The Status of Cyberattacks in International Conflicts Under the Fourth Industrial Revolution

Dr. Najm Abbood Mahdi Al Samarrai *

Abstract:

The world has witnessed many industrial revolutions, the most significant of which has been the fourth industrial revolution, which has brought about substantial changes in all aspects of life owing to the accelerated development of technology and its uses at all levels. This accelerated development prompted the use of modern technologies in armaments and attacks known as cyberattacks. These attacks are based on using Fourth Industrial Revolution techniques to cripple the effectiveness of military and civilian biosystems, leading to their collapse and inflicting the most significant possible casualties on the presumed enemy.

This paper seeks to publicize the Fourth Industrial Revolution and cyberattacks, clarify the impact of such attacks on the international community, how they are confronted and absorbed in humanitarian aspects, and emphasize the quest to resolve international cybercrime conflicts in ways affirmed in contemporary international law.

Keywords: Fourth Industrial Revolution - Cyber Attacks - Cyber International Conflicts - Cyber War.

---

* Assistant Professor of International Law, Arab Open Universty, Sultanate of Oman

وضع الهجمات السيبرانية في النزاعات الدولية
في ظل الثورة الصناعية الرابعة

الدكتور/ نجم عبود مهدي السامرائي*

الملخص:

شهد العالم ثورات صناعية عديدة، أهمها الثورة الصناعية الرابعة، التي أحدثت تغييرات كبيرة في جميع جوانب الحياة بسبب التطور المتسارع للتكنولوجيا واستخداماتها على جميع المستويات. وقد أدى هذا التطور المتسارع إلى استخدام التقنيات الحديثة في التسلح والهجمات المعروفة باسم الهجمات الإلكترونية، تعتمد هذه الهجمات إلى استخدام تقنيات الثورة الصناعية الرابعة لشل فعالية النظم البيولوجية العسكرية والمدنية، مما يؤدي إلى انهيارها وإلحاق أكبر الخسائر الممكنة بالعدو المفترض.

تسعى هذه الورقة البحثية إلى التعريف بالثورة الصناعية الرابعة والهجمات الإلكترونية، وتوضيح أثر هذه الهجمات على المجتمع الدولي، وكيفية مواجهتها واستيعابها في الجوانب الإنسانية، والتأكيد على السعي إلى حل النزاعات الدولية المتعلقة بجرائم الفضاء الالكترونية بطرق يؤكدها القانون الدولي المعاصر.

الكلمات المفتاحية: الثورة الصناعية الرابعة – الهجمات الإلكترونية – النزاعات الإلكترونية الدولية – الحرب الإلكترونية – الجرائم الإلكترونية.

---

* أستاذ القانون الدولي المساعد – الجامعة العربية المفتوحة – سلطنة عمان.

Introduction:

The fourth industrial revolution (4IR) is a technological transformation affecting cultures and economies worldwide. This revolution reflects the creation and introduction of various modern technologies that drive innovations and supernatural inventions across different sectors.

Considering this accelerated development, the problem of the impact of this revolution on international security arises with Fourth Revolution techniques for espionage and cyberattacks on vital State facilities, in so-called "cyberattacks".

Cyberattacks and their consequences are at the forefront of the world's agendas. The international community's concern is that cybercrime military operations sometimes become part of armed conflicts between States and can disrupt the functioning of critical infrastructure and vital services for the civilian population.

For example, healthcare systems are increasingly dependent on digitization and Internet connectivity but often lack protection and are particularly vulnerable to cyberattacks. Water and energy infrastructure, or hospitals, are often damaged in armed conflicts by shelling, and services operate only partially or not. If this coincides with a significant cybercrime accident, moreover, this can have serious consequences. Civilians are stuck in conflict, and violence suffices to worsen their difficulties.

Humanitarian international organizations increasingly rely on new and digital technologies to support humanitarian programs by recording and using information to guide and adapt responses or by facilitating communication between humanitarian personnel and civilians affected by conflict or violence. But this is also vulnerable

to cyber operations that may affect their ability to provide protection and assistance during humanitarian emergencies.

Consequently, conflict-affected populations are at increased risk of deliberate and unintentional harm, mainly through (misuse) of data by belligerents and spreading of misinformation, false information, and hate speech.

The research aims to identify international conflicts under the Fourth Industrial Revolution by identifying cyberattacks that are the most important cause of international conflicts under this new revolution and to identify international conflicts under the Fourth Industrial Revolution as ways of resolving them considering the rules of public international law.

The problem of this research stems from answering the following questions:

What is the industrial revolution? What are cyberattacks? What are international conflicts?

What are the objectives and means of cyberattacks during armed conflict?

What are the ways of resolving international conflicts under the Fourth Industrial Revolution?

What are the international models of cyberattacks and ways of confronting them?

The inductive and analytical approach to this research has been used to arrive at the results we will show. Accordingly, the study was divided into an introduction and three sections. The first section deals with the definition of international conflicts, the Fourth Industrial Revolution, and cyberattacks; the second section deals with international conflicts and ways of resolving them under the Fourth Industrial Revolution; and Part III deals with

cyberattacks occurring during armed conflicts, and finally, the research's conclusion containing recommendations and findings.

