contain any express rules regarding cyber weapons or cyber warfare. This makes analyzing the legality of using this space for conflicts a matter that raises many problems, especially with the fact that the attacks are non-moving and unarmed in the actual sense. However, the application of the provisions of international humanitarian law is based on its primary objective

[3] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

of protecting civilians from any aggression and the scourges of war (Rid and McBurney, 2012, p. 9; Dinstein, 2012, p. 266).

Indicating the legality of the use of weapons in cyberspace requires a statement of international legal frameworks and their relationship to existing principles, if applied. As a result, we list the most important principles in international humanitarian law and show their compatibility with the rules of cyber warfare.

— Restricting the rights of belligerents with regard to the weapons used, by imposing restrictions on combatants in cyberspace, because the effects of their weapons may reach the impact on the work of vital installations, facilities, and infrastructure. This leads to great losses (Touré, 2011, p. 11).

Based on the fact that weapons and attacks in cyberspace aim to achieve damage, this makes them a means of warfare distinguished by its accuracy and superior ability to hit the target. As a result, it is difficult to determine the extent of legal liability. This requires activating the principle of arms restrictions (Wardana et al., 2022, p. 453).

— Prohibition of causing unjustified pain. The cyberspace of many countries depends on communication networks, information and technology that are interconnected with each other to achieve the basic goals and public interests in the country. This confirms the close interdependence between the civilian and military character in cyberspace. This means that indiscriminate attacks may hit civilian facilities in a way that causes many unjustified pains to civilians and society. Despite the different mechanisms, the effects are similar (Touré, 2011, p. 12; Khashashneh et al., 2023, p. 71).

— Prohibition of indiscriminate attacks. Despite the accuracy of cyber weapons, their technological organization may be designed in a way that makes hitting targets randomly. This leads to unjustified damage to many people, civilian and military installations. As a result, Art. 51(8) and 57 of the First Additional Protocol approved the prohibition of indiscriminate attacks that are not directed at a specific target and that use combative means whose effects are not limited to the form required by the Protocol.

— Neutrality in international law. Cyberspace crosses international borders. This makes the use of weapons a violation of the princi-

ple of neutrality. Launching the attack during it leads, as a result, to make the attacks pass through three non-involved countries (Shehab, 2000, p. 17). This constitutes a violation of the First Additional Protocol, which stipulates that: "The states and parties involved in the conflict refrain from moving forces and sending war supplies through the lands of neutral parties."

III.2.2. International Agreements Related to Limiting the Use of Cyber Weapons

The international community has sought to limit the arms race in cyberspace, as this armament encourages competition between States in a way that turns it into war; especially if the two parties possess enormous technological power that enables them to launch electronic attacks (Dahmani, 2017, p. 16).

Based on the above, the international community and States have taken the initiative to take many preventive measures of a legal nature. Thus, laws were enacted on a national scale with the aim of criminalizing entities and parties that use electronic weapons, and then arranging penalties for violators (Ponangi, 2012, p. 129). As a result, a manual known as the Tallinn Manual on the International Law Applicable to Cyber Warfare was issued in 2013. Then, a second version of it was issued in 2017, which aimed to organize and define the rules to be followed by countries when launching attacks in cyberspace. Then, several standards were issued to limit cyber weapons and for data security and integrity (Darwish, 2016, p. 121).

The Tallinn Manual 2.0 comprises four sections and represents a groundbreaking advancement that substantially enhances the theoretical and practical understanding of international law concerning cyberspace. Part I is entitled "General International Law and Cyberspace" and addresses sovereignty, due diligence, jurisdiction, the law of international responsibility, and cyber operations. Part II discusses "Specialized Regimes of International Law and Cyberspace," encompassing international human rights law, diplomatic and consular law, maritime law, aviation law, space law, and international communications law. Part III addresses "International Peace and Security and Cyber Activi-

