

Cyber Warfare in Light of Technological Transformations: An Analysis of Concept and Content

Aouid Tounes¹, Nouasria Maroua^{*2}

¹ University of Oum Elbouaghi (Algeria), aouidi.tounes@univ-ueb.dz

² University of Oum Elbouaghi (Algeria), nouasria.maroua@univ-ueb.dz

Received: 27/10/2025

Accepted: 26/11/2025

Published: 22/12/2025

Abstract:

In light of the rapid advancement of technology and the profound transformations it has brought across political, economic, and social sectors, armed conflicts have undergone significant evolution, technological innovation has fundamentally altered the legal, strategic, and operational dimensions of warfare, giving rise to new forms of conflict that challenge traditional conceptions of combat, among these emerging paradigms, cyber warfare stands out as a pressing and complex issue on the contemporary international agenda, unlike conventional conflicts, cyber warfare takes place within a virtual domain that transcends geographic boundaries, allowing both state and non-state actors to project power, exert influence, and pursue strategic objectives with unmatched speed and scope.

As a result, cyberspace has become a pivotal arena for exercising national power, achieving political, economic, and military goals, and asserting technological supremacy, this shift has also created novel legal, ethical, and operational challenges, compelling states to adapt their security, defense, and international cooperation strategies accordingly.

Keywords : Technological Development, Cyber Warfare, Cybercrimes, Cyber Attack, Traditional Wars.

1. INTRODUCTION

Humanity today is witnessing a profound transformation driven by a massive technological revolution that has brought about a fundamental change in various aspects of human, economic, social, and intellectual life. The impact of this digital revolution has extended to both individuals and societies alike, to the extent that it has become difficult to find a field untouched by its far-reaching effects.

^{*} *Corresponding author*

On this basis, it becomes evident that contemporary technological developments have played an active role in achieving human progress and welfare, both in times of peace and during armed conflicts, due to their direct impact on enhancing the economic and military capabilities of States. However, this very progress has also altered the nature of traditional warfare and led to the emergence of new patterns of conflict, most notably cyber warfare, which relies on the exploitation of digital technologies and cyberspace as means to target a State's critical infrastructure, through the penetration or disruption of its electronic networks, resulting in both material and moral damages affecting individuals and property alike.

In this context, cyber operations have increased remarkably, including those conducted or sponsored by States, giving rise to complex legal issues related to the determination of international responsibility, the regulation of the principle of sovereignty in cyberspace, and the assurance of information security for States.

Accordingly, cyber warfare represents a newly emerging form of contemporary conflict that employs digital technologies and electronic systems as tools to confront States, entities, or individuals, through a range of activities that include cyberattacks, cyber propaganda, acts of sabotage, and cyber espionage.

These attacks are often carried out by State-sponsored actors or independent organizations seeking to achieve political, economic, or military objectives, thereby extending their repercussions to national economies, national security, and even the daily lives of individuals.

In light of this, combating cyber warfare requires effective international cooperation and continuous efforts to enhance cybersecurity through the modernization of technical infrastructure and information systems, the training of qualified personnel in data protection, and the establishment of comprehensive preventive strategies to counter potential cyberattacks.

Based on the foregoing, the main research problem of this study can be formulated as follows: **How has contemporary technological advancement contributed to reshaping the nature and patterns of warfare?**

From this central question arise several subsidiary questions that the study seeks to answer, namely:

What is meant by the concept of cyber warfare?

What are the distinctive characteristics of cyber warfare that differentiate it from other forms of modern conflict?

What are the legal and practical implications of cyber warfare across various sectors?

2. Cyber Warfare – Definition and Characteristics

Given the novelty of the term cyber warfare and its continuous evolution within the context of the digital revolution, there is still no universally accepted or comprehensive legal definition of it, the definitions proposed so far vary according to the intellectual premises and analytical approaches adopted by jurists and scholars.

In order to achieve a precise understanding of this subject and to elucidate its legal implications, a methodological approach requires first defining the concept and objectives of war within its traditional framework, and then proceeding to analyze the meaning and characteristics of cyber warfare.

This sequence allows for a clear demonstration of the historical and substantive development that the concept of war has undergone in the context of public international law.

