

The Implications of Cyberwarfare for Human Rights under International Law

Halima Touati¹

¹Doctor of International Humanitarian Law and Human Rights, Abderrahmane Mira University of Bejaia, Faculty of Law and Political Sciences, halima.touati@univ-bejaia.dz

Soumission : 30/11/2025 Acceptation 03/03/2026 Publication :16/10/2026

Abstract:

This study seeks to examine the effects of cyberwarfare on human rights in light of international human rights law, against the backdrop of the rapid development of digital technology, the growing tendency of individuals and institutions to use cyberspace, and the increasing scale of cyberattacks. It aims to highlight the implications of cyberattacks for the fundamental rights and freedoms guaranteed to individuals under the international human rights legal framework, particularly the right to life, as the cornerstone and essence of all rights, physical integrity, the right to privacy, the protection of personal data, and other civil and political rights. It also addresses the impact of cyberwarfare on economic, social, and cultural rights, particularly the rights to health, work, and education, as well as individuals' livelihood security.

Keywords: Cyberwarfare, Human Rights, Cyberspace, International Law.

Introduction

The rapid development of information and communication technologies has given rise to new forms of conflict that are no longer confined to conventional military confrontations but have extended into cyberspace, which has become an arena for launching attacks against information systems, communication networks, and critical infrastructure. In this context, cyberwarfare has emerged as one of the contemporary challenges raising legal issues concerning the protection of human rights.

The danger of cyberwarfare lies in its consequences, which extend beyond disrupting technological systems or destroying data to potentially infringing fundamental rights, such as the right to life and physical integrity, the right to privacy and the protection of personal data, freedom of expression, and the right of access to information. Attacks targeting hospitals or electricity and water networks may endanger human lives, while hacking and digital surveillance operations may violate the right to privacy. Meanwhile, attacks against media outlets and communication networks may contribute to restricting freedom of expression and limiting the circulation of information.

Although international human rights law emerged before the advent of cyberspace in its present form, its general provisions remain relevant in addressing threats arising from the use of digital technology, since fundamental rights do not cease to enjoy protection merely because the violations are committed through electronic means. In this regard, protection is grounded in a set of international instruments, foremost among them the Universal

Declaration of Human Rights of 1948, the International Covenant on Civil and Political Rights of 1966, and the International Covenant on Economic, Social and Cultural Rights of 1966, in addition to the principles underpinning the protection of human rights.

The significance of studying this subject lies in the need to clarify the extent to which the rules of international law can provide effective protection for human rights amid rapid technological transformations, and to identify the areas of interaction between international obligations to respect fundamental rights and the requirements of cybersecurity. Its practical importance is also evident in light of society's growing reliance on digital infrastructure, which makes the protection of cyberspace an increasingly important component of efforts to safeguard human dignity and ensure the continued enjoyment of rights and freedoms.

Accordingly, the central research question of this study can be formulated as follows: **To what extent do the rules of international human rights law provide effective protection for human rights against the implications of cyberwarfare?**

This central question gives rise to several subsidiary questions, the most important of which are: What is meant by cyberwarfare, and what are its main legal characteristics? Which human rights are most likely to be affected by its consequences? To what extent are the rules of international human rights law applicable to cyberattacks?

To address this research problem, the study adopts the analytical method by examining international legal instruments and conventions relevant to human rights, alongside the descriptive method to define cyberwarfare and identify its characteristics. The applied method is also employed in examining the effects of cyberattacks on fundamental rights.

Accordingly, the study is divided into two main sections. The first examines the conceptual and legal framework of cyberwarfare and its relationship with the protection of human rights, while the second is devoted to investigating the implications of cyberwarfare for civil and political rights, as well as economic, social, and cultural rights, and the violations and damage resulting from cyberattacks.

Section One: The Conceptual and Legal Framework of Cyberwarfare and Human Rights

Addressing the relationship between cyberwarfare and human rights requires defining the fundamental concepts associated with it and identifying the international legal rules governing the protection of rights and freedoms in cyberspace. Rapid technological development has given rise to new forms of cyberattacks that may threaten individuals' security and privacy and impair the exercise of their fundamental rights.

In the face of these challenges, it is important to define cyberwarfare and identify its characteristics, and then examine the international legal framework that guarantees the protection of human rights in the digital environment. Accordingly, this section addresses the concept of cyberwarfare, followed by the international legal framework for protecting human rights in cyberspace.

Subsection One: The Concept of Cyberwarfare

Defining cyberwarfare is an essential step toward understanding its nature and characteristics. Given the interplay between its technical and legal dimensions, it is important to identify its

definition, principal manifestations, and effects. Accordingly, this subsection examines the concept of cyberwarfare and its fundamental characteristics.