ties" and is primarily derived from the Tallinn Manual 1.0. This section addresses peaceful resolution, non-intervention, the application of force, and collective security. Part IV delineates "The Law of Cyber Armed Conflict" within the overarching context of the law of armed conflict, specifically addressing the conduct of hostilities, designated individuals, objects, and activities, as well as occupation and neutrality. The text posits that nations' need to safeguard networks within their territory is underpinned by the concepts of universally acknowledged sovereignty and non-intervention. This section examines sovereignty as the cornerstone of international law and non-intervention as its complementary principle, assessing the applicability of these concepts in cyberspace through the relevant provisions of the Tallinn Manual 2.0. The initial rule in the Tallinn Manual 2.0 asserts, "The principle of State sovereignty is applicable in cyberspace." If sovereignty represents authority and power, as stated in the first rule of the Tallinn Manual 2.0, nations are expected to exercise their sovereignty over individuals, entities, and activities in cyberspace in the same manner that they do in the physical realm. Sovereignty in cyberspace can be viewed from two perspectives: rights-based and obligation- or duty-based. State sovereignty, as a fundamental premise of statehood, signifies the supreme power of a State regarding its territorial integrity and political independence. Given that a significant portion of cyberspace resides within the sovereign territories of States and is owned by governments or corporations within those borders, States possess authority over the information and communication technology (ICT) infrastructure situated within their national territories and explicitly affirm their commitment to safeguarding their national cyberborders. Consequently, the cyber infrastructure falls under the authority of the flag state and its sovereign rights. The physical infrastructure required for cyberspace operates on land and is consequently subject to state sovereignty (Schmitt, 2017).

III.2.2.1. Use of Cyber Weapons in Accordance with the Hague Conventions on Armed Conflicts

The Hague Conventions are a series of international agreements related to armed conflicts. Among them, the Hague Convention (IV)

Respecting the Laws and Customs of War on Land is particularly relevant, as it established fundamental rules for the conduct of hostilities between States. In particular, Art. 22 states that "The right of belligerents to adopt means of injuring the enemy is not unlimited," setting a foundational limitation on methods of warfare. However, these agreements primarily addressed conventional armed conflicts and did not include explicit provisions regarding the use of cyber weapons. They were based on the definition and regulation of the use of conventional weapons and the protection of victims in international armed conflicts (Chang, 2014, p. 379).

However, an extrapolation of their provisions shows that some of the general principles stipulated in them can be applied in cyberspace disputes. Among the most important of these principles are distinction and proportionality. The principle of proportionality states that actions that unduly target civilians and civilian property must be avoided, and that the use of weapons be proportionate to the specific military objective (Dempsey, 2020, p. 12).

International efforts aimed at trying to regulate the use of weapons and working to develop them take place within an appropriate legal framework. Examples include talks at the United Nations, the Organization for Security and Co-operation in Europe (OSCE) and the United Nations Group of Governmental Experts on Cyber security (Geers, 2010, p. 547). However, no appropriate legal framework has been put in place to regulate the use of cyber weapons. These issues are related to data protection, cyber security, and dealing with new challenges in the digital field, in order to update the applicable international laws and national legislations (Horschig, 2020, p. 352).

In the first decade of the third millennium, electronic attacks emerged. The use of electronic weapons in cyberspace has increased. This led to the emergence of the dilemma of the legal adaptation of these weapons and the extent of the ability to apply the principles of international humanitarian law to these wars and conflicts. These weapons and cyberspace did not exist during the periods in which the most important international agreements were drafted, including the first set of the Hague Conventions adopted in 1899 and the second set adopted in 1907.

III.2.2.2. Use of Cyber Weapons in Accordance with the Geneva Conventions and Additional Protocols to Them

Both the Geneva Conventions and their protocols have sought to establish the legal framework to regulate the use of cyber weapons and the legal provisions relating to cyber attacks (Bernstein, 2018, p. 133).

The Geneva Conventions and their protocols apply to cyber weapons because they violate the legal principle imposed on weapons in a conflict situation between combatants and civilians. Electronic weapons target all economic, social, political and other sectors important to civilians. Targeting these sectors causes great harm to them. Likewise, electronic weapons are not based on distinguishing between civilian and military targets, nor civilian and military installations.

This is confirmed by the text of Art. 48 of the First Additional Protocol, which stipulates, "The parties to the conflict shall work to distinguish between the civilian population and combatants and between civilian properties and military objectives. Then they direct their operations only against military objectives, in order to ensure the respect and protection of the civilian population and properties."

Also, Art. 51(2) of the First Additional Protocol proclaimed: "The civilian population, as such, may not be the object of attack, acts of violence or threats aimed at spreading terror among civilians are prohibited." The fourth paragraph in the same article stated: "Attacks that are not directed against a specific military target or those which use a method or means of combat, their effects cannot be limited as required by the Appendix. Therefore, they are liable to hit, in every such case, military targets, civilians and civilian properties without distinction."