2.1 Definition of War

War constitutes one of the most prominent and long-standing forms of organized violence in international relations, throughout history, it has represented the primary means for resolving disputes and achieving interests among States.

Despite the abundance of definitions addressing this concept, determining its precise meaning remains problematic due to the diversity of legal and political perspectives through which it has been examined.

2.1.1 The Meaning of War

2.1.1.1 The Meaning of War in Traditional Law

Within the framework of traditional law, war was regarded as a legitimate instrument for achieving the political or economic objectives of States. In its early stages, it was not subject to any specific legal regulation; rather, it was characterized by disorder and arbitrariness in its means and methods, indeed, many major powers such as France and Germany emerged within the context of expansionist wars, which made war at that time a natural phenomenon in international relations.

The very principle of war was not condemned per se; what was denounced were its adverse consequences, such as economic devastation and human losses. Consequently, jurists and legal scholars were divided concerning the legitimacy of war: some considered it a sovereign right of States to defend their interests, while others emphasized the necessity of subjecting it to legal and ethical constraints that would limit its use¹.

¹ Mohamed Sami Genina, Research on the Law of War, Journal of Law and Economics, No. 1, Egypt, 1941, p. 8

2.1.1.2 The Meaning of War in Modern Law

The Meaning of War in Modern Law Within the framework of modern international law, the use of force in international relations was not prohibited prior to 1914. However, international legal scholarship gradually began to restrict such use and to define the concept of war with greater precision, while seeking to codify it and render it more humane through the establishment of legal and ethical norms governing the conduct of belligerent parties.

The First World War marked a qualitative turning point in the perception of war, as aggressive war came to be regarded as synonymous with unlawful war¹.

Accordingly, war can be defined, within its traditional framework, as:

“An armed conflict between two opposing parties belonging to different States, whereby the belligerent States defend their interests, objectives, and rights.”

In its modern conception, however, this definition has expanded to encompass any armed conflict of an international character—whether or not it is formally designated as a war—so long as it involves the element of organized armed confrontation between entities possessing international legal personality².

2.1.2 The Objectives of War

As for the objectives of war, they may be summarized as follows:

- Supporting or weakening an existing political or social system, or seeking to bring about its change.
- Achieving economic or strategic interests related to resources or vital geographic locations.
- Expanding influence or establishing control over new territories in order to secure the State’s needs and safeguard its interests in foreign markets³.

2.2 Cyber Warfare

Since the emergence of the Internet as a modern global means of communication, it has undergone profound transformations that have significantly influenced the nature of relations between individuals and States within the informational space, this cyberspace has become an extensive arena for interaction and mutual influence.

¹ Saïd Chayeb, *The Effects of War on International Treaties*, Master’s Thesis in Law, Faculty of Law, University of Algiers 1, Academic Year 2012–2013, p. 13.

² Mohamed Abu Khalif, *Definition of War*, article available at: <https://mawdoo3>, accessed on June 2, 2024, at 16:39.

³ Alia Mahmoud Mohamed El-Leithi, *Modern Trends in the Theory of Wars: An Application to the U.S. War on Afghanistan*, article available at: <https://jsst.journals.ekb.eg>, accessed on June 4, 2024, at 08:48.

This newly established reality has given rise to a new form of criminal conduct known as cybercrime, characterized by the serious threats and substantial harm it inflicts upon the security and stability of States¹, Consequently, it becomes essential to examine the meaning of cyber warfare and to identify its defining characteristics.

2.2.1 The Meaning of Cyber Warfare

The term “**cyber**” is linguistically derived from the Greek word *kybemetes*, which means “to steer” or “to control remotely.”