Paragraph One: The Meaning of Cyberwarfare

It is difficult to establish a comprehensive and precise definition of cyberwarfare among international law scholars, perhaps because attacks targeting the Internet and computer systems are a relatively recent phenomenon. These attacks have been described as operations intended to disrupt or destroy information stored on computers and Internet networks. They may also target critical infrastructure, such as hospitals, banks, communication networks, security agencies, and other sensitive facilities¹

The absence of a specific definition of cyberwarfare does not mean that the subject has been neglected. Rather, several scholars have sought to define it, each according to their own intellectual perspective. International law scholar Michael N. Schmitt has defined it as **“a set of actions undertaken by a state to attack enemy information systems with the aim of influencing and damaging them, while defending its own information systems”**²

Winkfield, meanwhile, has defined cyberwarfare as **“a type of information warfare that causes disruption to an adversary’s information systems.”**

Richard Clarke, for his part, has defined cyberwarfare as **“actions through which a state penetrates the computers and networks belonging to another state, with the aim of inflicting serious damage on them or disrupting them”**³.

In his book *Cyber War*, Richard Clarke also discussed scenarios that states might resort to in the context of such warfare, including governments launching cyberattacks against electricity-generating power plants, oil pumping stations, and other sensitive targets within a state.

Cyberwarfare is also defined as a virtual war of an intangible nature, in which the instruments of conflict rely on electronic confrontations and technological software⁴. In the same context, the Group of Experts affiliated with the North Atlantic Treaty Organization (NATO), in Rule 30 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare and Cyber Operations*, defined cyberwarfare as **“all cyber operations, whether defensive or offensive, that are believed to cause human injury or death, or damage to or destruction of physical objects”**⁵

¹ Osama Sabri Mohamed, “Electronic Warfare and the Principle of Distinction in International Humanitarian Law,” p. 6, July 2019. Article available at the following website:
file:///C:/Users/mbi/Downloads/131565.pdf

² Naseeb Najib, “Cyberwarfare from the Perspective of International Humanitarian Law,” *The Critical Review of Law and Political Science*, Faculty of Law and Political Science, University of Tizi Ouzou, Vol. 16, No. 4, 2021, p. 222

³ Yahya Mufrih Al-Zahrani, “The Strategic and Legal Dimensions of Cyberwarfare,” *Journal of Research and Studies*, No. 23, 2017, p. 235

⁴ Jaloud Walid Ghassan Saeed, *The Role of Electronic Warfare in the Arab–Israeli Conflict*, Master’s thesis in Political Planning and Development, Faculty of Graduate Studies, An-Najah National University, Palestine, 2013, p. 81

⁵ Darwish Saeed, “Cyberwars and Their Impact on Human Rights: A Study in Light of the Provisions of the Tallinn Manual,” *Algerian Journal of Legal, Economic and Political Sciences*, p. 181

Based on the foregoing definitions and the conclusions that may be drawn from them, cyberwarfare can be defined as warfare conducted in cyberspace, in which virtual digital weapons are used to penetrate electronic networks and affect critical infrastructure. The concept is associated with cyberattacks carried out under military command and aimed at infiltrating electronic systems at the international level. This form of warfare is considered one of the most dangerous and threatening forms of warfare in the contemporary world, owing to the difficulty of identifying those responsible for launching such attacks, as well as the fact that, in some cases, they cannot be detected until after they have occurred.

Paragraph Two: Characteristics of Cyberwarfare

Cyberwarfare is distinguished by a set of characteristics that define its nature and methods of execution. The most significant of these characteristics can be summarized as follows:

First: The Temporal Scope of Cyberwarfare

The application of the legal rules governing cyberwarfare is linked to the existence of an armed conflict within the traditional understanding of armed conflicts. This is evident in Rule 20 of the *Tallinn Manual*, concerning the application of the law of armed conflict, which stipulates that cyber activities are subject to this body of law when conducted in the context of an armed conflict, whether international or non-international.

However, the link between cyberwarfare and armed conflicts does not preclude the possibility of cyberattacks occurring outside this framework. State practice has witnessed numerous attacks targeting the electronic systems of critical facilities, resulting in the disruption or destruction of military defence networks, the penetration of public- and private-sector networks, and damage to states' infrastructure. Some of the most notable examples are as follows:

1- The Cyberattack on Estonia

Estonia was subjected to a series of cyberattacks following the outbreak of public protests within the Russian-speaking Estonian community, triggered by the Estonian government's decision, issued on 26 April 2007, to relocate a memorial commemorating the Russian Red Army during the Second World War. This decision provoked discontent among the Russian authorities, who formally condemned it, before the Estonian government subsequently accused Russia of being behind the cyberattacks targeting the country, viewing them as an act of retaliation for that measure.

These attacks resulted in widespread disruption of numerous government and military websites. Their effects also extended to media outlets, banking websites, emergency services, and other critical facilities, thereby disrupting many essential services and preventing the population from accessing them under normal conditions.