1. Definition of International Conflicts, the Fourth Industrial Revolution, and Cyberattacks

Relations between States are volatile and sometimes unstable. Conflicting interests lead to conflict between States. It is prudent that States seek an amicable settlement of the dispute and rely on means of violence only if necessary. The efforts of peace-loving politicians since the end of the last century have tended to replace the peaceful means of resolving international disputes. For this purpose, major conferences such as the Hague Conferences held in 1899 and 1907 contained provisions for the peaceful settlement of international disputes. Subsequently, the Charter of the League of Nations and the conventions under the umbrella of the Mission, and the Charter of the United Nations and subsequent international conventions were added to these provisions[1].

This Section is divided into three parts, the first dealing with the definition of international conflict, the second discussing the definition of the Fourth Industrial Revolution, and the third discussing the definition of cyberattacks.

1.1. Definition of International Conflict

Disputes between States are a severe threat to the International Legal Order. They demonstrated the contradiction, complexity, and divergence of States' positions on them, leading to the risk of

[1] Ali Sadiq Abuheef, al-Qanoon al-Dawli al-Aam, al-Marif Publishing, Alexandria 2015, p.556.

endangering international peace and security. Therefore, international organizations and States and people are keen to resolve conflicts in international relations in peaceful ways without the use or threat of force—global security and stability, which States seek to avoid in minimal cases[2] .

An international dispute is a dispute over a legal or factual matter, consisting of a contradiction or conflict of legal opinions or interests between two or more subjects of international law, and therefore, is not an international dispute if one of the parties is a subject of private international law, such as natural persons and private institutions.

International disputes are "contradictory claims between two or more international subjects, requiring resolution by means specified in public international law[3] ".

An international dispute is defined as "a dispute over a question of law (such as the interpretation of an international treaty) or of fact (such as a dispute over the location of the boundary line) consisting of a contradiction, conflict of the legal opinion of one or more subjects of international law." The international dispute was also defined as "the dispute between two States over a particular legal object or incident or because of a conflict in their economic, political or military interests and their different legal arguments." The permanent wisdom of international justice defined the dispute as "a dispute over a point of law or fact, consisting of a

[2] Mukhalad Rukhais Altarwana, al-Qanoon al-Dawli al-Aam, Wail House for Publishing and Distribution, Amman 2017, 377.

[3] Abdulkareem Awadh Kahlifah, al-Qanoon al-Dawli lil bihar, al-Jamia al-Jadidah house, Alexandria 2013, p.168.

contradiction or conflict in the positions subjects of international law[4] ".

It is clear from the preceding definitions that conditions must be met to make the conflict, and most importantly, that the conflict must be international, and the conflict must arise between international legal subjects, between States or between States and international organizations, or between international organizations. Add to that the dispute is permitted, as this dispute relates to the interpretation and application of treaty land, maritime, or disputed areas, or exploitation and investment of the sea resources،[5] . The other condition is the existence of contradictory claims between the parties to the conflict that the international dispute must be based on a contradictory claim by a party offset by a contradictory claim by another party; one party asks the other party to do or refrain from doing or handing over something. Lastly, these allegations lead to conflict, and the conflict is peaceful in its settlement in the event of a dispute between two States that cannot be resolved satisfactorily by the parties; this dispute is not subject to the rules of international dispute settlement extradition, for example, one State requesting another State to extradite an offender on its territory. However, the dispute settlement becomes impossible if the offender flees to an unknown destination or dies[6] .

1.2. Definition of the Fourth Industrial Revolution

The international community has witnessed numerous industrial revolutions that have affected human life by providing humankind

---

[4] Mukhalad Rukhais Altarwan, Op.Cit. pp.379-380.

[5] Suhail Hussain Alfatlawi, al-Qanoon al-Dawli lil bihar, al-Thaqafa Bookstore, Amman 20212, pp.271-272.

[6] Mukhalad Rukhais Altarwan, Op.Cit., pp.380-381

with outstanding services that have facilitated and changed our way of life. The first industrial revolution, the second and the third, the last of which was the fourth industrial revolution, brought about dramatic changes in all aspects of life to develop dramatically and accelerate the world of technology, making the convergence and integration of the physical and virtual world possible, using high-speed technologies and development in all areas[7].

Industry Revolution IV (IR4) first appeared in 2011 at the Hannover Expo. The German government officially announced the Revolution in 2013 as a strategic initiative to develop highly sophisticated and accurate technological industries and try to play a leading role in this revolution. The World Economic Forum in Switzerland named the fourth industrial revolution in 2016 in an announcement by the Forum's chief executive, Klaus Schwab.

There were two main reasons for the fourth industrial revolution: the technological demands of industrial companies and the urgent need for other political and economic aspects of change and development. The announcement of the Fourth Industrial Revolution included nine critical elements of the Revolution: e-physics, IoT, big data, 3D printing, robots, simulation, augmented reality, cloud computing, and cybersecurity. Further concepts of the Fourth Industrial Revolution were discovered. Some ideas were renamed, or some explanations and clarification were added[8].