Therefore, it is understood from the texts of the previous articles that it is forbidden for the conflict, in its traditional or electronic form, to be based on the use of indiscriminate means that lead to indiscriminate attacks. By applying the texts of these articles to electronic weapons in cyberspace, it is clear that they are characterized by a random nature. This confirms the applicability of the provisions of the previous articles to it and that it is prohibited due to its effects that may affect civilians and their interests (Zaruqa, 2019, p. 1016).

IV. Conclusion

The initial Tallinn Manual addressed the legal framework governing armed combat. The recently published Tallinn Manual, referred to as Tallinn 2.0, addresses a wider spectrum of cyber operations, encompassing both peacetime and wartime activities. This article succinctly outlines the principal aspects of the Tallinn Manual 2.0, highlighting significant areas of disagreement among the experts who authored the manual. The article provides insights into the future trajectory of international law concerning cyber activities.

The absence of specific controls on the use of cyber weapons in armed conflicts leads to many risks to international peace and security, and to the rights of civilians in the event of armed conflicts in particular. In light of the recent increase in cyber attacks using cyber weapons and the difficulty of determining who launched these attacks and the lack of a legal basis regulating them, it was necessary to put in place controls governing the use of cyber weapons, taking into account the rules of international humanitarian law.

Therefore, the rules of international humanitarian law should be applied to cyber weapons. The use of cyber weapons to launch military operations has turned the laws of armed conflict upside down. The intended targets of any attack using cyber weapons are more likely to be civilian than military and will affect the civilian population rather than the military forces. Therefore, the international community and the United Nations must work to amend the rules of international humanitarian law, especially with regard to international responsibility as a result of the use of this type of modern technology in weapons, in a way that guarantees the protection of civilians and the maintenance of international peace and security.

In fact, many countries of the world rely on cyberspace to use cyber weapons and launch attacks on opponents to harm them into submission. The international community's awareness of the importance of cyberspace and its great ability to cause damage to military and civilian infrastructure and installations has increased, especially in the light of the use of advanced electronic weapons. It has become the best choice for States as a result of its characteristics and advantages that

enable the party to the conflict to direct the strongest blows with the greatest damage and the lowest costs. Cyber weapons have become a recognized reality and cannot be overlooked or ignored. No country can escape exposure to the use of any of these weapons.

Finally, countries must seek to find new strategies that are compatible with the special nature that distinguishes cyberspace from physical reality and with the security challenges that arise with the continuous development of technology. The international legal rules regulating armed conflicts must be reviewed in a manner consistent with the continuous technical and technological development. The international criminal justice system must also be activated, and cyber weapons must be included in international legal agreements related to the control of the use of weapons and armaments to regulate attacks and weapons used in cyberspace.

References

Abdali, A., (2008). Fear industry in the media and its impact on public opinion. *Criterion Journal,* 8(16), pp. 283–300. Available at: https://www.asjp.cerist.dz/en/article/16309.

Abdel Hamid, S., and a Atef, Y., (2015). *Media and Cyberspace*. Cairo: Atlas for publishing and media production.

Abdel-Sabour, S., (2017). Cyber conflict: The nature of the concept and the characteristics of the actors. *Journal of International Politics,* 52 (208), pp. 5–10. Available at: https://www.siyassa.org.eg/News/12076.aspx.

Abdul Hamid, Y., (2020). International Legal Challenges to Regulating Artificial Intelligence — The Case of Autonomous Weapons. *Legal Journal,* 8 (9), pp. 3127–3168. Available at: https://journals.ekb.eg/article_141847.html.

Abdul Rahman, I., (2003). *Primary foundations of international humanitarian law*. Cairo: Arab Future House.

Abdul Sadiq, A., (2017). Patterns of cyber warfare and its implications for global security. *Journal of International Politics*, 52 (208), pp. 31–36. Available at: http://www.siyassa.org.eg/News/12072.aspx.

Abdul Salam, T. and Al-Atabi, M., (2018). Psychological warfare and its use in the strategy of the ISIS entity (analytical psychological study). *Inspector General Journal,* 1(23), pp. 39–123. Available at: https://www.iasj.net/iasj/article/159736.

Abdul Wahed, S., (2021). Cyber wars; A study in its concept, characteristics and ways to confront it. Master's Thesis, Middle East University.