2- The Cyberattack on Iran

During 2010 and 2011, Iranian nuclear facilities were subjected to a cyberattack involving the *Stuxnet* virus⁶, which is regarded as one of the most prominent cyberattacks targeting facilities with both civilian and military dimensions. The virus was discovered shortly before

⁶ Evelyne AKOTO, "Do State Cyberattacks Constitute Acts of Aggression under Public International Law?" Part One, *Ottawa Law Review*, Vol. 46, No. 1, 2014–2015, p. 17

the Iranian facilities were targeted, and Iranian statements accused the United States and Israel of being behind the attack ⁷

According to the Iranian account, the attack disrupted the centrifuges used for uranium enrichment, thereby affecting the progress of Iran's nuclear programme. It also had several consequences, most notably increased diplomatic tensions between Iran and both the United States and Israel, damage to Iranian industrial facilities, and technical problems that reduced the number of operational centrifuges used in the uranium enrichment programme.

Second: Cyberwarfare as a Rapidly Executed Form of Digital Warfare

Cyberwarfare is one of the most prominent manifestations of the advances achieved through the information and communications revolution, as digital technologies have become an essential tool for conducting offensive operations and achieving states' strategic objectives.

The continuous development of cyber capabilities and technologies, together with their increasing diversity and the innovation of methods for their use, has contributed to strengthening the significance of this type of warfare and its connection with states' vital interests ⁸

One of the most important characteristics of cyberwarfare is the high speed at which attacks are carried out, giving the attacking party an advantage over the defending party, particularly in view of the difficulty of detecting attacks and responding to them in a timely manner. Cyberwarfare is also characterized by the broad scope of its targets, as its effects are not confined to traditional battlefields but extend to sovereign sites, sensitive facilities, and states' critical infrastructure, making it a source of multidimensional threats.

Third: Cyberwarfare as Asymmetric Warfare

Cyberwarfare, also known as Internet warfare, is characterized by its asymmetric nature in comparison with conventional warfare, since conducting cyberattacks does not require the possession of a large military arsenal or advanced conventional combat capabilities. States, and even certain non-state actors, can now use electronic means to inflict serious damage on the systems and networks of other states, thereby posing a genuine threat to their security and vital interests.

This characteristic stems from the nature of the weapons and tools used in cyber combat, which differ from conventional weapons in terms of their means and mechanisms of impact. In this regard, Rule 41 of the *Tallinn Manual* addresses cyber weapons, which include viruses, malicious software, electronic surveillance systems, and other technological tools that can be employed to carry out cyberattacks and achieve their objectives⁹.

Subsection Two: The International Legal Framework for the Protection of Human Rights in Cyberspace

⁷ Gharib Hakim and Chergui Sabrina, "The Implications of Cyberwarfare for International Relations: A Study of the Cyberattack on Iran (Stuxnet Virus)," *Cahiers de Politique et de Droit*, Vol. 12, No. 2, 2020, p. 104

⁸ Ahmed Ashraf Al-Saeed, *Electronic Hacking*, Dar Al-Nahda Al-Arabiya, Egypt, 2013, p. 47.

⁹ Ali Abdul Rahim Al-Aboudi, "The Threat of Cyberwarfare and Its Implications for International Peace and Security," *Scientific Academic Journal*, College of Political Science, Al-Nahrain University, Baghdad, Vol. 57, Iraq, 2019, p. 99

The application of international human rights law to cyber operations relies on a set of international rules and principles that establish protection for fundamental rights and freedoms and impose obligations on states to respect these rights and ensure their enjoyment. Although these rules predate technological developments in this field, most of their provisions can be applied to cyber activities whenever the relevant conditions for their applicability are met.

Paragraph One: The Treaty-Based Foundation for the Application of International Human Rights Law to Cyber Operations

First: The Universal Declaration of Human Rights of 1948

The Universal Declaration of Human Rights of 1948 explicitly enshrines numerous rights inherent to every human being and emphasizes the need to ensure that they are not violated. Article 12 stipulates that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence. Article 19 also guarantees freedom of opinion and expression, including the right to receive and impart information and ideas through various media of expression. These rights and their provisions become particularly important when addressing cyber operations targeting personal communications, restricting the dissemination of information, or infringing individuals' freedom to express their opinions¹⁰.

Second: The International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights of 1966 provides a binding treaty-based framework for States Parties. Article 17 prohibits arbitrary interference with privacy and correspondence, while Article 19 guarantees freedom of expression and establishes the conditions under which restrictions on this freedom may be imposed¹¹.

Third: The International Covenant on Economic, Social and Cultural Rights

The International Covenant on Economic, Social and Cultural Rights is no less important than the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, particularly when cyber operations affect healthcare services, educational services, or other rights relating to economic, social, and cultural rights¹².