Klaus Schwab defined the Industrial Revolution as "a combination of advanced production technologies and intelligent

---

[7] Asia Ba'adi, al-Thawra al-Sinaia al-Rabia, Journal of Economics and Sustainable Development, Vol. 5, Issue 2, 2022, pp.561-577.

[8] Qasim Kareem, al-Tahool naho al-Thawra al-Sinaia al-Rabia min Khilal Badh al-Namathij al-Dawliya, Economic Studies Journal, Vol. 16, Issue 1, 2022, pp.368-385.

systems that integrate with organizations and individuals by creating a world in which virtual and physical manufacturing systems flexibly collaborate at the global level[9] .

The Fourth Industrial Revolution is "an industrial revolution based on the numerical revolution that makes technology an essential part of societies by penetrating and centralizing in various fields for development through many means: robots, industrial intelligence, nanotechnology, quantitative computing, biotechnology, the Internet of Things, 3D printing, and autonomous vehicles[10]".

The Fourth Industrial Revolution was defined as "the wealth of virtual physical systems, the age of communication and the Internet Revolution, where technological advances have been historically unprecedented by connecting billions of human beings to mobile devices, characterized by the wondrous ability to analyze and store knowledge, as well as other changes they bring at the business, government and even the future [11]".

1.3. Definition of Cyberattacks

American mathematician Norbert Weiner was the first to use the term cyber in 1948 while studying sedition in command, control, and communication in the animal world. It seems that the different dictionaries did not refer to the source of the word "cyber." The

---

[9] Aramah Dalal and Litrch Thahabiah, Tadaiat al-Thura al-Sinaia al-Rabia ala Sulalat al-Qiamah al-Alamiya, Economic Integration Journal, Vol. 9, Issue 4, December 2021, pp. 525-542.

[10] Haidi Ibrahim Hajaj, al-Tasharuk al-Marifi lil Mutakhasisin fi Musasat al-Malomat al-Arabia fi Dhil al-Thura al-Sinaia al-Rabia, Cybrarians Journal, Vol. 16, Issue 56, 2019, pp. 1-11.

[11] Qasim Kareem, Op. Cit. pp. 368-385.

dictionaries of military terminology did not refer to the source of the word but instead defined it in the scope of its military use. For example, the Dictionary of American Military Terminology indicated that cyber was "any act used through electronic networks to control or disrupt other electronic software." Several definitions of cyberattacks have emerged, and each report has clarified the concept from a different angle, with a convergence in the meaning of "targeting websites through other electronic means of communication[12]".

A cyberattack is "an attempt to steal data or to obtain unauthorized access to computers and networks using one or more computers and is often the first step an attacker takes in getting unauthorized access to computers, individual or commercial networks before carrying out a data breach [13] ".

Michael N. Schmitt defined it as "State action to attack the information systems of the attacking State." The International Committee of the Red Cross (ICRC) has defined cyberwar as "means and methods of war consisting of cyberspace operations that rise to or take place in the context of armed conflict, within the meaning of international humanitarian law[14] "Ogla Fuertes defined it as "an Internet attack based on the infiltration of unauthorized websites, with the aim of disabling, destroying or

---

[12] Ahmed Obais Alfatlawi, al-Hajmat al-Sibrania; Mafhomaha wal Msuliya al-Dawliya al- Nashia anha, Journal of al-Muhaqiq al-Hili for Legal Sciences, Vol. 8, Issue 4, 2016, pp. 610-688.

[13] what is a cyber-attack? published in Fortine website: https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack

[14] Rami Abood, Degitologia: al-Internet, Iqtisadiat al-Marifah, al-Thura al-sinaia al-Rabia, al-Mustqbal al-Arabi for publishing and distributing, Cairo 2016, p. 46.

acquiring data available in them, a series of cyberattacks by one State against another". It was also defined as "any conduct in defense or attack, reasonably expected to cause injury or death of a person, material damage or destruction to the attacking target[15] ".

Cyberattacks are divided into four sections: loss of privacy, loss of command and control, loss of confidential and vital information, and physical sabotage of associated devices and installations. Experts support the recent results and impact-focused attitude, which counts cyberattacks as a means of targeting the facility associated with this space, and some consider this to be the original definition of cyberattacks to "build upon the results of these attacks[16] ".

2. Cyberattacks during Armed Conflict:

Cyberattacks are the most significant challenge facing specialists in international law because of the difficulties that have arisen in determining the nature of such attacks and the resulting global criminal or civil responsibility because States resort to such attacks for certain gains, such as dominating the reality of armed conflict. Cyberattacks on States' information infrastructure and Internet services severely threatened internal security as the concepts of power, conflict, and war changed, and their nature was linked to cyberspace[17] .

---

[15] Ahmed Obais Alfatlawi, Op. Cit, pp.610-688.

[16] Ali Muhammad Kadhum Almusawi, al-Musharaka al-Mubashira fi al-Hajmat al-Sibrania, al-Musasa al-Haditha for book, Beirut 2019, p.25.