From a terminological standpoint, Michael N. Schmitt defines cyber-attacks as:

“Actions undertaken by a State to attack the information systems of an adversary with the purpose of influencing or damaging them, while simultaneously defending its own information systems.”²

Cyber-attacks are also defined as:

“Electronic hostilities launched by a State or non-State actors, targeting the informational infrastructure of other States, with overlapping political, economic, or criminal objectives.”³

In the same context, cyber warfare has been defined as:

“A military operation involving the use of electromagnetic energy to exploit communications and network-based systems, as well as their associated infrastructures.”⁴

Thus, it becomes evident that the distinctive feature of cyber warfare lies in its nature as an extension of traditional warfare—where power is exercised through digital means and information networks rather than conventional physical instruments of force.⁵

Despite the relative convergence of the various definitions of cyber warfare in substance, legal scholarship concurs that the term remains surrounded by a degree of ambiguity and lack of precision, much like the very notion of cyberspace itself, some jurists have defined cyber warfare in terms of the means and instruments employed,

¹ Chouib Djilali et al., *The Concept of Cyber Warfare and Cybersecurity*, *Journal of Rights and Freedoms*, Vol. 11, No. 1, 2023, p. 160.

² Yahya Yassin Saoud, *Cyber Warfare in Light of the Requirements of International Law for Sciences*, *The Legal Journal*, Cairo University, Vol. 4, No. 4, 2018, p. 84.

³ Abdel Moneim Moneeb, *Cyber Warfare and Inter-State Conflict*, Afaaq Al-Maarefa Publishing and Distribution, Saudi Arabia, p. 234.

⁴ An'am Abdul-Ridha Sultan Al-Okabi, *The Employment of Cyber Wars in the Development of the Concept of Power among Major States*, *Political Issues Journal*, Issue No. 73, p. 428.

⁵ Islam Ramadan Raheeb, *Cyber Warfare in Light of International Law*, *Journal of Legal and Economic Research*, Beni Suf University, Vol. 36, No. 1, p. 119.

namely electronic and digital technologies, others have approached the concept from the perspective of its objectives and underlying military strategy, viewing cyber warfare as an activity aimed at achieving strategic or tactical goals within the framework of modern armed conflicts¹.

Accordingly, in order to determine the precise meaning of cyber warfare, it is necessary to examine its fundamental components:

- **Cyberspace:**

Cyberspace is defined as the virtual world of computers or the electronic medium used to facilitate communication through a large computer network composed of several interconnected sub-networks spread across the globe².

The U.S. Department of Defense defines it as “a domain characterized by the use of computers and other electronic devices to store, modify, and exchange data through networked systems and the associated physical infrastructures; it constitutes an operational domain with distinctive characteristics.”³

- **Cyber Power:**

Cyber power represents the ability to achieve desired outcomes through the use of electronically interconnected information resources within cyberspace.

In another sense, it is the capability to employ cyberspace to create advantages and exert strategic influence over events in other operational environments through the various instruments of power.

- **Cyber Strategy:**

Cyber strategy refers to the development and employment of the necessary capabilities to operate within cyberspace, integrated with other operational domains to achieve or support the attainment of objectives across the elements of national power.

Cyber strategy relies on an organized combination of goals, means, and methods to accomplish military, political, economic, diplomatic, and broader national security objectives through the utilization of cyber capabilities, allocation of resources, and management of the costs required to address potential risks.

¹ Islam Ramadan Raheeb, op. cit., pp. 113–114.

² Lina Sartaoui, The Concept of Cyberspace, article available on the following website: <https://mawdoo3.com>, date of access: June 20, 2024, at 15:30.

³ Zineb Chenouf, Cyber Warfare in the Digital Age: Post-Clausewitz Wars, Algerian Journal of Security and Development, Vol. 09, No. 02, July 2020, p. 92.

Accordingly, the primary contribution of a national cyberspace strategy lies in providing a clear framework for achieving all other strategies, particularly the national security strategy¹.

2.2.2 Characteristics of Cyber Warfare:

Cyber warfare represents one of the most prominent manifestations of conflict in the digital age. It possesses a set of distinctive features that differentiate it from traditional warfare, and its main characteristics can be summarized as follows:

- Cyber warfare is a highly technological form of conflict, relying primarily on advanced technological tools and complex information systems.
- It is characterized by extreme speed and agility, granting the attacker a clear advantage over the defender, given the difficulty of predicting or intercepting an attack in a timely manner.
- It is a war with undefined objectives and unpredictable consequences, as it transcends traditional battlefields to target vital institutions and sites of sovereign and sensitive nature within the state.
- Traditional deterrence mechanisms are relatively ineffective, since cyberattacks often leave no sufficient physical or digital evidence to identify their origin or the time of their execution².
- It easily transcends territorial and geographical boundaries, as attacks can be launched from anywhere in the world without physical constraints or distance limitations, and their execution is not affected by the balance of military power between states.
- It is marked by the difficulty of identifying the perpetrator, as in many cases it is nearly impossible to trace the entity behind the attack due to the concealed nature of cyberspace operations and the sophisticated techniques used to obscure digital traces³.