In addition to treaty provisions, the relevant framework also encompasses resolutions and interpretations issued by United Nations bodies. Human Rights Council Resolution 20/8, adopted on 5 July 2012, on the promotion, protection and enjoyment of human rights on the Internet, particularly freedom of expression, reaffirmed the importance of protecting human

¹⁰ For further details, see Articles 12 and 19 of the *Universal Declaration of Human Rights*, adopted by the United Nations General Assembly under Resolution No. 217 A (III), dated 10 December 1948. Algeria declared its accession to the Declaration by incorporating it into its first Constitution on 10 September 1963, *Official Gazette of the People's Democratic Republic of Algeria*, No. 64, issued on 10 September 1963

¹¹ *International Covenant on Civil and Political Rights*, adopted by the United Nations General Assembly under Resolution No. 2200 A (XXI), dated 16 December 1966, and entered into force on 23 March 1976. Algeria ratified the Covenant pursuant to Decree No. 89-67, *Official Gazette of the People's Democratic Republic of Algeria*, No. 20, issued on 17 May 1989

¹² *International Covenant on Economic, Social and Cultural Rights*, adopted by the United Nations General Assembly under Resolution No. 2200 A (XXI), dated 16 December 1966, and entered into force on 3 January 1976. Algeria ratified the Covenant pursuant to Decree No. 89-67, *Official Gazette of the People's Democratic Republic of Algeria*, No. 20, issued on 17 May 1989

rights in the digital environment. Similarly, Resolution 28/16, adopted on 26 March 2015, addressed the right to privacy in the digital age.

Paragraph Two: The Role of Customary Rules and General Principles of International Law in Protecting Human Rights during Cyber Operations

In addition to the legal basis established by international human rights treaties, another basis for applying international human rights law to cyber operations derives from a set of legal principles governing the exercise of states' powers, as well as customary rules that reinforce the legal protection of these rights.

First: The Role of International Customary Rules in Protecting Human Rights during Cyber Operations

International customary rules regulate the conduct and practices of states in matters that have not been addressed in sufficient detail or explicitly by international treaties. With regard to military operations, the importance of these rules lies in reaffirming the principle that technological development does not exempt states from their existing international obligations. Ensuring the continued application of human rights protection rules in cyberspace is therefore an important element in maintaining the protection of individuals against violations that states may commit through digital means, such as arbitrary interference with private life¹³

Accordingly, where a customary rule protects a particular right, the transfer of an activity that may infringe that right from the physical sphere to the digital sphere does not eliminate the legal protection afforded to it.

Second: The Role of General Principles of International Law in Protecting Human Rights during Cyber Operations

Under Article 38 of the Statute of the International Court of Justice, general principles of law constitute one of the sources of international law. The work of the International Law Commission further indicates that, as a general rule, general principles of law are not subject to a hierarchical ranking in relation to treaties and customary international law.

Among the fundamental principles that constitute the essential foundation for the protection of human rights under all circumstances are the following:

1/ The Principle of Respect for Human Dignity

The principle of respect for human dignity constitutes a fundamental basis for the protection of human rights. Under all circumstances, cyber operations must remain subject to international obligations that protect individuals against arbitrary treatment. This principle is reflected in the prohibition of using digital technologies to target individuals and deprive them of their rights, while ensuring respect for rights and freedoms when using surveillance systems and collecting and analysing data.

2/ The Principle of the Universality of Human Rights

This principle is based on the premise that human rights are inherent to individuals by virtue of their humanity. These rights do not cease to apply when activities move from the physical

¹³ United Nations Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, Resolution No. A/HRC/RES/32/13, 2016, p. 2

sphere to the digital sphere¹⁴. The United Nations Human Rights Council has endorsed this approach through Resolution No. 20/8, which affirmed the need to protect rights enjoyed in the physical world both online and offline¹⁵.

Accordingly, cyberspace cannot be regarded as a domain exempt from the international rules governing the protection of human rights.

Section Two: The Implications of Cyberwarfare for the Exercise of Human Rights and Fundamental Freedoms

The rapid development of digital technology has given rise to increasing cyber threats, which have become a challenge to the protection of human rights and fundamental freedoms. The seriousness of these attacks lies in their far-reaching effects on various categories of rights, including civil and political rights, as well as economic, social, and cultural rights. They may infringe privacy and freedom of expression, disrupt essential services, and restrict the enjoyment of the rights to work, education, and health.

In view of these effects, it is important to examine the implications of cyberwarfare for the various categories of fundamental rights. Accordingly, this section addresses the implications of cyberattacks for civil and political rights, followed by their implications for economic, social, and cultural rights.

Subsection One: The Implications of Cyberwarfare for Civil and Political Rights

Civil and political rights, also known as first-generation rights, are fundamental rights intended to protect human dignity and individual freedoms. They include the right to life, the right to physical integrity, the right to privacy, freedom of expression, and the right of access to information. These rights are enshrined in several international instruments, foremost among them the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966.

With the advent of digital technology, the protection of these rights has come to face numerous unprecedented challenges, as cyberattacks can extend beyond the technical sphere to affect individuals' lives and freedoms, either directly or indirectly. Disruptions to hospital systems or electricity networks may threaten life and physical integrity, while breaches of databases may expose personal information. Meanwhile, attacks targeting communication networks and media platforms may restrict freedom of expression and access to information.