[17] Nasseb Najeeb, al-Harb al-Sibrania min Mandhor al-Qanoon al-Dawli al-Insani, Critical Journal of Law and Political Science, Vol. 16, Issue 4, Algeria 2021, pp.218-236.

This section was divided into two parts, the first dealing with the legal character of cyberattacks and the second looking at Realistic models of international cyberattacks.

2.1. The Legal Character of Cyberattacks:

Cyberattacks sometimes turn into armed conflict, called cyberwarfare or cyberattacks by the rules of international humanitarian law. They are offensive or defensive electronic operations that may cause injuries, killings, destruction, or property damage, and thus, cyberattacks can have a broader scope than cyber warfare. Sometimes, they occur and do not cause war; sometimes, they are grounds for starting war between States. Cyberattacks are vaguely targeted and undefined because they move through international border information and communication networks with new electronic weapons suited to the nature of rapid electronic development and the easy and rapid transmission of data; these attacks are directed against vital installations or manipulated through intelligence agents. and therefore, the critical criterion for distinguishing traditional attacks from cyberattacks is the nature of the weapon used. It can be said that cyberattacks are attacks in which the effects of such weapons use non-conventional weapons and which consist of widespread destruction[18] .

Some international law experts consider that the methods of cyberattacks are related to terror and terrorism, so these attacks have been defined as "an Internet-based system of terror, aimed at carrying out numerous actions to intimidate the security of individuals, groups, institutions, and States and bring them into

[18] Yahiya Ysin Saud, al-Harb al-Sibraniya fi Dhaw al-Qanoon al-Dawli al-Insani, Legal Journal, Vol.4, Issue 4 Year 2018, pp.80-108.

psychological, economic, political and social crises resulting from so-called silent terrorism [19] .".According to ICRC Legal Adviser Cordola Durg, cyberattacks are operations against or through a computer or computer system through data flow to achieve various purposes, including the penetration of a particular design, the collection, transfer, destruction, alteration, or encryption of data, or the modification or manipulation of operations controlled by the hacked computer. In some circumstances, procedures may be considered attacks, as defined in international humanitarian law [20] .

The Charter of the United Nations prohibits using force in international relations. The interpretation of the term "force" was questioned: was it the use of armed force against a State? Or includes economic or political pressure and other means. There is another tendency to see what is meant by "By force" in all forms of the use of armed force, as well as other images that have a clear violation or impact on the national security of another State; therefore, different interpretations associated with cyberattacks, including to the concept of force, as the use of cyberspace has had a significant impact on technological command and control.

The elements of power have, therefore, become the harmony between technical, demographic, economic, and industrial capabilities, military power, the will of the State, and other factors contributing to the State's potential to exert coercion, persuasion, or political influence in the actions of other States to achieve the power of the objective, whether legitimate or unlawful, the change in the concept of force leads to a change in the perspective of war.

---

[19] Nasseb Najee, Op.Cit, p.233.

[20] Ahmed Alfatlawi, Azhar A. Alfatlawi, al-Masuliya al-Nashia an Istikhdam Wasail al-Qital al-Fataka fi Nashr al-Awbia, Journal of rights, Vol.41, Year 2021, pp.49-88.

Traditional wars based on the destruction of the opponent, the occupation of his land, or the seizure of his resources have moved into wars operating to capture the race for technological advances, steal economic and practical secrets, control information, and work to penetrate national security without aircraft or missile attacks, or cross borders[21] .

There is a difference between the terms cyberattack and cybercrime. The right of the abused State to cyberattack is different from its right to respond to cybercrime; cyberattacks can potentially shut down the Closure of nuclear centrifuges, air defense systems, and electrical networks, all of which threaten national security. Such attacks must be treated as war and are thus like armed attacks regulated by international humanitarian law. Cybercrime is a criminal offense against persons or groups, such as objectionable entry, destruction, or unlawful interception of data stored in systems by transferring them from one organ to another [22] .The United States Technical Assessment Office defined it as "the crime in which computer data and information software play a crucial role[23] " It was described as "unlawful and legally punishable conduct by a criminal will be replaced by computer data." And so, the aim of cybercrime is very different from the goal of cyberattacks because it's the result of the attack that determines who's behind it. The cyberattack is carried out by a State or terrorist organizations for national security requirements cybercrime ", while cybercrime is far from State policy and the State is precluded from being the

[21] Yahiya Ysin Saud, Op. Cit, p.86.

[22] Ali Fadhil Sulaiman, Ha q al-Difaa al-Shari al al-Hajmat al-Sibrania, Tikrit University Journal for rights, Vol. 4, Year 4, Issue 1, 2020, pp. 245-260.

[23] Mohammad M. Alamri, Madkhal ila al-Amin al-Sibrani, Zahran Hours for Bulishing, Amman2020, p. 43

attacker and even persons or groups of piracy who carried out the cybercrime [24].

