سيادة الدولة على فضائها الالكترونى وحقها فى الدفاع الشرعى

ضد الهجمات السيبرانية من منظور القانون الدولى

State Sovereignty over Cyberspace and Its Right to Legitimate Defense against Cyber attacks in the Scope of International Law

إعداد

الدكتور/ عوض عبد الكريم المطيرى

أستاذ القانون العام المساعد كلية الشريعة والقانون

جامعة المجمعة – المملكة العربية السعودية

البريد الإلكترونى : awadah.a@mu.edu.sa

ملخص باللغة العربية

أصبح الفضاء الإلكتروني ساحة للصراعات والحروب، حيث أنه يتم استغلال الثغرات القانونية الناجمة عن غياب النصوص القانونية في القانون الدولي التي تنظم هذا المجال. ومع تزايد التهديدات السيبرانية التي تستهدف البنى التحتية الحيوية المعلوماتية للنظام الدولي، تزايدت الحاجة إلى وضع تشريعات دولية سيبرانية ملائمة. كما أن الهجمات السيبرانية اسهمت في تغيير موازين الصراعات المسلحة الحديثة، حيث وفرت بدائل حديثة للعمليات الهجومية والدفاعية لكافة الأطراف، بما في ذلك الدول ذات الموارد المحدودة. ومع تصاعد وتيرة هذه الهجمات في السنوات الأخيرة، أصبح من الممكن أن تصل إلى مستوى العدوان المتمثل في التدمير أو التعطيل الذي يطال البنية التحتية الحيوية الخدمية كشبكات الكهرباء، وشبكات الطاقة، والصناعات، والمرافق الصحية، مما يؤدي إلى معاناة كبيرة للمدنيين وخسائر في الأرواح وتدمير الممتلكات وتعطيل الخدمات الأساسية.

كان مفهوم السيادة مرتبطًا بعوامل جغرافية محددة، إلا أن تطور وسائل الاتصال أحدث تغييرات جذرية في هذا المفهوم. ومع تعاظم أهمية الشبكة الدولية للمعلومات التي أصبحت تمثل أصولاً تفوق في قيمتها رأس المال الاقتصادي، ومع ظهور مفهوم السيادة السيبرانية الذي يعيد صياغة معايير السيادة في عصر المعلومات. لم يعد مفهوم السيادة مقتصرًا على الحدود الجغرافية، بل توسع ليشمل الفضاء الرقمي الذي خلقته وسائل الاتصال الحديثة. ومع التحول الرقمي السريع، باتت السيادة السيبرانية محور اهتمام كل دولة. وتسعى دول العالم أي ضم هذا

الفضاء ضمن سيادتها والعمل على حمايته من أي تهديدات. مما دفع المجتمع الدولي إلى تعزيز التعاون من خلال إبرام العديد من الاتفاقيات الدولية لمكافحة الجريمة السيبرانية وضمان حماية الدول لهذا الفضاء من أي اعتداء.

كلمات مفتاحية بالعربية: السيادة السيبرانية، الهجمات السيبرانية، القانون الدولي، البنية التحتية، الأمن السيبراني، التعاون الدولي.

Abstract

Cyberspace has become an arena for wars and conflicts, as the gap of the absence of texts in international law regulating this space has been exploited. Thus, the need for cyber laws has increased with the escalating threat of cyber-attacks to the information infrastructure in the international system. These attacks have served as a balancing factor in modern armed conflicts by providing new methods for both offensive and defensive operations for all actors, including those with fewer resources. Hence, the frequency of cyber-attacks has been intensified in recent years and can be escalated to the level of aggression, either by destruction or disruption against a wide range of critical infrastructure such as communication networks, electricity grids, energy networks, industries, and health facilities. Alarmingly, such attacks can cause severe suffering to civilians, loss of lives, destruction of property, and disruption of basic services.

The traditional concept of sovereignty was associated with some conventional factors. However, with the advancement of communications, the concept of sovereignty has faced radical changes. Furthermore, it has become increasingly difficult to control information considering the connection to the International Information Network, which has formed a significant asset surpassing the importance of economic capital in our current era. This has given rise to the concept of cyber sovereignty, framing the standards of sovereignty in the information age. It is no longer confined to geographical boundaries, as communication means have created a new space. Moreover, considering the rapid digital transformation, the concept of cyber sovereignty has become a focal point of interest for any state in the world, pushing the international community to embody cooperation in reality. This has led to the conclusion of numerous international agreements in the field of international cooperation to combat cybercrime.