Paragraph One: The Impact of Cyberwarfare on the Right to Life and Physical Integrity

The right to life is regarded as the essence of human rights, as it constitutes a necessary condition for the enjoyment of other rights and freedoms. Protecting this right in the digital age presents several challenges, as such protection is no longer limited to preventing direct

¹⁴ Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the International Covenant on Civil and Political Rights*, Document No. CCPR/C/21/Rev.1/Add.13, 2004, para. 4

¹⁵ United Nations Human Rights Council, *The Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, Resolution No. A/HRC/RES/20/8, 2012, para. 1

physical attacks against individuals but may also extend to addressing risks arising from attacks on the digital systems upon which essential services depend.

The danger of cyberwarfare lies in its potential to cause physical damage and human harm through unconventional means. An attack may target an information system controlling a critical facility, producing consequences that affect people's lives and physical integrity, even where the attack does not involve the direct use of conventional weapons ¹⁶.

Cyberattacks against critical infrastructure, such as hospitals, electricity and water networks, communication systems, and transport systems, constitute some of the most serious threats to the right to life and physical integrity because of their direct connection to individuals' daily lives. A cyberattack targeting an information system that controls electricity supplies, for example, may cause medical equipment and intensive care units to stop functioning or be disrupted, as well as lead to errors in patient data, potentially increasing risks to patients. Similarly, attacks targeting water distribution systems may disrupt the supply of safe drinking water, thereby creating health risks for the population. The consequences of cyberattacks may also affect individuals' physical integrity directly or indirectly when industrial machinery and control systems are targeted ¹⁷.

The right to life, liberty, and personal security is enshrined in Article 3 of the Universal Declaration of Human Rights, which provides as follows: **"Everyone has the right to life, liberty and security of person."** Furthermore, Article 6(1) of the International Covenant on Civil and Political Rights stipulates that the right to life is inherent in every human being, that this right shall be protected by law, and that no one shall be arbitrarily deprived of their life.

Accordingly, the right to life entails not only the obligation to refrain from directly causing death but also the obligation to protect individuals by maintaining and safeguarding the essential services necessary for the preservation of human life.

Paragraph Two: The Impact of Cyberwarfare on the Right to Privacy and the Protection of Personal Data

The right to privacy is one of the fundamental rights that guarantees individuals protection against unlawful interference in their private lives, including their correspondence and personal data. The importance of protecting this right has increased significantly in the digital age as individuals and institutions increasingly rely on digital technologies to store personal data and use electronic means extensively for communication and information exchange.

The right to privacy and the protection of personal data may be affected by cyber operations targeting mobile phones, computers, databases, and communication networks through hacking and espionage intended to obtain confidential and personal information without the consent of its owners and use it for intelligence, strategic, or coercive purposes against

¹⁶ *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position*, document submitted to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and to the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019, pp. 4–5

¹⁷ *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, ICRC Expert Meeting, 21–22 January 2020, Geneva, pp. 20–21.

targeted entities. Sensitive data that may be compromised include health information, financial data, administrative records, identity information, communication records, and information relating to members of the armed forces, public officials, and other individuals. Moreover, the consequences of such breaches extend beyond the loss of confidentiality and may include identity theft, blackmail, discrimination, defamation, and the exposure of data subjects to security risks. The disclosure of personal data belonging to individuals working in sensitive facilities, such as hospitals or humanitarian organizations, may expose them or their families to additional risks ¹⁸.

The right to privacy is internationally recognized. Article 12 of the Universal Declaration of Human Rights stipulates that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, or to attacks upon their honour and reputation. It also affirms their right to legal protection against such interference or attacks. Similarly, Article 17 of the International Covenant on Civil and Political Rights prohibits arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence, as well as unlawful attacks on their honour and reputation, while guaranteeing the right to legal protection against such interference or attacks. However, when examining these rights, it is necessary to distinguish between the right to privacy as a fundamental right and personal data protection as a legal field encompassing rules governing the collection, processing, storage, security, and disclosure of personal data ¹⁹.

From a legal perspective, not every unauthorized access to data constitutes a violation of international human rights law. The legal characterization depends on the nature of the conduct, the entity responsible for it, the circumstances in which it occurred, and the extent to which it interferes with a legally protected right. Nevertheless, the unauthorized intrusion into personal data may constitute an infringement of privacy and may also violate data protection legislation or cybercrime laws, depending on the applicable domestic legislation. This does not, however, preclude the widespread use of cyber surveillance without adequate safeguards, which may expose intimate details of individuals' private lives, including their communications, relationships, activities, and opinions ²⁰.

Paragraph Three: The Implications of Cyberwarfare for Freedom of Expression and the Right of Access to Information

The digital space and digital tools, such as the Internet, social networking sites, and electronic media platforms, have facilitated the exercise of freedom of expression and the right of access to information. However, the growing reliance on these tools has also made them a domain through which operations aimed at influencing information can be carried out. In the

¹⁸ CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*

¹⁹ United Nations Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, para. 10

²⁰ United Nations Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, paras. 3–4

context of cyberwarfare, such operations may take various forms, including hacking media institutions, disrupting news websites, blocking digital services, taking over accounts, manipulating published content, or disseminating disinformation with the aim of influencing public opinion. The legal implications of these practices vary according to their nature, the actors responsible for them, and the context in which they occur.