2.2. Realistic Models of International Cyberattacks:

According to one ecologist, "Many means of command and control for most of the Earth's vital processes have moved into space in satellite imagery and space stations, and a wide range of wars, battles, dialogues, and revolutions have moved into the virtual world created by man since his invention of the computer, electronic memories, and information networks, creating a new virtual geography. "This development has introduced an international approach in a new way that was not foreseen in the development of prevailing legal regimes. After global interaction during armed conflicts on Earth, sea, air, or outer space, modern technologies have made electronic information systems different from conventional warfare. Cyberspace has become a real competitor to traditional international scope[25] .

American writer David Ignacius said in an article in the Washington Post that the Cold War may be over, and it's time to start the cyberwarfare between rival nations. They pointed to Russian hacks and hacking of vital American sites and targets. Other Russian pirate targets included former U.S. Secretary of State Colin Powell's emails and those related to drug and doping tests for top American athletes .He noted that in this era of cyberwarfare, which is now beginning, Russian pirates, in turn, seem to have started crossing borders, with clear targets including the

---

[24] Ali Fadil Sulaiman, Op. Cit, p.245-260.

[25] Mohammad Almagdhob, al-Wasit fi al-Qanoon al-Dawli al-Aam, Alhalabi. Alhoqoqiya Publishing, Beirut 2018, pp. 814-815.

Democratic National Committee or Democratic Party's electronic files in the United States[26] .

The New York Times revealed that cybercrime analysis has demonstrated that the cyberian warriors' unit in the Chinese military is responsible, with a slight level of suspicion, for most attacks on American companies and even ministries, and US President Biden warned that cyberattacks are a form of war aggression against his country, giving way to a similarly military response[27] .

President Biden has put the issue at the forefront of his attention, speaking on many occasions, and used the Office of the Director of U.S. Intelligence to focus on it, explaining the nature of the ongoing attacks on the United States, whether by governments or criminal hacking aimed disrupting corporate systems and imposing ransom on them to restart them. Biden offered the strongest warning about what this could lead to: "If a real war against a significant power ends up, it will result from a major cyberattack that has caused catastrophic consequences[28] .

In December 2009, the South Korean government issued a report explaining that North Korean hackers had been subjected to a cyberattack to steal secret defense plans that included information on the form of South Korean and U.S. action if a war occurred on the Korean peninsula. According to experts, Estonia's 2007 international cyberattack was used to disrupt government,

---

[26] Washington Post; al-Harb al-Baridah Intahat wa Badaat al-Harb al-Ilktronia, Aljazeera net wesite; Last visit; 30/7/2023: https://www.aljazeera.net/news/presstour/2016/9/16/واشنطن-بوست-الحرب-الباردة-انتهت-وبدأت

[27] Mohammad Almagdhob, Op.Cit, pp. 818-819.

[28] Bada Tasaod al-Hagmat al-Ilktronia; Baiden yohadhir min Dokhol Harb Dhid Qwa Kobra; Aljazeera net website; last visit; 30/7/2023: https://www.aljazeera.net/politics/2021/7/30/الإرهاب-الإلكتروني-واشنطن-تنذر-موسكو

commercial, banking, and media websites. This led to tens of millions of dollars in losses, and the paralysis of the country, and no one was able to find the actual perpetrator or the source of the attack, one of the most significant difficulties associated with cyberattacks[29].

Some believe that the forthcoming wars could begin with a cyberattack to cripple the effectiveness of the electronic systems of vital installations, military and civilian (Electricity, water, energy, telecommunications, transport, and banks), leading to their collapse and the State enduring more disasters than conventional armed conflict, and could be the next cyberwar or directly (between two or more States) or through a third party (ordinary person or specialized organization)[30] .

3. International Conflicts and Ways to Resolve them in the Fourth Industrial Revolution:

Those responsible for modern-day military institutions believe that the victor's shoulder in current or future wars tends to be coupled with the master of Information warfare in all its forms, including cyberattacks, for lack of costs compared to the magnitude of damage it can cause. Modern nations and their advanced armies have, therefore, begun to increase their activities and intensify their efforts in cyberspace, which is a source of strength but sometimes reveals weaknesses. The State's critical infrastructure (water, electricity, and transportation), military command, control and control networks, and the sophisticated techniques of the modern

---

[29] Faisal Mohammad Abdulgafar, al-Harb al-Ilktronia, Aljanadria for Publishing and Distributing, Amman, 2016, p.13.

[30] Mohammad Almagdhob, Op. cit, p.820.

battlefield all depend on cyberspace. The elements mentioned above can be the target of the attacking State against the adversary and may be the target of the opposition's attack[31] .

This section is divided into two parts. The first discusses international conflicts under the Fourth Industrial Revolution, and the second discusses conflict resolution under the Fourth Industrial Revolution.

3.1. International Conflicts under the Fourth Industrial Revolution:

The Fourth Industrial Revolution brought transformations and changes in many areas of life, including economic, social, and cultural. Under this revolution, many of the barriers that separated States, such as geography and language, opened the way for the transmission of information; the change in States' behavior and mutual disputes took place. This Revolution had several dimensions that had implications for international conflicts.