Keywords in English: Cyber sovereignty, Cyber-attacks, International law, Infrastructure, Cybersecurity, International cooperation.

1- Introduction

Technological advancements have contributed to the addition of new tools and unconventional capabilities that states can depend on to manage international relations and protect their territories. To explain, these advancements have added new dimensions to a state traditional tool of force, whether hard or soft, namely the force of cyberspace. Additionally, the impact of the technological revolution on various aspects of life has not been limited to societal, economic and political interactions only but has extended to create a new arena of unconventional warfare away from the arenas of land, air and sea - the cyberspace arena. Under this arena, several factors have encouraged states and non-state actors to use it as a tool for conflict, competition, dominance and unconventional terrorism. Typically, armies are composed of three military elements: air force, land force and navy force. On the other hand, in the age of the digital revolution, battles take place in cyberspace between adversaries, most of whom are unidentified, attacking the digital infrastructure of states they classify as enemies. These cyber-attacks aim at acquiring sensitive intelligence information, significantly destroying the information-based economy infrastructure, or simply notifying the enemy of their presence in cyberspace. (Gomathy, 2024, P.12)

Despite the evolution of political systems, the formation of international relations, and the positive aspects they have brought, they have also implied countless threats and risks at all levels, whether for individuals, institutions or countries. The huge technological advancements have created new sovereign arenas, prompting states worldwide to impose their security controls over them. Therefore, cyber security has become one of the most crucial pillars of the national security system for most states in the new cyber-natured world. Accordingly, the global digital scene in the era of technological and informational revolution calls for an understanding of the boundaries of the digital interaction between cyberspace and the national security sovereignty of the countries around the world. As the geographical borders of nations blurring due to technological advancements that have enabled states to access a cyberspace containing various national, security, economic, and political elements and information, the concept of state sovereignty has evolved beyond what it was before the new technological innovations that disregard international boundaries. Thus, states have grown fearful of these innovations for their sovereignty and, consequently, their national security, which has become vulnerable to threats posed by cyber-attacks. (Amar, 2019, P.163)

Despite the aim of contemporary international law to foster global peace and security, the world is witnessing almost continuous and pervasive conflicts, notably known as cyber warfare. Generally, modern technology has contributed to the development of the field of international relations; military technology has changed the course of contemporary international relations despite the existence of International Law. It is worth mentioning that cyber-attacks are increasingly recognized as one of the essential weapons that states aspire to obtain and protect their territories from any breaches in order to secure them militarily. This raises questions about the extent of states sovereignty over their cyberspace and the concept of this cyber sovereignty. It also questions the extent to which a state can exercise its legitimate right to defend this cyberspace against any external cyber-attacks.

1.1Research Problem

The problem of the study lies in the extent of the danger posed by cyber-attacks resulting from technological advancements that have led to the misuse of information systems, aimed at harming the interests of state institutions. The technological and informational advancements have given rise to various forms of warfare, including cyber-attacks, which differ from traditional warfare methods but do not differ significantly in their outcomes from the use of military force in terms of damaging state interests and destroying its infrastructure. Rather, in some cases, they can cause even greater damage than traditional wars, threatening international relations. States are constantly seeking to arm themselves and allocate huge budgets to manufacture and purchase weapons to provide protection and impose their sovereignty over their land, sea and air territories.

In addition, with the emergence of cyber-attacks, new sovereign arenas have arisen, prompting countries worldwide to impose their security control over them. It is no longer limited to the land, sea, and air territories of states, but technological advancement has created a new space containing massive amounts of information related to the national security of countries around the globe. In light of this digital transformation, the concept of national cyber sovereignty has become extremely important for any state in the world. This situation forces any state facing a cyber-attack on its cyberspace to invoke its legitimate right to defend itself against any threats to that space and to establish full control over it.

1.2 Research questions:

- What is the concept and scope of state sovereignty over its cyberspace?
- What are the types of cyber-attacks?
- What is the legal relationship between cyberspace and state sovereignty?
- Is a state entitled to exercise the right of legitimate self-defense against cyber-attacks?

1.3 Research Methodology

At first, this paper adopted a descriptive approach by initially clarifying some concepts about the nature of cyber-attacks and their connection to the concept of cyberspace. Then, it described the nature and types of cyber-attacks. Succeeding that, it continued to characterize the concept of state sovereignty over its cyberspace.