As fundamental pillars of societies that uphold civil and political rights, the right of access to information and freedom of expression have their legal basis in Article 19 of the Universal Declaration of Human Rights, which provides as follows: *“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”*²¹. Article 19 of the International Covenant on Civil and Political Rights also enshrines the right to hold opinions without interference and the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, whether orally, in writing or in print, in the form of art, or through any other media of one’s choice²².

These rights may be affected by cyber operations targeting communication networks, news websites, and platforms on which individuals rely to obtain and disseminate information. Such targeting may disrupt the publication of news, prevent journalists from accessing their sources, or deprive populations of access to essential information. When communication network services are interrupted as a result of a cyberattack, the impact may extend beyond the disruption of personal communications to include difficulties in accessing official alerts, public services, and humanitarian information. Similarly, hacking a media website may result in the publication of fabricated content under its name, potentially undermining public trust in the information disseminated²³.

Subsection Two: The Implications of Cyberwarfare for Economic and Social Rights

Economic, social and cultural rights, also known as second-generation human rights, constitute an integral part of the human rights framework and aim to achieve social justice and provide the conditions necessary for a dignified life. Technological development and increasing reliance on digital systems have given rise to new challenges that threaten individuals’ ability to enjoy these rights. As cyber operations have become increasingly prevalent and are no longer limited to disrupting information systems, economic institutions, public utilities, and digital infrastructure have become targets. Vital sectors falling within the scope of these rights, including education, employment, culture, and healthcare, are increasingly exposed to cyberattacks, potentially depriving individuals of essential services.

Paragraph One: The Impact of Cyberwarfare on the Right to Health

The right to health is directly affected by cyberattacks, given the increasing reliance of healthcare institutions on digital systems to store medical records, schedule appointments, operate certain medical equipment, and manage emergency services. Hacking or disrupting

²¹ See the Universal Declaration of Human Rights of 1948, op. cit

²² For further details, see Article 19 of the International Covenant on Civil and Political Rights, op. cit

²³ United Nations Human Rights Committee, General Comment No. 34: Article 19-Freedoms of Opinion and Expression, UN Doc. CCPR/C/GC/34, 12 September 2011, paras. 11, 13 and 15.

these systems may lead to delays in diagnosis and treatment, the cancellation of certain medical procedures, and difficulties in accessing medicines and essential services, potentially endangering patients' lives, particularly in critical cases.

The effects of these attacks are not limited to the continuity of healthcare services but also extend to the confidentiality and integrity of medical data, as hacking or tampering with health records may infringe upon patients' privacy and undermine the accuracy of medical decisions²⁴. Like other rights guaranteed to individuals under international law, the right to health has its legal basis in Article 12 of the International Covenant on Economic, Social and Cultural Rights, which recognizes the right of everyone to the enjoyment of the highest attainable standard of physical and mental health²⁵. General Comment No. 14 of the Committee on Economic, Social and Cultural Rights further clarifies the elements of this right, particularly the availability, accessibility, acceptability, and quality of healthcare services²⁶.

Paragraph Two: The Implications of Disrupting Digital Infrastructure for the Right to Education and Work

On the basis of Article 6 and Articles 13 and 14 of the International Covenant on Economic, Social and Cultural Rights, it can be concluded that the right to education and the right to work are among the most important internationally protected rights belonging to the second generation of human rights²⁷. As educational processes have become increasingly dependent on e-learning platforms, registration and examination systems, student databases, and electronic payment systems for tuition fees, transportation, and university services, disrupting or hacking digital systems may interfere with administrative registration, cause data loss, and make lessons and educational materials difficult to access. It may also affect payment systems and banking services. This inevitably reduces students' opportunities to pursue their studies regularly. Accordingly, cyberattacks that disrupt services essential to education may threaten the effective enjoyment of this right²⁸.

Furthermore, the reliance of economic and commercial institutions on digital systems has made many jobs dependent on the integrity of databases, accounting and payment systems, and platforms for managing employees, goods, and services. Consequently, disrupting these

²⁴ World Health Organization (WHO), *Examining the Threat of Cyber-Attack on Health Care During the COVID-19 Pandemic*, Geneva, 2024

²⁵ For further details, see Article 12 of the International Covenant on Economic, Social and Cultural Rights, adopted by the United Nations General Assembly under Resolution No. 2255 (A/XXI) on 16 December 1966, which entered into force on 23 March 1976 and was ratified by Algeria pursuant to Decree No. 89-67, *Official Gazette of the People's Democratic Republic of Algeria*, No. 20, issued on 17 May 1989

²⁶ Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The Right to the Highest Attainable Standard of Health*, UN Doc. E/C.12/2000/4, United Nations, 2000, para. 12

²⁷ For further details, see Articles 6, 13 and 14 of the International Covenant on Economic, Social and Cultural Rights of 1966

²⁸ *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position*, document submitted to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and to the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019

systems through cyberattacks may bring certain professional activities to a halt. Such disruptions may also affect the payment of workers' wages, transactions between employers and employees, and workers' social security coverage ²⁹.