Abdul-Ghaffar, F., (2016). *Electronic Warfare*. Amman: Al-Janadriyah for publication and distribution.

Al Makhmari, M., Al-Hammouri, A., Al-Billeh, T. and Almamari, A., (2024). Criminal liability for misuse of social media in Omani and UAE legislation. *International Journal of Cyber Criminology*, 18(2), pp. 92–106. Available at: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/420/121.

Al-Billeh, T., (2022a). Freedom of Religious Belief and the Practice of Religious Rites According to the Jordanian Legislation: Difficult Balance between International and Regional Requirements as well as the National Legislative Controls. *Balkan Social Science Review,* 20, pp. 117–137. Available at: https://js.ugd.edu.mk/index.php/BSSR/article/view/5503/4660.

Al-Billeh, T., (2022b). Legal Controls of the Crime of Publishing a Program on the Internet in Jordanian Legislation. *Pakistan Journal of Criminology,* 14(1), pp. 1–14. Available at: http://www.pjcriminology.com/publications/legal-controls-of-the-crime-of-publishing-a-program-on-the-internet-in-jordanian-legislation/.

Al-Billeh, T., Al-Hammouri, A., Khashashneh, T., Makhmari, M.A. and Al Kalbani, H., (2024a). Digital Evidence in Human Rights Violations and International Criminal Justice. *Journal of Human Rights Culture and Legal System*, 4(3), pp. 842–871, doi: 10.53955/jhcls.v4i3.446.

Al-Billeh, T., Hmaidan, R., Al-Hammouri, A. and Makhmari, M.A., (2024b). The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards. *Jurnal Media Hukum*, 31(2), pp. 333–350, doi: 10.18196/jmh.v31i2.23480.

Al-Burhami, A.R. and Ali, M., (2022). Cyberspace and Its Impact on the Concepts of Power, Security and Conflict in International Relations.

Journal of Politics and Economics, 16(15), pp. 423–430, doi: 10.21608/jocu.2022.134235.1172.

Al-Burhami, M., (2022). Cyberspace and its impact on the concepts of power, security and conflict in international relations. *Journal of the Faculty of Politics and Economics,* 16(15), pp. 423–443. Available at:https://jocu.journals.ekb.eg/article_248952.html.

Al-Busaili, J., (1990). *Electronic warfare and its impact on wars*. Kuwait: The Arab Institute for Studies and Publishing.

Al-Daami, G., (2019). *Public opinion-making from the age of print to the Internet: inherited traditions and absolute power*. Amman: Dar Amjad for publication and distribution.

Al-Dabbagh, M., (1997). *Reference in psychological warfare*. Beirut: The Arab Institute for Studies and Publishing.

Al-Dulaeen, N., (2014). *Advocacy and psychological warfare*. Amman: Dar Al-Aasar Al-Alami for publication and distribution.

Al-Fatlawi, A., (2016). Cyber attacks: their concept and the international responsibility arising from them in the light of contemporary international organization. *Al-Hilli Journal of Legal and Political Sciences,* 8(4), pp. 611–687. Available at: https://iasj.net/iasj/download/3f12bd1a72924acd.

Al-Khawajah, N., Al-Billeh, T. and Manasra, M., (2023). Digital Forensic Challenges in Jordanian Cybercrime Law. *Pakistan Journal of Criminology*, 15(3), pp. 29–44. Available at: https://www.pjcriminology.com/publications/digital-forensic-challenges-in-jordanian-cybercrime-law/.

Alkhseilat, A., Billeh, T.A., Albazi, M. and Ali, N.A., (2024). The authenticity of digital evidence in criminal courts: a comparative study. *International Journal of Electronic Security and Digital Forensics,* 16(6), pp. 720–738, doi: 10.1504/ijesdf.2024.142010.

Al-Mubaideen, S., (2020). *E-government: models, applications and international experiences*. Amman: Al-Yazuri Scientific House for publication and distribution.

Al-Sadiq, A., (2006). *Cyberpower: Weapons of Mass Proliferation in the Age of Cyberspace*. Cairo: Arab Center for Cyberspace Research.

AlSadiq, A.A., (2016). *Cyberspace and international relations, a study in theory and practice*. Cairo: Academic Library.

Al-Shammari, S. and Ismail, Z., (2020). Cybersecurity as a new pivot in the Iraqi strategy. *Al-Nahrain University Journal* 62, pp. 273–296.