Regarding the final part of the paper, an analytical approach was adopted in order to examine the applicability of the principle of the right to legitimate defense under Article 51 of the United Nations Charter concerning cyber-attacks. Subsequently, it analyzed whether a state has the right to legitimate defense against these cyber-attacks. In addition, the framework will include a set of international legal texts on the use of force and self-defense, and their alignment with the concept of cyber-attacks.

1.4 Significance of the Study

With the increasing complexity of cyber-attacks and governments facing multiple battles, the significance of the study lies in the fact that cybersecurity has become a vital area for targeting national security. Cyber-attacks are a vast and novel field internationally, and the international and legal response to them is relatively limited due to the immense legal and political implications that arise, which have not been adequately addressed by modern international law in its current form. The foundations and principles of this law were established in the aftermath of World War II by the United Nations. The new International Law was based on the prevailing warfare data of its time, as the drafters could not have anticipated the unprecedented technological advancements that humanity would make.

The international rules governing the crime of aggression and the activation of a state’s right to self-defense were designed according to the concept of conventional weapons at that time. Thus, international legal rules emerged, addressing the conditions for self-defense against armed attacks, including the principle of proportionality between the act (the crime of aggression) and the response to that aggression. This principle was only limited to the nature and type of conventional armed forces. Conversely, the type of weapons has changed over time due to technological advancements in recent decades. For this reason, there was a need to study new military weapons, namely cyber-attacks, and their legal implications, foremost among them being the legitimate means of defense against them and the regulations governing the use of this international legal right, known as the principle of proportionality in legitimate defense.

Likewise, complex and fragmented regulations exist cyber attackers are working transitionally, with laws increasingly complex and fragmented among multiple domestic authorities of states. This leads to the multiplicity and fragmentation of data protection rules, weakening cyber defense mechanisms, and thus necessitating international cooperation.

1.5 Objectives of the Study

It goes without saying that cyber-attacks against critical infrastructure can reach the level of threatening international peace and security, constituting acts of aggression. Hence, this study, in light of the scarcity of research in this subject at the level of legal studies, will investigate the definition of the concept of cyberspace, the nature and types of cyber-attacks in general, as well as the concept and limits of state sovereignty over its cyberspace.

In order for the study to be more relevant to our contemporary reality and to provide the most recent legal references related to aggressive cyber-attacks and the resulting liability, it was necessary to track legal and political stances, especially international and national practices. This would be beneficial in terms of inference and profound understanding, leading to a more effective confrontation.

The rapid expansion and terrifying spread of cyber-attacks and their sever consequences on humanity raise the issue of searching for a legal framework to regulate them, especially in light of the legal vacuum surrounding them. This research paper aims at shedding light on the problem of the extent of a state sovereignty over its cyberspace and its right to the legitimate defense against any cyber-attacks.

2. Sovereignty over Cyberspace: Concept and Analysis:

2.1The Meaning of Cyberspace:

Amidst the tremendous development taking place in the world around us, especially in the fields of technology and the internet, coupled with the increasing emergence of the internet and the great information revolution globally, there emerged the onset of the vast cyber world. This emergence has contributed to the creation of an environment for cyberspace, characterized by what we can call cyber power, which has a great impact on the entire world. This power has a clear and distinctive impact, as cyberspace has become the site and focal point of conflict between states instead of the real world being the battleground, indicating the importance of this space and its active role locally and internationally.

Additionally, cyberspace has emerged as a new arena in cross-border international relations capable of possessing comprehensive power platforms, whether by governments or non-governmental organizations. It is also an extension of human activity, both civilian and military. It parallels what humans do in other international fields such as land, sea, air, and outer space. (Yahya Yassin, P.87)

Before delving into cyberspace, let's take a step back and understand the origin and meaning of the word 'cyber'. The word is derived from 'Cybernetics', a term previously used to describe how machines and living organisms communicate and control each other. Based on this word, many terms had emerged and used in science fiction stories and films, such as the term 'Cyberspace,' which is commonly used to refer to the internet and communication networks as if they were a fictional or virtual space. Recently, some terms derived from the word 'cyber' have been introduced, such as:"

- Cybercrimes: they are the crimes committed using the internet and computers.
- Cyberwar or cyber-attack: it means having an unauthorized access to networks, computers, and information with the intent to steal, sabotage, or destroy. It may occur between states, groups, or individuals as well.
- Cyberterrorism: this term refers to the exploitation of the internet and its applications to threaten specific individuals or destroy infrastructure for political or ideological reasons.