Accordingly, cyber warfare fundamentally differs from traditional warfare, both in nature, means, and scope of impact. It represents a new form of conflict based on technology and information systems, reflecting a profound transformation in the concepts of power and methods of confrontation in modern international relations⁴

3. Features of Cyber Warfare

Since the emergence of the Internet as a modern global means of communication, the world has witnessed profound transformations in concepts and interactions at both the international and individual levels, as previously discussed, cyberspace has evolved into a new domain teeming with human interactions and complexities across various spheres of life. This evolution has given rise to new forms of criminal behavior known as cybercrimes, which, in some instances, have escalated into a more dangerous

¹ Zineb Chenouf, op. cit, p 93.

² Chouib Djilali et al, op. cit, 163.

³ Islam Ramadan Rahib, op. cit, p 118.

⁴ Ibid, p 119.

phenomenon cyber warfare with devastating effects that threaten the security and stability of states.

In this context, the present section aims to distinguish the concept of cyber warfare from related notions, to analyze its various forms and types, and to examine its impact on states' critical infrastructure and national economies, with the ultimate goal of providing a comprehensive understanding of the nature of this new form of warfare and highlighting its growing threat in the contemporary world.

3.1 Distinguishing Cyber Warfare from Related Concepts

The study of cyber warfare requires a precise understanding of its conceptual boundaries, as this term intersects with several closely related notions such as cyberattacks and cybercrimes, which may share similar technological tools and methods of execution but differ significantly in their nature, scope, and legal implications.

3.1.1 Distinction between Cyber Warfare and Cyberattacks

Cyber warfare constitutes a specific type or subset of cyberattacks that occur in the context of an armed conflict or that produce physical effects comparable to those caused by traditional kinetic attacks.

In contrast, cyberattacks refer to any malicious cyber activity directed against another state, whether committed in peacetime or during an armed conflict, and regardless of whether such acts result in significant physical damage to life or property, or merely cause disruption to computer systems — provided the acts serve security or military purposes¹.

3.1.2 Distinction between Cyber Warfare and Cybercrime:

Cybercrime is defined as “a criminal activity carried out through the use of computer and electronic technologies, targeting cyber systems, networks, and electronic data²”.

Furthermore, the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna in 2000, defined cybercrime as:

“Any offence that can be committed on or through a computer system or computer network, encompassing in principle all crimes that may be perpetrated within an electronic environment³.”

Thus, while cyber warfare, cyberattacks, and cybercrimes all operate within the cyberspace domain, they differ in actors involved, objectives pursued, and legal

¹ Nour Amir Almousli, *Cyber Attacks in Light of International Humanitarian Law*, Magister Thesis, Syrian Virtual University, 2021, p. 15.

² “The Concept of Cybercrimes, Their Types, Methods of Commission, and Means of Combating Them,” article available at: <http://doafeer.net>, accessed on 04/06/2024, at 15:24.

³ Osama Mohamed Naji Elshazly , *The Legal Aspects of Cyber Warfare: A Study within the Framework of International Humanitarian Law*, Rouh Al-Qawanin Journal, Issue No. 103, Part II, July 2023, p. 1255.

implications factors essential for understanding the multifaceted nature of digital conflicts in contemporary international law.

It is observed that the common denominator between cybercrimes and cyber warfare lies in the domain in which they occur namely, cyberspace, as the environment where various digital operations are conducted. However, there are fundamental distinctions between the two phenomena that can be highlighted as follows:

- **In Terms of Actors:**

Cybercrimes are most often committed by individuals and are typically directed against financial institutions, corporations, or private entities, in contrast cyber warfare is generally conducted by states, governmental bodies, or non-state actors against another sovereign state.