Paragraph Three: The Effects of Cyberwarfare on Individuals' Livelihood Security

Livelihood security is one of the fundamental pillars of protecting human dignity and ensuring the effective enjoyment of economic and social rights, as it is linked to an individual's ability to meet basic needs on a regular basis, including food, housing, clothing, healthcare, water, and energy. Such security is not achieved merely by an individual having a financial income; it also requires the stability of essential services, the regular functioning of economic transactions, the continuity of supplies, and access to necessary resources and goods.

Livelihood security has become increasingly dependent on the integrity of information systems and electronic networks amid the digital transformation affecting various vital sectors. Banking services, payment systems, electricity and water distribution networks, food and pharmaceutical stock management, and social assistance programmes now rely, to varying degrees, on digital infrastructure. Although digitalisation generally facilitates transactions and improves the efficiency of service delivery, it has also created new vulnerabilities that cyberattacks can exploit to disrupt economic activities, impair the functioning of essential facilities, or gain unauthorised access to funds and personal data. Consequently, the effects of cyberwarfare on livelihood security are not limited to direct technical or financial losses; they may also extend to depriving individuals of certain essential services, reducing their ability to meet basic needs, and exacerbating their economic and social vulnerability ³⁰.

The legal basis for this issue is found in Article 11 of the International Covenant on Economic, Social and Cultural Rights, which recognises the right of everyone to an adequate standard of living for themselves and their family, including adequate food, clothing and housing, as well as the continuous improvement of living conditions. This issue is also connected to Article 9 of the same Covenant, concerning the right to social security, and Article 12, concerning the right to health, given the interrelationship between livelihood stability and the ability to enjoy these rights ³¹.

Conclusion

The study of the implications of cyberwarfare for human rights under international law demonstrates that technological development, despite the opportunities it offers for progress, communication, and service improvement, has also given rise to new forms of threats affecting individuals' fundamental rights and freedoms. Violations of human rights are no

²⁹ Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The Right to Social Security (Article 9 of the Covenant)*, UN Doc. E/C.12/GC/19, 4 February 2008.

³⁰ International Committee of the Red Cross, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts: ICRC Expert Meeting*, Geneva, 21–22 January 2020, published on 7 June 2021. The report addresses risks to civilian services, pp. 21 and 24

³¹ See the aforementioned articles of the International Covenant on Economic, Social and Cultural Rights of 1966

longer confined to traditional physical acts; cyberspace has become an environment in which harm may arise that affects civil and political rights, as well as economic, social and cultural rights.

The study has shown that the danger of cyberwarfare lies in the diversity and interconnectedness of its effects. Targeting information systems and critical infrastructure may disrupt essential services and harm individuals' interests, while the consequences of cyberattacks may extend beyond the digital sphere to affect the daily lives of populations and their social and economic stability.

From a legal perspective, the study concludes that the use of cyber means does not, in itself, place the acts committed outside the scope of international law. The general rules of international human rights law remain relevant to the protection of rights and freedoms in the digital environment. The study also demonstrates that the effectiveness of international human rights protection against cyberwarfare depends not merely on the existence of legal rules, but also on the extent to which States implement their obligations, their capacity to protect digital infrastructure, the adoption of effective preventive and responsive measures, the continuity of essential services, the protection of personal data, and the provision of remedies for affected individuals.

Based on the foregoing, the fundamental challenge posed by cyberwarfare lies not in technological development itself, but rather in how technology is used and the extent to which the applicable legal rules are respected. Accordingly, ensuring the protection of human rights in cyberspace requires an integrated approach combining the development of legal rules, the strengthening of enforcement mechanisms, and the improvement of States' technical and institutional capacities.

The study therefore recommends developing effective mechanisms for investigating violations and determining responsibility for them, requiring relevant institutions to adopt appropriate measures to protect data and critical infrastructure, and ensuring the existence of plans to maintain the continuity of healthcare, educational, and social services in the event of cyberattacks. It also recommends intensifying legal and applied research on cyberwarfare to keep pace with technological developments and strengthen the effective protection of human rights.

Consequently, building a safer cyberspace that respects human rights remains a shared responsibility requiring States to comply with international law, cooperation among international and national institutions, and the participation of stakeholders in the digital sector. These efforts aim to reduce the harm caused by cyberattacks and ensure that technology does not become a means of undermining the rights and freedoms recognised under international law. However, it should be noted that the mere occurrence of a cyberattack does not automatically constitute a human rights violation; rather, a legal assessment is required to establish the relevant facts, determine the resulting harm, and assess the applicability of the relevant legal rules.