- Cybersecurity: this is the most commonly used term today and it refers to everything related to the protection of networks, digital data, and connected devices. (Jovanovic Filip, 2024, P.35)

Due to the existence of this cyberspace that has become the focal point of attention everywhere, and a communication point among all people across the globe, it has become necessary to deeply and greatly understand what cyberspace means. Cyberspace, or electronic space, is a term derived from 'cyber', which means leadership or management. However, it has recently come to signify the realm of the internet, encompassing everything related to it. There are various definitions of cyberspace. (Sunde, Inger Marie, 2017, P.44).

The term "cyberspace" first appeared in the 19th century in the science fiction novel Neuromancer by William Gibson. He described cyberspace as "a consensual hallucination experienced daily by billions of users in every nation... It is a complexity that has gone beyond the imagination." Thus, according to him, cyberspace is not a static data space, but rather its communication channels connect to the real world, allowing users of this space to interact with that world. Despite the fact that this phrase was coined in a science fiction context, it has become widely used among academics and specialists in the field, especially with the emergence and spread of the internet and the widespread use of digitization. (Donets, 2022, P.4)

Cyberspace is considered a virtual space created by humans, deals with and entirely depends on the existence of computers and the internet. Also, there are huge and large amount of information and devices that deal with the large cyberspace. It includes both the software and hardware components of computers, encompassing an infinite number of interconnected computers, networks, software programs and users. (Salah, P. 28)

Cyberspace also refers to the space in which computer networks exist and through which electronic communication occurs. In a broader sense, it is defined as a complex, material and immaterial field that includes a set of elements: computers, network systems and software, information processing, data transmission and storage, and users of these elements. It is classified to describe systems and services connected either directly or indirectly to the internet, wired and wireless communications and computer networks.

According to the previously stated information, cyberspace is an open, boundless, and expansive space encompassing both the real and virtual worlds. It includes a physical basis linked to an infrastructure consisting of automated media devices and wired and wireless communications systems. Moreover, it is linked to a virtual domain established by connecting the infrastructure to the World Wide Web, which contains vast amounts of data and information that is transmitted across the virtual world. This makes such data vulnerable to any threat. (Eriksson, 2022, P.96).

2.2 Meaning of Cyber Threats on Cyberspace:

Cyber threats originating from virtual spaces usually aim at creating an impact on the power balances in the tangible world. These threats constitute a new means of controlling other domains i.e. land, sea, air, and outer space of targeted states. This is mainly done by targeting computer systems to control land, sea, air movements, nuclear power stations, power grids, civil infrastructure, and military infrastructure in general, using malicious software or other means. The consequences of such attacks can be serious for targeted states and its repercussions may even escalate to threaten international peace and security. (Sufian, 2022, P.272).

Thus, cyber threats refer to attacks carried out using internet mechanisms, networks, and computers, aiming to cause damage to devices and electronic networks connected to the internet. It appears that cyber threats aim to dismantle and bypass digital barriers serving a protection function as security barriers against cyber threats, for the purpose of stealing information and data, merely accessing it, sabotaging it, or even altering its content. All of this is done with the intention of harming the victim. There are several forms of cyber threats, the most important of which are:

- Traditional espionage attacks using high-precision technology aim at carrying out secret attacks to access data and information related to state institutions, both civilian and military. These attacks can be carried out by one state against another with the aim of achieving a superior position in international conflict and competition. Digital technology has replaced traditional means in espionage for various political, financial, religious and sectarian purposes.
- Carrying out attacks to sabotage the adversary's information systems, whether civilian or military, as well as disseminating false information within their intelligence systems, to gain tactical and strategic precedence for the attacking party.
- Disrupting the victim's information systems leading to the suspension of many institutions' operations, such as transportation systems, internet networks, and all entities relying on digital technology to perform their functions. This type of attack has severed effects on the state's economy that are difficult to quickly recover from. (Elbahy, 2018, P.209)

2.3 Types of Cyber-attacks:

Before delving into analyzing cyber-attack types, it is essential to present the source of these attacks, where they originate from, and how they gain strength based on the nature of their source. To begin, the first source of these attacks may be individuals, as digital technology has empowered individuals, providing them with the means to possess cyber power that amplifies their ability to conduct digital piracy operations. Moreover, it has granted them the opportunity to access financial, institutional, and corporate accounts, to acquire funds or sabotage certain institutions' websites. Without digital technology, individuals would not be able to physically access these institutions. Additionally, organized groups are considered another source of these attacks. These groups have also benefited greatly from the advancement of digital technology in conducting their attacks, whether on official entities represented by states or unofficial ones. They carry out cyber piracy operations and hack accounts, particularly financial ones, with the aim of stealing funds.