- **In Terms of Objectives:**

Cybercrimes usually aim to demonstrate the perpetrator's technical skills, penetrate computer systems, or achieve personal financial gain, Conversely, cyber warfare seeks to undermine the national and political security of the targeted state and to achieve strategic or military objectives¹.

It is worth noting, in conclusion, that cyber warfare may, in certain instances, overlap with the notions of both cyberattacks and cybercrime, a single act may simultaneously constitute a cyberattack in terms of its means of execution and a cybercrime in terms of its legal consequences, depending on the identity of the actor, the purpose pursued, and the resulting effects.

Indeed, cyber warfare may take the form of a large-scale electronic attack targeting critical infrastructure, which, at the same time, may constitute a criminal act under national and international laws related to combating cybercrime².

For example, a cyber warfare operation may take the form of a large-scale electronic attack targeting critical national infrastructure, while at the same time qualifying as a criminal act under relevant national and international legal frameworks on the suppression of cyber-related offences.

3.2 Types of Cyber Warfare

Cyber warfare is characterized by the diversity of its forms and manifestations, given the differences in the means employed, the objectives pursued, and the actors involved. This complexity makes it difficult to confine cyber warfare within a single or uniform model.

¹Osama Mohamed Naji Elshazly, op. cit., pp. 1255–1256.

²Noor Amir Almousli, op. cit., p. 15.

Accordingly, this section seeks to classify the main types of cyber warfare and highlight their most prominent forms, with the aim of clarifying the distinctive characteristics of each type and analyzing their technical and legal dimensions.

3.2.1 Cold Cyber Warfare:

This type of cyber warfare is marked by continuity and persistence, it typically consists of ongoing, low-intensity cyberattacks exchanged between states over extended periods of time, often as a result of ideological or political conflicts, cold cyber warfare usually reflects historical disputes between nations or rival entities and is conducted covertly as an alternative to declared conventional warfare.

It involves various cyber activities such as commercial and scientific espionage, threats to national economic interests, hacking of official government websites, and the dissemination of anti-state messages or propaganda through compromised platforms¹.

3.2.2 Medium-Intensity Cyber Warfare

This form of cyber warfare often serves as a precursor to, or operates in parallel with, conventional armed conflict, it relies on measures of greater severity than those characteristic of cold cyber warfare, including: military espionage activities; disruption of communications between military forces and their command structures; electronic jamming of radar systems; and the seizure or manipulation of wired and wireless communications equipment.

Medium-intensity cyber operations tend to employ cyberspace on a broad scale to incapacitate communications networks serving both military and civilian systems, their intensity derives from the capabilities and resources of the parties involved, and such operations may pave the way for subsequent kinetic military action, a frequently cited example is the 2008 Russia–Georgia conflict, during which disruptive cyber operations accompanied conventional hostilities.

3.2.3 High-Intensity (Severe) Cyber Warfare

Unlike the lower-intensity forms that the international community has already observed (for example, the Russia–Georgia 2008 conflict and NATO’s campaign against the former Yugoslavia), high-intensity cyber warfare remains largely hypothetical and has not manifested in fully independent form on the battlefield.

It denotes a standalone cyber campaign—independent of concurrent conventional warfare—whose objective is the comprehensive takeover and domination of an adversary’s electronic assets and weapons-control systems.

Such a campaign would seek to place those systems under the attacker’s control and to employ autonomous or remotely actuated weapons against the adversary’s physical infrastructure, it would deliver powerful electronic strikes against critical

¹ Islam Ramadan Rahib, op. cit, p. 119.

infrastructure to effectuate the destruction of vital installations (for example, dams and power generation facilities), thereby producing extensive, widespread devastation in the targeted State¹.

It is worth noting that there are other types of cyber warfare that can be mentioned for reference, the most prominent of which are as follows:

- **Offensive Cyber Warfare:**

This type of warfare is directed at corrupting, destroying, or undermining the credibility and accuracy of data and information, with the aim of weakening confidence in information systems and compromising their security, such as:

- Electronic eavesdropping operations.
- Cyber hacking.
- Cyberterrorist attacks.