References

- Ahmed Ashraf Al-Saeed, *Electronic Hacking*, Dar Al-Nahda Al-Arabiya, Egypt, 2013, p. 47.
- Ali Abdul Rahim Al-Aboudi, “The Threat of Cyberwarfare and Its Implications for International Peace and Security,” *Academic Scientific Journal*, College of Political Science, Al-Nahrain University, Baghdad, Vol. 57, Iraq, 2019, p. 99.
- *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, ICRC Expert Meeting, 21–22 January 2020, Geneva, pp. 20–21.
- Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The Right to the Highest Attainable Standard of Health*, UN Doc. E/C.12/2000/4, United Nations, 2000, para. 12.
- Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The Right to Social Security (Article 9 of the Covenant)*, UN Doc. E/C.12/GC/19, 4 February 2008.
- Drouiche Saïd, “Cyberwarfare and Its Impact on Human Rights: A Study in Light of the Provisions of the Tallinn Manual,” *Algerian Journal of Legal, Economic and Political Sciences*, p. 181.
- Evelyne AKOTO, “Do State Cyberattacks Constitute Acts of Aggression under Public International Law? Part One,” *Ottawa Law Review*, Vol. 46, No. 1, 2014–2015, p. 17.
- For further details, see Article 12 of the *International Covenant on Economic, Social and Cultural Rights*, adopted by the United Nations General Assembly under Resolution No. 2255 (A/XXI) on 16 December 1966, entered into force on 23 March 1976, and ratified by Algeria pursuant to Decree No. 89-67, *Official Gazette of the People's Democratic Republic of Algeria*, No. 20, issued on 17 May 1989.
- For further details, see Article 19 of the *International Covenant on Civil and Political Rights*, op. cit.
- For further details, see Articles 12 and 19 of the *Universal Declaration of Human Rights*, adopted by the United Nations General Assembly under Resolution No. 7/3 A (III) on 10 December 1948. Algeria declared its accession to the Declaration by incorporating it into its first Constitution on 10 September 1963, *Official Gazette of the People's Democratic Republic of Algeria*, No. 64, issued on 10 September 1963.
- For further details, see Articles 6, 13 and 14 of the *International Covenant on Economic, Social and Cultural Rights* of 1966.
- Gharib Hakim and Cherki Sabrina, “The Implications of Electronic Warfare for International Relations: A Study of the Cyberattack on Iran (Stuxnet Virus),” *Cahiers de Politique et de Droit*, Vol. 12, No. 2, 2020, p. 104.
- Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)—The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*.

- Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, UN Doc. CCPR/C/21/Rev.1/Add.13, 2004, para. 4.
- International Committee of the Red Cross, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts: ICRC Expert Meeting*, Geneva, 21–22 January 2020, published on 7 June 2021. The report addresses risks to civilian services, pp. 21 and 24.
- *International Covenant on Civil and Political Rights*, adopted by the United Nations General Assembly under Resolution No. 2255 (A/XXI) on 16 December 1966, entered into force on 23 March 1976, and ratified by Algeria pursuant to Decree No. 89-67, *Official Gazette of the People's Democratic Republic of Algeria*, No. 20, issued on 17 May 1989.
- *International Covenant on Economic, Social and Cultural Rights*, adopted by the United Nations General Assembly under Resolution No. 2255 (A/XXI) on 16 December 1966, entered into force on 23 March 1976, and ratified by Algeria pursuant to Decree No. 89-67, *Official Gazette of the People's Democratic Republic of Algeria*, No. 20, issued on 17 May 1989.
- *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position*, document submitted to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and to the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019, pp. 4–5.
- *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position*, document submitted to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and to the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019.
- Jaloud Walid Ghassan Saeed, *The Role of Electronic Warfare in the Arab–Israeli Conflict*, Master's thesis in Political Planning and Development, Faculty of Graduate Studies, An-Najah National University, Palestine, 2013, p. 81.
- Nassib Najib, “Cyberwarfare from the Perspective of International Humanitarian Law,” *Critical Journal of Law and Political Science*, Faculty of Law and Political Science, University of Tizi Ouzou, Vol. 16, No. 4, 2021, p. 222.
- Osama Sabri Mohammed, *Electronic Warfare and the Principle of Distinction in International Humanitarian Law*, p. 6, July 2019. Article available at the following website:
<file:///C:/Users/mbi/Downloads/131565.pdf>
- See the aforementioned articles of the *International Covenant on Economic, Social and Cultural Rights* of 1966.
- See the *Universal Declaration of Human Rights* of 1948, op. cit.

- United Nations Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)—The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, para. 10.
- United Nations Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)—The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, paras. 3–4.
- United Nations Human Rights Committee, *General Comment No. 34: Article 19—Freedoms of Opinion and Expression*, UN Doc. CCPR/C/GC/34, 12 September 2011, paras. 11, 13 and 15.
- United Nations Human Rights Council, *The Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, Resolution No. A/HRC/RES/20/8, 2012, para. 1.
- United Nations Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, Resolution No. A/HRC/RES/32/13, 2016, p. 2
- World Health Organization (WHO), *Examining the Threat of Cyber-Attack on Health Care During the COVID-19 Pandemic*, Geneva, 2024.
- Yahya Mufreh Al-Zahrani, “The Strategic and Legal Dimensions of Cyberwarfare,” *Journal of Research and Studies*, No. 23, 2017, p. 235.