Furthermore, states have taken cyberspace as one of the essential domains they rely on to pursue their interests. They have the ability to harness digital technology, which helps them in carrying out their functions, whether in terms of cyber deterrence and defense to confront cyber threats from other parties or in the function of launching cyber-attacks on states and other entities in order to achieve specific interests. Thus, it could be said that the motivations and objectives of cyber-attacks from these sources are determined by the nature of the actor, as each actor has interests that differ from those of other actors.(Al-Awdi, 2022, P.9)

Accordingly, the types of cyber-attacks differ depending on the actor’s primary goal. Firstly, the attack may be aimed at denial of service, seeking to disrupt the target's ability to provide usual services. This method is often used against the websites of service providers, banks, or institutions of various types in order to influence them. Secondly, the goal of these attacks may be to damage or modify information by accessing the victim's data through the internet or private networks and modifying important data without the victim being aware of it. The data remains present but is misleading, which may lead to catastrophic results. Finally, the aim of these operations may be espionage by accessing the data and information network in order to obtain information related to national security. (Mahmood,2020, P.31).

2.4 State Sovereignty over Cyberspace

Despite the fact that the concept of security and national sovereignty has long been associated with traditional factors related to geography, with the globalization of communications, information exchange, and the ease of its transmission across geographical boundaries, digital technology has become an integral part of our daily lives, penetrating all its aspects, from economy to politics to society. Consequently, the concept of "digital sovereignty" has emerged as an important concept for states to independently control their digital infrastructure, big data, and cybersecurity. This independence includes making decisions about the use of digital technology in all areas along with protecting the personal data of all citizens and defending against external cybersecurity threats. Militarily, this includes a country's ability to develop both offensive and defensive cybersecurity capabilities without relying on foreign-made technology. Economically, this includes issues ranging from imposing taxes on big tech to creating local startups.

The concept of sovereignty dates back to the Treaty of Westphalia in 1648, which established the principle that a state has sovereignty over its territory and affairs without interference from other states in its internal affairs. Sovereignty is one of the pillars upon which the edifice of contemporary international law was built, and its concept is one of the important concepts that has attracted the attention of legal scholars and political researchers. (Cerf, 2018 P. 2).

2.4.1 Cyber Sovereignty, Concept and definitions

The definition of cyber sovereignty largely depends on the conventional political definition of nation sovereignty. State sovereignty can be defined as a state's independence from other nations, i.e., not being discipline to the sovereignty of another country, and being independent in controlling its internal affairs with no exterior interference, known as the exterior sovereignty of the state. In addition, state sovereignty is defined as an exclusive authority over any powers within its geographical region, in addition, known as the domestic sovereignty of the state. The traditional political concept of states is linked to the geographical region over which the state exercises its sovereignty. Its regulations apply to citizens and legal persons residing within, and its executive authorities have the ability to apply these regulations within its jurisdiction. (Paul. (2023. p12).

Given the contradiction between the transnational nature of cyberspace and the tangible geographical basis of traditional political sovereignty, for some time, states have been theoretically and practically excluded from exercising any degree of sovereignty in cyberspace. However, with the increasing importance of the Internet and the connection of vital political and economic interests to it, states have sought to assert their sovereignty in the cyberspace, giving rise to the concept of cyber sovereignty, with significant differences in its definition.

Generally, cyber sovereignty can be said to mean that a state imposes its sovereignty over both the physical elements of the communications and information infrastructure positioned within its borders and the activities carried out using these elements on its territory, comprising the data generated through these activities.

The concept of state cyber sovereignty is based on two main pillars. The first is that governments are responsible for cyber-attacks launched from their territory, as these attacks fall under state sovereignty. Sovereignty "grants rights to states and imposes obligations on them." Thus, states are expected to control their electronic infrastructure and prevent its use intentionally or unintentionally to harm governmental and non-governmental entities outside their borders. Consequently, the state and its citizens who participated in cyber-attacks fall under the scope of cyber sovereignty. The second pillar is that governments are responsible for their cyberspace, the security of their infrastructure, and the protection of their citizens from internal and external attacks. Furthermore, this includes their ability to defend against attacks, respond to cyber incidents, take proactive measures in cyber warfare, recover after attacks, and ensure resuming operations with minimal losses and in the shortest time possible. (Yassin. 2024, P.5)