Al-Sheikh, N., (2019). Psychological wars, rumors and self-destruction. *Journal of International Politics,* 218(54), pp. 248–253.

Al-Shuaibi, M. and Al-Naqeeb, N., (2022). Electronic war tongues. *Journal of Educational Sciences and Human Studies* 25(1), pp. 537–573, doi: 10.55074/hesj.voi25.544.

Al-Tai, A., (2018). Conventional wars and cyber wars, a comparative study of concepts and rules of engagement. *Journal of Legal and Political Sciences,* 16(2), pp. 5–40. Available at: https://drive.google.com/file/d/12oegM-Vvvlpms3Pk2HvfwheB6qfzK-8T/view.

Amar, O., (2019). Cyber Warfare Under International Humanitarian Law. *Dirasat: Shari'a and Law Sciences,* 46(3), pp. 134–155. Available at: https://journals.ju.edu.jo/DirasatLaw/article/view/101907/10621.

Ashour, F., (2018). The impact of cyberspace on national security. Master Thesis, Kasdi Merbah University.

Belqziz, A., (1989). *Arab national security*. Cairo: The Egyptian General Book Organization.

Bernstein, S., (2018). Reckoning with the Cyber Revolution: A Journalist's Take on Cyber Weapons. *SAIS Review of International Affairs,* 38(2), pp. 133–35, doi: 10.1353/sais.2018.0023.

Berri, M., (2019). *Cybernetics, the science of the ability to communicate, control and control.* Beirut: The Islamic Center for Strategic Studies.

Bougrara, Y., (2018). Cybersecurity The strategy for security and defense in cyberspace. *Journal of African Studies and the Nile Basin, Arab Democratic Center,* 1(3), pp. 100–120. Available at: https://www.democraticac.de/?p=56084.

Chang, N., (2014). Cyber Weapons and Transition in Security Dilemma. *Journal of International Area Studies,* 17(4), pp. 379–403, doi: 10.18327/jias.2014.01.17.4.379.

Czosseck, C. and Podins, K., (2012). A Vulnerability-Based Model of Cyber Weapons and Its Implications for Cyber Conflict. *International Journal of Cyber Warfare and Terrorism,* 2(1), pp. 14–26, doi: 10.4018/ijcwt.2012010102.

Dahmani, S., (2017). The impact of cyber threats on national security: the United States of America as a model. Master's Thesis, Mohamed Boudiaf University.

Darwish, S., (2016). What is electronic warfare in light of the rules of international law? *Annals of the University of Algiers,* 29, pp. 117–137. Available at: https://www.asjp.cerist.dz/en/article/6724.

Dempsey, P., (2020). News — Comment. View from Washington: Cyber Security — Iranian Hackers' Weapons of Muddled Digitisation. *Engineering & Technology,* 15(1), 12, doi: 10.1049/et.2020.0116.

Dinstein, Y., (2012). The principle of distinction and Cyber war in international armed conflicts. *Journal of Conflict and Security Law*, 17(2), pp. 261–277, doi: 10.1093/jcsl/krs015.

Dwan, J.H., Paige, T.P. and McLaughlin, R., (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, 3(2), pp. 49–62, doi: 10.5204/lthj.1583.

Farhat, A., (2019). Cyberspace Shaping the Battlefield of the 21st Century. *Journal of Legal and Political Sciences,* 10(3), pp. 88–107. Available at: https://www.asjp.cerist.dz/en/article/108478.

Geers, K., (2010). Cyber Weapons Convention. *Computer Law & Security Review,* 26(5), pp. 547–551, doi: 10.1016/j.clsr.2010.07.005.

Ghoneim, M., (2019). Towards an integrated model for the study of existence in cyberspace: Al-Hajrasy as a model. *Scientific Journal of Libraries, Documentation and Information,* 1(1), pp. 253–406. Available at:https://jslmf.journals.ekb.eg/article_24939.html.

Haataja, S., (2022). Nicole Perlroth (2021) This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. New York: Bloomsbury Publishing. *Law, Technology and Humans,* 4(2), pp. 230–232, doi: 10.5204/lthj.2658.

Hilali, A., (1997). *Inspection of computer systems and the accused's information guarantees*. Cairo: Arab Renaissance House.