It can be said that the recent international conflicts are "international disputes managed remotely through the use of smart weapons, rationalizing society through the Internet, to destroy, fail and to damage the corners of the State in all areas." These include waging wars by gathering information, beating people's economies, using modern technology for espionage, spreading rumors, and sowing discord between the conflicting parties. These wars depend on systems, not people, and they are remotely controlled, using piloted missile weapons, laser-guided intelligent bombs, satellites and drones, and satellite-controlled mines through activation or decommissioning .

---

[31] Ali Mohammad Almusawi, Op. cit, p.33.

One of the most essential concepts of cyberattacks in the era of the Fourth Industrial Revolution is Speed, shock, intimidation, and rapid critical operations via targeted micro-munitions to increase the effectiveness of information control through new numerical systems flexible and proliferate robotic systems used to detect and track individual vehicles, ships or aircraft beyond visibility. It provides targeted information and independent decision-making to achieve strategic objectives that have broken the opposition's will rather than mobilizing troops[32] .

Cyber operations raise humanitarian concerns, mainly when their impact is not limited to the data of the targeted computer or computer system. It aims to impact the "real world" by manipulating supporting computer systems; one can use enemy air traffic control systems or systems to flow oil pipelines or nuclear plants. As a result, the potential humanitarian impact of some cyber operations is significant. The cyber operations in Estonia, Georgia, and Iran do not have severe consequences for the civilian population. However, it can interfere with airports or other transportation systems, dams, or nuclear power plants through cyberspace. Thus, potential catastrophic scenarios must be addressed, such as plane collisions, leaks of toxins from chemical plants, and disruption of infrastructure or vital services such as power systems or water. The most important victims of these operations are more likely to be civilians[33] .

---

[32] Yunos Muaid Yunos, Rakaiz Horob al-Jil al- Sadis wa Atharoha fi Istratijiat al Qwa al Faila fi al-Nidham al-Almi, Tikrit Journal for Political Scinces, Vol. 4, Issue, 30, 2022, pp. 33-76.

[33] Cordula Droege, ICRC legal adviser, no legal vacuum in cyberspace, interview published on ICRC website last visit: 5/9/2023:

3.2. Resolving International Conflicts in the Fourth Industrial Revolution

International law experts believe cyber warfare is a war in the customary sense, and the fundamental difference between conventional and cyber warfare is intelligence and cost. War in the Fourth Industrial Revolution era has a global impact, and if this war results in devastating consequences such as power outages, the Internet, or the destruction of a nuclear reactor's electronic system. A military attack "would amount to an act of war requiring a response as a military attack .The rise in the frequency of cyberattacks, which may be a state of war, has led experts to ask: When do we impart an act of hostilities, what are the rules of engagement, how can a State defend itself, how can the aggressor be identified, what is the form of response to the attacks, and can there be the talk of cyberlearning?

In response to previous questions, the views of its specialists and experts differed; according to ICRC Legal Adviser Laurent Gisel, article 36 of Protocol I of 1977 obliges States parties to bring new weapons into conformity with international humanitarian law. Gisel noted that the development of rules of international law could be included to provide comprehensive protection to civilians, in line with the development of cybertechnology or to accommodate its impact on humans. It must be stressed that States still need to be able to agree on a special law on the use of cyberspace and how to resolve disputes arising from such use. According to one expert, States are alienating the law's regulation issue because they want to

https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

remain unrestricted in the conduct of their wars, including using space in cyberspace [34] .

Accordingly, NATO's Centre of Cooperative Excellence for Cyberspace Defense invited a group of international law experts to study the possibility of establishing rules for applying international humanitarian law rules to cyber war, and experts prepared a legal instrument called Manuel de Tallinn[35] .This manual provided an answer to the most sensitive points related to State cyberattacks, or those carried out by non-state actors, such as rules of cybercrime and the reciprocity of cybercrime, the possible observance of international humanitarian law known as the principle of non-discrimination, and the legitimacy of targeting electronic counterpart by physical military means such as military drones[36] .

The Tallinn Manual is the most comprehensive measure that seeks to interpret the rules of international law in the context of cyber war. The Manual provides a valuable set of rules that clarify different views on the thorny issues raised by the modern technology age. The ICRC participated in the deliberations of the Group of Experts as an observer but only agreed with some of the rules contained in the Manual. The manual provides an essential insight into various topics related to non-conventional international conflicts, including bilateralism of international and non-international armed conflicts, recognizes that cyber operations may constitute armed tendency depending on the circumstances, and also states that the principles of precaution and proportionality must

---

[34] Mohammad Almagdhob, Op. cit, p.822-823.

[35] See the Tallinn Manual on this website; last visit; 3/9/2023.
https://iipsl.jura.uni-koeln.de/sites/iipsl/Home/Schmitt_Tallinn2_nocode.pdf

[36] Dirweesh Said, al-horob al-Sibrania wa Atharoha al Hoqooq al-Insan, Algerian Journal for Legal, Economics and Political Sciences, Vol. 54, Issue 5, 2017, pp.177-200.

be respected if the Internet is attacked, and other texts referred to in the manual[37] .