Therefore, the recognition of state sovereignty in cyberspace, as affirmed by the United Nations General Assembly, indicates that states must respect international law and the corresponding rights and obligations of sovereignty in their use of information and communication technologies, including cyberspace. This implies that states must apply and respect all the implications of their sovereignty in all their activities within cyberspace. The General Assembly has based this on the fact that cyberspace does not exist without physical infrastructure such as: "servers, hubs, and cables", which are physically located within states and therefore fall under their control and oversight. According to what has been mentioned, cyber sovereignty is defined as the application of state sovereignty principles to cyberspace. (Rule 139, Respect for International Humanitarian Law)

Finally, a state has full cyber sovereignty over its cyberspace and cybersecurity. Cybersecurity includes the technical and administrative means used to prevent unauthorized use and misuse, as well as to restore electronic information and communication systems. This aims at ensuring the availability and continuity of information systems operations, securing the protection and confidentiality of personal data, and taking all necessary measures to protect citizens and consumers from risks in cyberspace. Subsequently, any attack executed by a state against the electronic networks of another state with the aim of disrupting the functioning of the public and private activities and facilities of the targeted state and harming its interests constitutes a violation of its sovereignty.

Hence, there is a close connection between the concept of cyber sovereignty and the concept of cyber security. Cyber security is defined as the set of technical and administrative means used to prevent unauthorized use and misuse, as well as to restore electronic information and communication systems. This aims at ensuring the availability and continuity of information systems operations, securing the protection and confidentiality of personal data, and taking all necessary measures to protect citizens and consumers from risks in cyberspace. Subsequently, any attack executed by a state against the electronic networks of another state with the aim of disrupting the functioning of the public and private activities and facilities of the targeted state and harming its interests constitutes a violation of its sovereignty. (Abdul Karim, 2022, P. 38)

3. Cyber-attacks and a State's Right to Legitimate Defense of its Cyberspace

This section of the research will primarily discuss the approach with existing rules of international law, specifically those relating to the use of force and self-defense and attempt to apply them to cyber-attacks.

Exploring the applicability of the rules of international law to cyber warfare firstly requires the legal adaptation of that issue in terms of the legitimacy or illegitimacy of cyber warfare in light of the use of force in international relations. The relationship between the right to resort to war and the law of war is inherently tense; contemporary rules of international law prohibit the use of force, except for the right of states, individually or collectively, to defend themselves, or by the use of the Security Council's law enforcement measures, through the application of Article 51 of the Charter of the United Nations.

The prohibition of the use or threat of using force among states contained in Article 2 (4) of the Charter of the United Nations is a fundamental principle of general international law. Nevertheless, this general prohibition of the use of threat or force is not absolute, as the provisions of the UN Charter have authorized the use of force in two exceptional cases provided for in the Charter through Article 2(4), which by implication authorizes the use of force in cases that do not conflict with the United Nations principles. These two exceptions are as follows: first, the state of collective security according to a resolution issued by the Security Council based on Article 42 of the Charter; and, secondly, the state of individual or collective self-defense under Article 51 of the Charter.

3.1 Self Defense Under Article 51 of the United Nations

Article 51 of the Charter of the United Nations is a crucial article addressing a state's right to self-defense in response to armed attacks, granting States the right to self-defense, including the use of force, when facing armed attacks. The interpretation and application of article 51 are still subject to debate and analysis in legal studies, as nothing in the present Charter diminishes or weakens the states' inherent right, individually or collectively, to self-defense when facing an armed aggression. Under international law, a state may use force in self-defense if there is an armed attack or imminent threat of armed attack against it. In such cases, the state has the right to respond with force to protect itself. The principle of immediacy recognizes that the use of force in self-defense must be proportionate and necessary to repel any imminent threat. This means that the response must take place promptly and without significant delay, taking into consideration the speed and urgency of the situation.

Consequently, the concept of force is not only limited to military force but also includes all forms of threats, regardless of the means used, as long as the intent is hostile. Intervention or threat of using force takes many forms, including military or financial intervention, or intervention with the aim of sabotage. Additionally, intervention can be individual or collective, explicit and direct, or it can be apparent or concealed, as in cyber-attacks.

Certain types of cyber-attacks are considered to have the same repercussions as the physical use of military force, represented in widespread destruction, causalities among military personnel and civilians and the collapse of the state's infrastructure, including:

1- Targeting state infrastructure: this covers power plants, petroleum and fuel facilities, satellites, financial and banking services, communication systems, transportation networks, broadcasting services, air and sea navigation, and targeting vital programs, such as space and nuclear programs, as targeting these systems can result in thousands of victims in no time.