- **Cyber Protection:**

It refers to all the efforts undertaken by cyber armies to protect the electronic systems of the state. These operations are mainly defensive in nature and aim to safeguard electronic systems from sudden attacks that may target them².

3.3 Cyber Warfare Support:

This includes a set of measures taken to provide assistance in protecting the state's electronic systems in anticipation of any potential or sudden attack or threat that may cause harm in the future³.

Ultimately, all types of cyber warfare revolve around the immense and unlimited technological capabilities provided by cyberspace.

3.3.1 Emerging Impacts of Cyber Warfare

A lack of adequate cybersecurity measures across states and their sectors, coupled with insufficient implementation of required security standards according to expert studies and research, can render cyberspace vulnerable to cyberattacks targeting the networks of security, military, and other critical institutions. Such attacks aim to seize control over these essential systems.

It is important to note that determining the full scope of cyberattacks is extremely challenging due to their vast range and diversity, especially given rapid technological advancements that enable penetration into various critical state sectors, thereby granting attackers substantial capacity to inflict both direct and indirect effects.

¹Ibid, p 200.

² Osama Mohamed Nagy El-Shazly, *op. cit.*, pp. 1252.

³Faris Mohammed Al-Amarat, *Cybersecurity: Concept and Contemporary Challenges*, Dar Al-Khaleej for Publishing and Distribution, p. 130.

Based on this, the following highlights the main impacts of cyberattacks through illustrative examples that reflect their severity and wide-reaching implications:

3.3.2 Infrastructure Impacts:

Cyberattacks can destroy or disrupt the infrastructure of the targeted state, paralyzing its institutions, destabilizing internal operations, and causing disruptions by targeting central control systems, energy resources, financial systems, communications networks, and transportation¹.

3.3.3 Economic Impacts:

Cyberattacks were ranked as the fifth-highest risk globally in 2020 and have become a new benchmark for both public and private sectors. This high-risk industry continued to grow in 2021, with projections suggesting cyberattacks could double by 2025. Furthermore, the 2020 Global Risk Report by the World Economic Forum indicates an extremely low detection or prosecution rate, reaching only 0.05% in the United States.

According to the FBI, the cost of cybercrime in the United States reached \$3.5 billion in 2019; however, actual losses may be significantly higher, as many exploitation and intrusion activities often go unnoticed². Consequently, a cyberattack on this sector inevitably leads to serious challenges, including economic deterioration and increased unemployment, particularly because the financial and banking sector constitutes a vital component of the economy³.

3.3.4 In the healthcare sector:

Most countries worldwide, including Algeria, have adopted the principle of transitioning toward an information and knowledge society across all sectors, including healthcare. This shift has led to emerging threats to information security. These threats generally take two forms. The first involves tracking and collecting data related to individuals and institutions by breaching their information systems, exploiting vulnerabilities and security weaknesses within these systems to seize data. The stolen data may then be monetized through sales to competing institutions or entities engaged in processing personal data, intellectual property, patents, or any information with financial value⁴.

In the same context, the advancement of electronic control and monitoring systems has increased the likelihood of cyberattacks targeting healthcare sectors, due to gaps in information security systems, healthcare institutions provide public services to patients and those in need, making them susceptible to service disruption, cyberattacks can

¹ Islam Ramadan Rahib, op. cit, p. 125

² Ibid, p 126.

³ Ibid.

⁴ Abd Elkader Amimer et al., Cybersecurity Challenges and Their Applications to the Health Sector in Algeria, Madar for Digital Communication Studies, Vol. 2, No. 2, 2022, p. 37.

impede healthcare delivery and interfere with the response to deadly viruses, directly or indirectly, for example, a cyberattack on a hospital in Hollywood demanded a ransom of 3.6 million and disrupted patient care for several days, another incident in Singapore in 2016 affected medical devices for over ten months, compromising the accounts of 1.5 million users, including 16,000 prescriptions¹.

It is noteworthy that hospitals are not the only targets; pharmaceutical companies are also vulnerable, particularly regarding intellectual property theft. However, the most critical targets are scientific research facilities conducting medical or biological research. An expert at a meeting of the International Committee of the Red Cross noted that in many cases, malware may not even be necessary to execute a cyberattack due to weak protection of medical devices; even producing a software update designed to interfere with vital equipment, such as pacemakers, could be sufficient.