Hilmi, N., (1999). *International law according to the rules of public international law*. Cairo: Arab Renaissance House.

Horschig, D., (2020). Cyber weapons in Nuclear Counter-Proliferation. *Defense & Security Analysis,* 36(3), pp. 352–371, doi: 10.1080/14751798.2020.1790811.

Isa, H.A., Alwerikat, N. and Al-Billeh, T., (2022). The Concept of the Public Employee in Jordanian Law: Different Constitutional, Administrative, and Criminal Law Definitions. *BiLD Law Journal*, 7(2s), pp. 331–337. Available at: https://bildbd.com/index.php/blj/article/view/318.

Khalifa, I., (2014). *Electronic force and dimension shift in force properties*. Alexandria: Library of Alexandria.

Khashashneh, T., Al-Billeh, T., Al-Hammouri, A. and Belghit, R., (2023). The importance of digital technology in extracting electronic evidence: how can digital technology be used at crime scenes? *Pakistan Journal of Criminology*, 15(4), pp. 69–85.

Mukhtar, M., (2015). *Can countries avoid the dangers of cyberattacks? Future Concepts*. Future Center for Research and Development.

Ni'ma, A., (2018). *Cyber attacks*. Beirut: Zain Legal Publications.

Perlroth, N., (2021). *This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race*. New York: Bloomsbury Publishing.

Ponangi, P., (2012). On the Offense: Using Cyber Weapons to Influence Cognitive Behavior. *International Journal of Cyber Society and Education,* 5(2), pp. 127–50, doi: 10.7903/ijcse.1101.

Rid, T. and McBurney, P., (2012). Cyber Weapons. *The RUSI Journal*, 157(1), pp. 6–13, doi: 10.1080/03071847.2012.664354.

Roscini, M., (2014). Cyber operations as nuclear counterproliferation measures. *Journal of Conflict and Security Law,* 19(1), pp. 133–157, doi: 10.1093/jcsl/krt028.

Saeed, W., (2013). *The role of electronic warfare in the Arab-Israeli conflict*. Master Thesis, An-Najah National University.

Samesim, H., (2010). *Psychological war*. Lebanon: The Cultural House for Publishing and Distribution.

Saud, Y., (2018). Cyber warfare in light of the rules of international humanitarian law. *The Legal Journal,* 4(4), pp. 80–108. Available at: https://jlaw.journals.ekb.eg/article_45192.html.

Schmitt, M.N., (2017). Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. *Harvard National Security Journal*, 8, pp. 239–282. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180699.

Shata, A., (1986). The Disobedient State: A Study of the Conflict Between States' Positions and Their International Commitments at the United Nations, with reference to Israel and South Africa in particular. PhD Thesis, Cairo University.

Shehab, M., (2000). *Studies in international humanitarian law*. Cairo: Arab Future House.

Shloush, N., (2018). Electronic piracy in cyberspace "the rising threat to the security of states". *Journal of the Babylon Center for Humanitarian Studies,* 8(2), pp. 185–206. Available at: https://iasj.net/iasj/download/bce8f50577f3c83f 185-206.

Touré, H., (2011). *International response to cyber warfare. Research on cyber security*. International Communications Union.

Wardana, A., Gunaryo, G. and Yogaswara, Y.H., (2022). Development of Cyber Weapons to Improve Indonesia's Cyber Security. *Journal of Sosial Science*, 3(3), pp. 453–459, doi: 10.46799/jss.v3i3.334.

William, B., (2011). *Cyber conflict and geocyber stability*. International Telecommunication Union and the International Federation of Scientists.

Zaruqa, E., (2019). Cyberspace and the shift in concepts of power and conflict. *Journal of Legal and Political Science,* 10(1), pp. 1016–1031. Available at: http://dspace.univ-eloued.dz/handle/123456789/5233.

Information about the Authors

Tareq Al-Billeh, PhD (Public Law), Associate Professor, Faculty of Law, Applied Science Private University; Practicing Lawyer, Amman, Jordan
t_billeh@asu.edu.jo (Corresponding Author)
ORCID: 0000-0001-7171-6004

Shahd Morad, LLM (Public Law), Lecturer, Faculty of Law, Applied Science Private University; Practicing Lawyer, Amman, Jordan
shahdmorad80@yahoo.com
ORCID: 0009-0001-1303-8337

Received 19.02.2025
Revised 14.03.2025
Accepted 26.03.2025