2- Stealing or manipulating military information and data: in this case, networks of security and military institutions are penetrated to steal military strategies or maps of the proliferation of weapons systems or designs for military equipment, or even military databases. This is done through hacking military or national databases and stealing, forging, or electronically destroying them, which may result in casualties among civilians or at least pose a threat to global security and peace, considering that hacking these databases constitutes a threat to the state's national security.

3- Controlling military systems: it refers to controlling command and control systems remotely beyond central command of weapons, units and military battalions. The relative advantage for the cyberspace force lies in its ability to connect military units to each other and to military systems, allowing for easy exchange and flow of information, rapid issuance of military orders, and the ability to hit and destroy targets remotely. However, this mentioned advantage may turn into a weakness point if the electronic network used for this purpose is not well secured, to prevent manipulation of military systems, or redirecting opponent weapons against false or friendly targets. (Rizq Ahmed, 2018, P. 341)

These types of attacks, which have the same repercussions as the use of traditional military force, are subject to the prohibition of the use of force imposed by the United Nations Charter. Thus, this type of cyber-attacks is dealt with under Article 2, paragraph 4 of the United Nations Charter, which requires the international community's intervention in order to maintain international security and peace, and the application of sanctions stipulated by the United Nations Charter against those who violate the principle of the prohibition of the use of force. Consequently, cyber force for military purposes, which has the same repercussions as the use of traditional military force, including widespread killing, destruction of nature and state infrastructure, theft and manipulation of military information and data, and control over military systems, falls within the scope of paragraph 4 of Article 2 of the United Nations Charter.

In this context, a comparison can be made between a cyber-attack and a conventional attack in that the perpetrator of both attacks has a motive to execute the attack, and the victim in both cases can be either a natural or legal person. On the other hand, the difference between them lies in the tool used and the location of the attack. In a cyber-attack, the tool is highly technological, and the location from which the attack is launched does not require the physical movement of the perpetrator because it is carried out remotely through communication lines and networks between the attacker and the target location. Moreover, cyber-attacks are not carried out by ordinary people but by a group of computers hacking professionals through electronic networks, forming a cyber-army.

4.Conclusion

Throughout history, states have sought to exercise sovereignty over their territories and citizens locally by exercising authority over the entire population without any parallel entity, force, or authority contesting its jurisdiction. Moreover, it is important to acknowledge that the exercise of this authority varies from one state to another or, in contrast to another, by asserting known and non-negotiable sovereign territorial borders. Therefore, a fully sovereign state has the authority to exercise its powers and is not subject to any higher authority, and its decisions are enforceable within its territory, and in the face of changes in international reality, including changes in threat patterns to cyber threats.

Furthermore, there are numerous challenges hindering the understanding of cyber sovereignty and a state's right to legitimate defense of its cyberspace. The most important challenges include: the difficulty of identifying the actor, the use of computers located in more than one country to execute these attacks, and the diversity of actors involved in such attacks, ranging from states to individuals and groups. These points complicate the process of determining the legal status of the attack: is it an aggression against the sovereignty of one state by another, or merely terrorist attacks to be dealt with from the perspective of threats to international peace and security?

4.1 Study Findings:

1- This research paper concluded that relying on the general rules of International Public Law, specifically Article 51 of the United Nations Charter on self-defense, can be applied to cases of cyber-attacks.

2- The use of force or mere threats, whether traditional force or cyber force, is generally prohibited in International Law. Yet, there are some exceptions to the use of force in legitimate self-defense, as indicated in Article 51 of the

United Nations Charter, whether against military or cyber-attacks.

3- A state cannot invoke the right of self-defense against cyber-attacks unless the repercussions are similar to those resulting from physical military force, represented in widespread destruction, casualties among military personnel and civilians, and the collapse of the state's infrastructure.

4- Adapting cyber-attacks within the existing framework of International Law is highly difficult due to their unique nature, in addition to the absence of an agreed upon official legal statement regarding this phenomenon of cyber and electronic armament among states.

5- Given that cyber threats transcend borders, states cannot protect themselves effectively against these threats and, thus, protect their digital sovereignty. Hence, the necessity of international cooperation in this context becomes essential.

6- Each state has the right, based on its sovereignty over its cyberspace, to establish laws and regulations to govern cyberspace in accordance with its interests and according to international practices in force in this regard.

7- Recognizing cyberspace as a sovereign domain, with states exercising authority over it, requires physical engineering and international laws in order to function effectively.