These examples illustrate that cyberattacks may target healthcare facilities and research laboratories containing pathogenic viruses or hazardous biological materials, including facilities conducting hybridization or storage, such attacks could manipulate control systems or infrastructure networks regulating material flow and facility access, if realized, these breaches could cause operational disruptions or leaks that may contribute to the spread of diseases and epidemics, this underscores the critical biosecurity dimension of cyberattacks and the urgent need to strengthen both cybersecurity and biosafety measures within sensitive facilities².

3.3.5 In the military domain:

Modern technologies and advanced innovations have significantly impacted the military field by disrupting communication signals between military units and command centers, issuing incorrect orders to autonomous weapons or drones by altering target coordinates, and directing them to strike targets within the state itself—producing consequences similar to those of conventional physical warfare

Some experts argue that contemporary technological developments have reduced the effectiveness of traditional military tools in favor of technological and informational instruments, conventional means no longer guarantee results nor achieve the state's objectives due to high costs and their obstruction to comprehensive development, whereas cyberspace exerts a compounded influence in achieving military objectives more efficiently and at lower costs³.

Consequently, the military cyberspace domain represents one of the areas experiencing a significant qualitative transformation in enhancing military capabilities and strategies at both the planning and operational levels, it plays a role far beyond being merely a weapon: at the planning level, cyberspace enhances military capacities

¹ Mohamed Salah Abdel-Lah Rabie, *Cyberattacks Between Their Legitimacy as a Means of Self-Defense and Their Condemnation as an Unlawful Aggression: An Analytical Study in Light of International Law*, *Journal of Legal and Economic Studies*, p. 4173.

² *Ibid.*, p. 4174.

³ Saber Salem, "Reflections of the Military Dimension of Cyberspace on the State's Geopolitics," *Stratégia*, Issue 17, p 34, 39

through real-time threat anticipation, situational awareness, and rapid decision-making; at the strategic level related to military decision-making, command systems augmented with artificial intelligence technologies help avoid many shortcomings associated with traditional strategic decision-making processes¹.

From the above, it is evident that the effects of cyber warfare extend across various vital sectors of states and can have severe repercussions, reaching, in some cases, the level of major disasters, particularly when outcomes rival the destructive impact of conventional military force.

Accordingly, cyber warfare constitutes a new form of modern conflict that is no less dangerous than conventional wars due to its ability to paralyze state institutions and weaken the foundations of national security and stability.

4. Conclusion

In conclusion, this study entitled “Cyber Warfare: A Conceptual Reading” has led to a set of important findings and conclusions, along with a number of recommendations aimed at enhancing legal and security awareness of the risks posed by this emerging form of digital conflict.

- **Findings**

- The study revealed that the traditional concept of state power, based on military capabilities, human resources, and conventional weapons, has undergone a radical transformation with the advancement of modern technology. Cyberspace has emerged as a new domain of conflict and influence across various sectors, giving rise to cybercrimes that often evolve into cyber wars with destructive consequences.
- It is clear that cyber warfare involves attacks by states or non-state actors, either unilaterally or reciprocally, distinguishing it from conventional warfare in terms of methods, objectives, and legal context.
- The impact of cyber warfare increases with the continuous development of digital technologies, making it more complex and hazardous to state security and stability.
- Cyber warfare represents one of the modern means of interstate conflict, making cybersecurity a cornerstone of national security.
- Cyber wars are among the most pressing issues on the international agenda today due to their close connection with global peace and security.
- Cyber warfare illustrates the negative side of technological advancement, as it can cause serious disruptions and instability, being a cross-border conflict not limited to any single state.

- **Recommendations**

Based on the study’s findings, a set of practical and academic recommendations can be proposed to support efforts to prevent and address cyber wars, including:

¹ Ibid, p 39.