Despite those actions, international cooperation still needed to establish rules for resolving cyberattack conflicts. Current international legal standards and instruments still need to be prepared to deal with cybersecurity challenges, and the international community should take swift action to address the legal deficit in addressing the challenges of cyberattacks and establish rules for resolving conflicts arising from such attacks.

It should be noted that one of the ICRC's tasks is to protect civilians from armed conflict and other conflict situations. Throughout its history, the ICRC has been working to adapt to new types of conflict and images of violence, as well as new weapons and means of war, and they have had to constantly modify their activities and methods to respond to the changing needs of different groups affected by the consequences of war and violence. This rapid and sustained response by ICRC has led to the emergence of new protectionist activities commensurate with new forms of armaments as well as reflection and ongoing work on the development and application of international humanitarian law, humanitarian policies, humanitarian programs, and operational standards. Today, as we stand against an emerging type of "information armament," the International Commission should develop its tools and interventions to enforce its mission to protect persons entitled to protection[38] .

---

[37] Musa bin Tagir, al-Harb al-Sibrania wal Qanoon al-Dawli al-Insani, Journal of Judicial Jurisprudence, Vol. 12, Special Issue, 2020, pp. 199-218.

[38] Alinsani editor, Baina Tasleeh al-Maloomat wa Ansanatiha, Humanity Journal, Vol.70, Feb. 2023, published in Journal website; last visit; 23/8/2023. https://blogs.icrc.org/alinsani/2023/02/28/7292/

The International Committee of the Red Cross (ICRC) noted the increased risk of intentional and unintentional harm to conflict-affected populations, mainly through (misuse) of data by warring parties and the spreading of misinformation, false information, and hate speech.

A few States have openly endorsed using cyber means to support their military operations, with estimates that more than 100 States have developed or are developing cyber military capabilities. According to ICRC, such attacks during armed conflicts do not occur in a legal vacuum governed by international humanitarian law. The ICRC's opinion was as follows:

"In our view, the law is clear on this issue: international humanitarian law limits cyber operations during armed conflict just as it limits the use of any other weapons, means, and methods of warfare during an armed conflict, new or old".

As the International Court of Justice has pointed out, the most prominent strengths of international humanitarian law are that it has been developed in ways that make it applicable "to all forms of war and all types of weapons," including "future forms and types". The basic rules are clear: targeting civilians and objects is prohibited, weapons and indiscriminate attacks must not be used, disproportionate attacks are prohibited, and medical services must be respected and protected[39] .

---

[39] Gisel, Rodenhäuser, Dörmann, twenty years on International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts, published in the website, last visit 6/9/2023: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913

Conclusions:

1- Cyberattacks remain a modern concept that has yet to be agreed upon in defining an international definition of cyberattacks, making it challenging to adapt global legal attacks and take global responsibility for them.

2- The attempt to establish a comprehensive legal regulation of cyberattacks faces many difficulties, most notably the failure of States to accept their restriction of rules that may limit their armed and unarmed activity at the international level, as well as the difficulty of identifying the cyberattacks.

3- The Fourth Industrial Revolution is a product of different technologies' integration and rapid development. It sought to connect the physical and virtual worlds by relying on creativity and innovation.

4- The impact of the Fourth Industrial Revolution on various fields, including military, intelligence, and armaments, has expanded. Cyberspace has become an area for using cyber weapons such as software, viruses, and artificial intelligence. These weapons have destructive potential against the target.

5- A cyberattack is a use of force from the perspective of international law that prohibits the use of force in international relations because of the effects of a cyberattack compared to an armed attack, and the results of a cyberattack may be more destructive and dangerous and may amount to a conventional attack.

6- The threat of cyberattacks can be reduced, and the security and safety of the State can be ensured in the future by developing a common international strategy that minimizes the seriousness of cyberattacks.

7- The International Committee of the Red Cross (ICRC) is endeavoring to accommodate accelerated developments in cyber conflict by adapting the effects of such attacks to established international humanitarian law.

8- International attempts have been made to establish rules governing cyber activity and its operations at the international level but have yet to succeed. Still, the rapid development of the use of cyberspace requires the speedy development of such rules to resolve any future cyber conflict and avoid humanitarian disasters to which people may be exposed.

9- The Tallinn Manual is a crucial document developed by an international organization that has addressed many cyber dispute issues. Although the Manual is not mandatory, it is the first document to emphasize observance of the norms of international humanitarian law, known as the principle of non-discrimination, and the legitimacy of targeting electronic counterparts by physical military means such as military drones.

References:

1- Books

- Abdulkareem Awadh Kahlifah, al-Qanoon al-Dawli lil bihar, al-Jamia al-Jadidah house, Alexandria 2013.
- Ali Muhammad Kadhum Almusawi, *al-Musharaka al-Mubashira fi al-Hajmat al-Sibr*ania, al-Musasa al-Haditha for book, Beirut 2019.
- Ali Sadiq Abuheef, al-Qanoon al-Dawli al-Aam, al-Marif Publishing, Alexandria 2015.
- Faisal Mohammad Abdulgafar, *al-Harb al-Ilktronia*, Aljanadria for Publishing and Distributing, Amman, 2016.