4.2 Study Recommendations

1- Based on the findings of this research paper, there is a necessity to find an international legislation called "Cyber International Law" that applies to all United Nations member states, establishing a new international legal framework to effectively address the challenges posed by cyber-attacks.

2- Amending the concept of the use of force in the United Nations Charter to align with recent developments in the field of non-conventional weapons, especially cyber-attacks.

3- Considering any violation of sovereignty through cyber-attacks on any state as an impact on the state's infrastructure, whether carried out by official or unofficial actors, as long as the consequences of cyber-attacks include destruction, casualties among military personnel and civilians, and the collapse of the state's infrastructure.

4- Activating international cooperation, the role of international treaties, and the principle of mutual legal, judicial and security assistance in combating cybercrimes by accelerating the establishment of an effective system for international cooperation and the protection of cyberspace for any state.

5- Defining the boundaries of cyberspace in a way that states can monitor and control, as the inability to perform this function empties cyberspace of its content.

6- For activating Article 51 on cyber-attacks, it is difficult to apply the condition of immediacy in responding to the attack due to the challenges accompanying the process of identifying the attack source not before a considerable length of time. This matter could negate the logic of granting a state the right to self-defense without resorting to the Security Council, which has the primary authority in maintaining international security and peace.

References and sources

1- Abdel Sadek, A. (2016). Cyber Weapons in the Light of International Humanitarian Law. Alexandria: Alexandria Library, Future Studies Unit.

2- Abdelkarim, Y. (2024). Defining the concept of state sovereign interests to demarcate cyberspace: Validity and practical framework.

3- Cerf, V. G. (2018). The peace of Westphalia. Communications of the ACM, 61(9).

4- Chouireb, D. (2023). The Concept of Cyber Warfare and Cyber Security, Volume (11), Issue (1).

5- Cyber-attacks in light of the provisions of the rules of international humanitarian law and international conventions.

6- Donets, P., & Krynytska, N. (2022). Here Be Dragons: The Evolution of Cyberspace from William Gibson to Neal Stephenson. American, British and Canadian Studies.

7- Elbahy, R. (2018). Cyber Deterrence: The Concept, Dilemmas, and Requirements. Journal of Political Science and Law. Arab Democratic Center for Strategic Political and Economic Studies.

8- Eriksson, J., & Giacomello, G. (2022). Cyberspace in space. doi:10.4324/9781003110224-8.

9- Fadl Muhammad Al-Awdi, J. (2022). The Impact of Cyber Terrorism on National Security.

10- Gomathy, C. K., Geetha, V., & Shyam, D. (2024). Cyber Law and Cyber Crime. International Journal of Scientific Research in Engineering and Management.

11- Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering.

12- Ismail, A. K. (2022). The Impact of Cyberspace on National Security. Journal of Research and Studies, Issue 1.

13- Jalal Fadl Muhammad Al-Awdi. (2022). The Impact of Cyber Terrorism on National Security.

14- Kalafi, S. (2022). Adapting Cyber-Attacks Considering the Provisions of International Law. Academic Journal of Legal Research, Issue 13.

15- Luknar, I., & Jovanovic, F. (2024). Various types of cyber threats. Srpska politička misao.

16- Mbanaso, U., & Dandaura, Professor. (2015). The Cyberspace: Redefining A New World. Journal of Computer Engineering (IOSR-JCE).

17- Mohammed Amar, O. (2019). Electronic Warfare in International Humanitarian Law. Studies of Sharia and Law Sciences, Volume 46, Issue 3.

18- Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. IEEE Internet of Things Journal.

19- Rule 139. Respect for International Humanitarian Law, "Each party to the conflict must respect and ensure respect for international humanitarian law by its armed forces and other persons or groups acting in fact on its instructions, or under its direction or control."

20- Samoudi, R. A. (2018). The Right to Self-Defense as a Result of Cyber Attacks in Light of the Rules of Public International Law. Sharjah University Journal of Legal Sciences, Vol. 15, Issue 2.

21- Smith, K., Jones, A., Johnson, L., & Smith, M. (2018). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society.

22- Sufian, K. (2022). Adapting Cyber-Attacks Considering The Provisions of International Law. Academic Journal of Legal Research, Issue 13.

23- Sunde, I. M. (2017). Cybercrime Law.

24- Timmers, P. (2023). Sovereignty in the Digital Age.

25- Yahya, Y. S. Cyber War in the Light of International Legal Law. Legal Journal, Volume (4), Issue (4), College of Law - Cairo University.