- Strengthening the protection of sensitive data, including personal, financial, and commercial information, from unauthorized access, use, or illegal manipulation.
- Training and raising awareness among institutional staff on the importance of cybersecurity and methods to protect data from cyber threats.
- Utilizing Virtual Private Networks (VPNs) to secure communications and safeguard digital privacy.
- Regularly updating security software and applications to counter new viruses and cyber intrusions.
- Enhancing international cooperation in combating cyber attacks and wars through knowledge exchange, information sharing, and coordinated security mechanisms.
- Monitoring user activity and online behavior to detect potential threats early while respecting legal privacy regulations.
- Developing effective national strategies that include rapid response plans and clear mechanisms to combat cyber wars and mitigate their impact on state security and stability.

Overall, it is evident that cyber warfare is not merely a technical phenomenon but a strategic and legal reality that requires states and societies to strengthen their digital preparedness and adopt proactive policies to ensure their security in the face of this emerging form of warfare in the 21st century.

Bibliography List :

1. Books :

1. Abdel Monem Moneeb, *Cyber Warfare and Conflict Between States*, Afaaq Al-Ma'refah Publishing and Distribution Company, Saudi Arabia.
2. Fares Mohamed Al-Amarat, *Cybersecurity: Concept and Contemporary Challenges*, Dar Al-Khaleej Publishing and Distribution.
3. Mohamed Sami Jnina, *Researches in the Law of War*, Law and Economics Journal, Issue 1, Egypt, 1941.

1. Journal Articles

1. Abdelkader Amimer et al., *Cybersecurity Challenges and Applications in the Health Sector in Algeria*, Madar for Digital Communication Studies, Vol. 02, No. 02, 2022.
2. An'am Abdel Reda Sultan Al-Okabi, *Employing Cyber Wars in Developing the Concept of Power of Major States*, Political Issues, Issue 73.
3. Chouib Jilali et al., *Concept of Cyber Warfare and Cybersecurity*, Rights and Freedoms Journal, Vol. 11, No. 01, 2023.
4. Islam Ramadan Rahib, *Cyber Warfare in the Light of International Law*, Journal of Legal and Economic Research, Beni-Suef University, Vol. 36, No. 01.

5. Mohamed Salah Abdellah Rabie, Cyber Attacks Between Their Legitimacy as Self-Defense and Illegitimacy as Unlawful Aggression: Analytical Study in Light of International Law, *Journal of Legal and Economic Studies*.
6. Osama Mohamed Naji El-Shazly, Legal Aspects of Cyber Warfare: A Study in the Framework of International Humanitarian Law, *Spirit of Laws Journal*, Issue 103, Part 2, July 2023.
7. Saber Salem, Implications of the Military Dimension of Cyberspace on the Geopolitics of the State, *Strategy Journal*, Issue 17.
8. Yahya Yassin Saud, Cyber Warfare in Light of the Requirements of International Law of Science, *Legal Journal, Cairo University*, Vol. 04, No. 04, 2018.
9. Zeinab Shnouf, Cyber Warfare in the Digital Age: Post-Clauswitz Wars, *Algerian Journal of Security and Development*, Vol. 09, No. 02, July 2020.

2. University Theses

1. Nour Amir Al-Mawsali, Cyber Attacks in Light of International Humanitarian Law, University Thesis, Syrian Virtual University, 2021, p. 15.
2. Said Shaib, Effects of War on International Treaties, University Thesis in Law, Faculty of Law, University of Algiers 1, Academic Year: 2012-2013.

3. Internet Websites.

1. Aliya Mahmoud Mohamed El-Laithi, Modern Trends in the Theory of Wars with Application on the US War on Afghanistan, (consulted on 04/06/2024, 08:48), <https://jsst.journals.ekb.eg>.
2. Concept of Cyber Crimes, Their Types, Methods of Committing and Combating Them, (consulted on 04/06/2024, 15:24), <http://doafeer.net>.
3. Impact of Cyber Attacks on the Global Economy, (consulted on 26/06/2024, 20:27) , <https://ae.linkedin.com>.
4. Lina Sartawi, Concept of Cyberspace, (consulted on 20/06/2024, 15:30), <https://mawdoo3.com>.
5. Mohamed Abu Khalif, Definition of War, (consulted on 02/06/2024, 16:39), <https://mawdoo3>.