- Mohammad Almagdhob, *al-Wasit fi al-Qanoon al-Dawli al-Aam*, Alhalabi Alhoqoqiya Publishing, Beirut 2018.
- Mohammad M. Alamri, *Madkhal ila al-Amin al-Sibrani*, Zahran Hours for Bulishing, Amman 2020.
- Mukhalad Rukhais Altarwana, al-Qanoon al-Dawli al-Aam, Wail House for Publishing and Distribution, Amman 2017.
- Rami Abood, Degitologia: *al-Internet, Iqtisadiat al-Marifah, al-Thura al-sinaia al-Rabia*, al-Mustqbal al-Arabi for publishing and distributing, Cairo 2016.
- Suhail Hussain Alfatlawi, al-Qanoon al-Dawli lil bihar, al-Thaqafa Bookstore, Amman 2012.

2- Journals:

- Ahmed Alfatlawi, Azhar A. Alfatlawi, al-Masuliya al-Nashia an Istikhdam Wasail al-Qital al-Fataka fi Nashr al-Awbia, Journal of rights, Vol.41, Year 2021.
- Ahmed Obais Alfatlawi, al-Hajmat al-Sibrania; Mafhomaha wal Msuliya al-Dawliya al-Nashia anha, Journal of al-Muhaqiq al-Hili for Legal Sciences, Vol. 8, Issue 4, 2016.
- Ali Fadhil Sulaiman, Ha q al-Difaa al-Shari al al-Hajmat al-Sibrania, Tikrit University Journal for Rights, Vol. 4, Year 4, Issue 1, 2020.
- Aramah Dalal and Litrch Thahabiah, Tadaiat al-Thura al-Sinaia al-Rabia ala Sulalat al-Qiamah al-Alamiya, Economic Integration Journal, Vol. 9, Issue 4, December 2021.
- Asia Ba'adi, al-Thawra al-Sinaia al-Rabia, Journal of Economics and Sustainable Development, Vol. 5, Issue 2, 2022.

- Dirweesh Said, al-horob al-Sibrania wa Atharoha al Hoqooq al-Insan, Algerian Journal for Legal, Economics and Political Sciences, Vol. 54, Issue 5, 2017.
- Haidi Ibrahim Hajaj, al-Tasharuk al-Marifi lil Mutakhasisin fi Musasat al-Malomat al-Arabia fi Dhil al-Thura al-Sinaia al-Rabia, Cybrarians Journal, Vol. 16, Issue 56, 2019.
- Musa bin Tagir, al-Harb al-Sibrania wal Qanoon al-Dawli al-Insani, Journal of Judicial Jurisprudence, Vol. 12, Special Issue, 2020.
- Nasseb Najeeb, al-Harb al-Sibrania min Mandhor al-Qanoon al-Dawli al-Insani, Critical Journal of Law and Political Science, Vol. 16, Issue 4, Algeria 2021.
- Qasim Kareem, al-Tahool naho al-Thawra al-Sinaia al-Rabia min Khilal Badh al-Namathij al-Dawliya, Economic Studies Journal, Vol. 16, Issue 1, 2022.
- Yahiya Ysin Saud, al-Harb al-Sibraniya fi Dhaw al-Qanoon al-Dawli al-Insani, Legal Journal, Vol.4, Issue 4 Year 2018.
- Yunos Muaid Yunos, Rakaiz Horob al-Jil al- Sadis wa Atharoha fi Istratijiat al Qwa al Faila fi al-Nidham al-Almi, Tikrit Journal for Political Scinces, Vol. 4, Issue, 30, 2022.

3- Websites:

- Alinsani editor, Baina Tasleeh al-Maloomat wa Ansanatiha, Humanity Journal, Vol.70, Feb. 2023, published in Journal website; last visit; 23/8/2023.
  https://blogs.icrc.org/alinsani/2023/02/28/7292/

- Gisel, Rodenhäuser, Dörmann, twenty years on International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts published in: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913
- Tallinn Manual on this website; last visit: 3/9/2023. https://iipsl.jura.uni-koeln.de/sites/iipsl/Home/Schmitt_Tallinn2_nocode.pdf
- Cordula Droege, ICRC legal adviser, no legal vacuum in cyberspace, interview published on ICRC website: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm
- Washington Post; *al-Harb al-Baridah Intahat wa Badaat al-Harb al-Ilktronia*, Aljazeera net website; Last visit; 30/7/2023: https://www.aljazeera.net/news/presstour/2016/9/16/واشنطن-بوست-الحرب-الباردة-انتهت-وبدأت
- Bada Tasaod al-Hagmat al-Ilktronia; *Baiden yohadhir min Dokhol Harb Dhid Qwa Kobra*; Aljazeera net website; last visit; 30/7/2023: https://www.aljazeera.net/politics/2021/7/30/الإرهاب-الإلكتروني-واشنطن-تنذر-موسكو/
- What is a cyber-attack? published on Fortine website: https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack