ZAOULI – N° 9, Vol. 4 - Mars 2025 pp. 782-807 ISSN : 2788-9343
Soumission : **05/10/2024** Acceptation : **12/12/2024** Publication: **31/03/2025**

Cybersecurity and National Sovereignty: A Legal Perspective on Emerging Threats in Cyberspace

khaled BRAIK
PhD in Public Law,
University of Tissemsilt
Braikkhaled73@gmail.com

Ibn Eloualid Khaled OUABEL
Contract Professor, Facu
lty of Law, University of Tissemsilt
Ouabelkhaled82@gmail.com

***Abstract*:**
The modern digital revolution has ushered in profound transformations that have reshaped how states perceive and engage in international relations – whether through new actors, altered functional roles, or redefined core concepts. This digital shift has recontextualized traditional notions such as security, threat, power, warfare, battlefield, weaponry, and borders. In turn, these have evolved into new terminologies like cyber power, the fifth domain, cyberspace, cyber warfare, cybersecurity, cyber threats, and cyber borders. Foundational principles such as state sovereignty have not remained immune to these changes. Against this backdrop, the present paper seeks to revisit and analyze the concept of cybersecurity as a strategic asset that states strive to acquire and defend as part of their national security architecture.

Keywords: *Digital Revolution, Cyber Threats, Cybersecurity, Digital Society*

Cybersécurité et souveraineté nationale : Une perspective juridique sur les menaces émergentes dans le cyberespace

Résumé :
La révolution numérique moderne a entraîné de profondes transformations qui ont remodelé la manière dont les États perçoivent les relations internationales et s'y engagent, que ce soit par le biais de nouveaux acteurs, de rôles fonctionnels modifiés ou de concepts fondamentaux redéfinis. Ce changement numérique a recontextualisé des notions traditionnelles telles que la sécurité, la menace, la puissance, la guerre, le champ de bataille, l'armement et les frontières. Ces notions ont à leur tour évolué vers de nouvelles terminologies telles que la cyberpuissance, le cinquième domaine, le cyberespace, la cyberguerre, la cybersécurité, les cybermenaces et les cyberfrontières. Les principes fondamentaux tels que la souveraineté de l'État ne sont pas restés insensibles à ces changements. Dans ce contexte, le présent document vise à réexaminer et à analyser le concept de cybersécurité en tant qu'atout stratégique que les États s'efforcent d'acquérir et de défendre dans le cadre de leur architecture de sécurité nationale.

Mots-clés : *Révolution numérique, cybermenaces, cybersécurité, société numérique*

Introduction

The information and communication technology (ICT) environment presents numerous threats that jeopardize the security of the digital society. The succession of industrial revolutions has brought about new spheres of human interaction characterized by virtuality, shifting social, political, and economic relationships to a complex level that resists regulation and containment. In this dynamic space, individuals acquire a digital identity in the form of numerical identifiers, along with the right to privacy regarding their personal information. Within this flexible cyber space, individuals' cultural identities, social personalities, and core values are continuously under threat, at risk of being diluted or reconfigured according to emerging ideological patterns. Consequently, the threats emerging from the information environment are more insidious than the rigid structures that historically endangered state security. These threats take on elusive forms, aiming to infiltrate the psychological framework of individuals and societies, making them primary targets.

As a result, the breadth of these risks has become a concern for states, institutions, and even individuals' private lives. This urgency has accelerated the imperative need for cybersecurity to provide digital protection. Furthermore, there is a growing necessity to develop mechanisms to confront such cyber threats—a responsibility that falls squarely on the domain of cybersecurity and the challenges it entails.

Cybersecurity has thus emerged as a foundational pillar of national security policy, driven by the rise of the information society and the digital domain, alongside the devel-

opment of e-government and its applications. Today, cybersecurity is regarded not only as a field within digital services but also as an added value and essential component of government operations, including in health care, distance learning, e-commerce, and beyond.

This reality necessitates a comprehensive, complex, and integrated approach to address the multitude of challenges presented by cyberspace. Accordingly, the strategic and informed use of core ICT knowledge becomes essential in devising effective countermeasures and solutions, with the goal of ensuring human development, achieving digital security, and fostering trust in cyberspace. As a starting point, it is vital to examine the very nature of cybersecurity and the challenges associated with it.

In response to the research problem, this study is structured around two major themes. The first explores the dimensions of technological developments and threats affecting cybersecurity and consists of two sub-sections. The first sub-section discusses the conceptual framework and dimensions of cybersecurity, while the second addresses the legal nature of cybersecurity and its related challenges. This is further divided into two parts: the first part compares the concepts of cyberspace and cyber threats; the second analyzes the challenges and objectives of cybersecurity.

1. Dimensions of Technological Developments and Threats to Cybersecurity

It is evident that the negative aspects of technological advancement outweigh its benefits, largely due to technology's integral role in facilitating offensive operations between nations.

This includes frequent information theft and systematic destruction of digital systems, thereby weakening national security. (Olivier Kempf, 2012), p. 9)

In today's era, technological advancement increasingly centers on areas such as the development of destructive weapons, indicating that the future may be rife with conflict and warfare stemming from weaponized technologies. (Kareem Hameed Abdulwahab, "Cybersecurity: Constraints and Challenges in Light of International Law, 2021, p. 315)

1.1. Conceptual Framework of Cybersecurity

Cybersecurity is a cornerstone of criminal security policy due to its crucial role in maintaining stability and protecting sensitive transactions. In response, states have allocated substantial financial resources to combat cyber warfare and safeguard national data infrastructure. Thus, it is important to understand the definition and dimensions of cybersecurity. (Suleiman Ketaf and Abdelhalim Bougraine, 2022, p. 39)

Linguistically, the term "cyberspace" is derived from "space," implying a boundless, radiant area, while "cyber" (from the Greek "kibernetes") means helmsman or navigator. (Abdelazim Allah Jafari, 2022, p. 698)

1.1.1 Definition of Cyberspace

There is no universally agreed-upon definition of cyberspace, largely due to varying national systems and structures. It is commonly described as a domain interwoven with the physical world, producing indirect yet complex interactions. Some characterize cyberspace as the "fourth arm" of the military, or even the "fifth dimension" of war-

fare, encompassing devices such as computers and information networks.

France's National Cybersecurity Agency (ANSSI) defines cyberspace as a communications domain formed through the global interconnection of automated digital data-processing systems. (Kareem Hameed Abdulwahab, op.cit., p. 315)

The International Telecommunication Union describes it as a physical and non-physical domain composed of components such as computers, software, networks, information processing systems, and data management tools. (Ismail Zarouka, 2019, p. 1017)

Similarly, the U.S. Department of Defense defines it as a global domain within the information environment, comprising communication networks and control systems (Fatima Bayram, 2020, p. 793)

The modern use of the term "cybernetic" is attributed to American mathematician Norbert Wiener, who introduced it in 1948 as a concept applicable to various humanistic and scientific fields. He described it as a science concerned with control, communication, and the mechanisms of interaction between humans and machines. (Atiyah Idris, 2019, p. 103)

Fiction author William Gibson popularized the term "cyberspace" in 1982, coining it from the notion of "mass hallucination" involving billions of users, combining cybernetics with the concept of "space." (Alaaeddine Farhat, 2019, p. 90)

1.1.2. Forms and Types of Cybersecurity

It is important to distinguish between cyberattacks and the actors who operate within cyberspace. Legal scholar Paulo Shakarian defines cyber warfare as an extension of

political conflict via cyber actions taken by state or non-state actors, posing significant threats to national security. (Paulo Shakarian, Jan Shakarian, and Andrew Ruef, 2013, p. 2)

Cyber warfare may be categorized into different types based on intensity—ranging from military-oriented wars to limited cyber conflicts aimed at specific objectives. However, limited warfare is increasingly unlikely given attackers' often ambiguous goals. There are also indiscriminate cyber wars that fail to differentiate between civilian and military targets, resulting in widespread destruction.

Cybersecurity addresses all these forms, focusing on protection within cyberspace through the use of ICT. It guards against various violations, including breaches of personal data confidentiality, misinformation, privacy invasions, and threats posed by deceptive entities impersonating reputable organizations to obtain sensitive data, such as credit card details or login credentials. Cyberterrorism, driven by diverse motives, also falls under this domain. Another threat is digital fabrication—modifying or falsifying multimedia content within cyberspace. (Zouwawi Lamia and Fahim Ramali, 2023, p. 149–152)

While cybersecurity closely relates to information security, they differ in scope. Cybersecurity is broader, encompassing protection of data across internal and external networks, including cloud servers. In contrast, information security focuses on safeguarding data systems from unauthorized access, theft, modification, or exposure, ensuring confidentiality and integrity for users.[1]

[1] Cybersecurity vs. Information Security," LinkedIn, accessed November 10, 2023

Cybersecurity confronts various types of attacks, such as password cracking, denial-of-service (DoS) attacks, threats to national security, societal manipulation via ideological infiltration, privacy breaches, and support for monopolistic practices. (Kareem Hameed Abdulwahab, op.cit., p. 316–318)

1.2. Origins and Dimensions of Cybersecurity

One of the key motivations behind cybersecurity is the need to establish legal, regulatory, and legislative frameworks capable of addressing challenges faced by societies, organizations, and individuals. This need arises from the global connectivity enabled by ICT, and the growing difficulty in tracking and punishing cybercriminals—especially in the context of e-commerce, online shopping, e-government, and digital administration, all of which demand a secure information environment. (Aws Majid Ghalib Al-Awadi, 2016, p. 6)

The idea of cybersecurity emerged in the 20th century, catalyzed by conventional warfare, with the term "cyber warfare" first appearing in 1934. (Suleiman Ketaf and Abdelhalim Bougraine, op.cit., p. 43)

1.2.1. Early Precursors to Cybersecurity

The initial foundations of what is now referred to as "cyber justice" can be traced back to the American Civil War of 1861, during which the telegraph was used for the first time in warfare. In 1888, German experts discovered that electrical energy produces signals in space in the form of controllable and observable frequencies. These later came to be known as Hertzian waves and were developed by British scientists into radio systems, particularly during the Russo-

Japanese War of 1904. (Naama Al-Fatlawi and Ahmad Abeet, 2016, p. 614)

The two World Wars of the first half of the twentieth century marked a turning point in how technology was used in the conduct of warfare and strategic planning. This led many nations to invest heavily in technological advancements, especially in wireless communications (such as radar). Consequently, sensitive receivers and highly directional antennas were produced. During this era, the growing bipolar rivalry between world powers further pushed the development of electronic tools, resulting in advanced weapon systems, diversified uses, and innovations in communication and remote-control technologies. (Ali Abd al-Rahim al-Aboudi, 2019, p. 93–94)

By the early 1990s, information emerged as a key source of competitive advantage, prompting institutions to fortify their security frameworks to protect their informational assets—covering data storage, processing, and internal dissemination—from corporate espionage and rival interference. As information and communication technology (ICT) became more pervasive, the concept of network security evolved to encompass areas such as e-commerce, e-governance, and broader transactional protection. New cyber challenges also began to emerge on strategic levels—such as cyber warfare and cyber defense—as well as legal (electronic surveillance, privacy protection), and economic dimensions (competition and innovation imperatives). (Ashraf Muhammad Abda, 2018, p. 117)

1.2.2. Dimensions of Cybersecurity

Cybersecurity spans multiple domains, forming an interconnected system that aims to ensure national security against potential cyber threats. The first dimension is the military aspect, from which the internet originally emerged. It was first developed for military purposes before being made accessible to the scientific community. The internet was initially intended to enhance military capacities. (Samir Bara, 2017, p. 260)

Economically, cybersecurity has become a vital component across all societal sectors—individuals, organizations, and governments—due to their increasing reliance on digital technology to store and process information. The widespread use of computers in industry and the management of financial systems has led to the formalization and interconnection of economic transactions. Financial networks, stock exchanges, and corporate systems are now heavily dependent on online infrastructures, amplifying the necessity for robust cybersecurity within the economic sector. (Abdel Fattah Bayoumi, 2007, p. 198)

Politically, cybersecurity has profound implications. It is associated with the leakage of sensitive documents, diplomatic tensions, and the reconsideration of foreign policies. Internally, it encompasses the use of social media for political messaging, election influence, virtual protests, and uncovering terrorist activities. (Abdallah Ahmad Hilali, 2007, p. 129)

The social dimension includes public awareness and education about cybersecurity. Empowering individuals with a comprehensive understanding of security measures is essential. This includes reinforcing personal responsibility, promoting deterrence strategies, and ensuring compliance with

criminal legislation. However, legal deterrence alone is not enough. There is an urgent need for education and training in ICT to instill a security-oriented digital culture. (Hamadoun Touré, 2007, p. 16–17)

On the legal-technological frontier, there is a reciprocal relationship—technological developments constantly test the adaptability of legal frameworks. While laws attempt to regulate both lawful and unlawful digital behavior, cybercrimes often transcend borders, and their perpetrators can be difficult to trace or identify. The lack of clearly defined legal terms and deterrents reflects the transnational and elusive nature of cybercrime, highlighting the necessity for robust international cooperation. (Atiya Idris, 2019, p. 106)

2. The Legal Nature of Cybersecurity and Associated Challenges

Dr. Mohamed Al-Majdoub defines cyber warfare as a collection of hostile acts targeting data associated with a digital state. These include unauthorized access, alteration, destruction, or interruption of information as it travels between computers—for instance, attacks on air traffic control systems, pipelines, and nuclear facilities. (Mohamed Al-Majdoub, 2018, p. 819)

The Geneva Conventions enhanced accountability mechanisms for violations of international humanitarian law by establishing a mandatory system requiring state parties to prosecute or extradite violators, regardless of nationality.[1]

[1] International Committee of the Red Cross, "Overview of the Geneva Conventions," https://www.icrc.org/ar/doc/war-and-law/treaties-customary-law/geneva-

In 2001, the World Federation of Scientists formed a permanent task force for information security. Its report, *Toward a Global Information Space: Managing the Threat from Cybercrime to Cyberwarfare*, became a foundational document presented to the United Nations World Summit on the Information Society in Geneva. (Touré, 2003, p. 17)

2.1. Cyberspace and Cyber Threats—Conceptual Approach

Understanding the nature of active players in cyberspace draws from liberal theory, which argues that the state is no longer the sole actor. Other powerful entities—including multinational corporations and non-state actors—have claimed significant control over cyberspace to serve their own interests. Some of these actors possess cyber capabilities that exceed those of nation-states. (Lamia Talha, 2000, p. 60)

Joseph Nye, a prominent political scientist, identified several cyber players, including nation-states with access to digital technologies, as well as private-sector companies like Google, Facebook, Microsoft, Apple, and Amazon—whose technological strength often surpasses that of many governments. (Ismail Zarouqa, 2019, p. 1019)

Organized crime groups have also leveraged digital technologies for cybercrime—outpacing traditional weaponry in impact. These groups engage in cyber piracy, drug trafficking, human trafficking, organ trade, and smuggling, significantly destabilizing global economies. (Abdelghani Sharqi, 2023, p. 276–277)

---

conventions/overview-geneva-conventions.htm (accessed November 11, 2023, at 18:45).

In 1996, U.S. President Bill Clinton established a commission to protect critical infrastructure, marking the first official acknowledgment of cyberterrorism. This led to the CIA founding the Information Warfare Center, staffed with 1,000 information security experts operating 24/7. Following the September 11, 2001 attacks, a global agreement involving 30 countries was signed to combat cyberterrorism Additionally, individual hackers have exploited digital tools to gain cyber power, enabling them to infiltrate financial systems and corporate databases, often for financial theft. (Talha, p. 61)

Cybersecurity encompasses a wide range of concepts, including **cyberspace**, which is the digital environment where cyber interactions occur; **cybercrime**, referring to illegal activities conducted via computers or the internet; and **cyber deterrence**, which aims to prevent cyberattacks against critical national assets. Cyber deterrence relies on three core pillars: defense credibility, retaliatory capability, and information system resilience.

It is also closely linked to **cyberattacks**, defined as actions that undermine the functionality of a computer network for political or national purposes by exploiting system vulnerabilities (Zaghda Al-Bahi, 2017, p. 52–53)

Finally, **information security** is a key subset of cybersecurity that focuses on maintaining the confidentiality and integrity of data shared on social platforms and digital networks. As cyber threats evolve, new information protection systems have been developed—including OS-level protec-

tions, application security, software safeguards, and regulated system access.[1]

There exists a partial and nuanced relationship between information security and cybersecurity. Information security involves the protection of data from unauthorized access, regardless of its format—whether on physical paper or stored electronically. Consequently, it does not necessarily encompass network security, just as network security does not inherently guarantee the security of information. In contrast, cybersecurity is concerned specifically with the safeguarding of data that is transmitted, stored, or processed within information and communication technology systems. It also aims to ensure the availability and integrity of services provided through cyberspace, including communication channels and electrical infrastructure.

Therefore, information security does not fully include cybersecurity, nor can cybersecurity be considered a comprehensive domain of information security, particularly as the latter also covers non-digital data. Their intersection lies in their shared objective of protecting information, but they diverge in scope and technical focus. (Mahmoud Abdulrahman Khalaf and Ahmed Abdulkarim Abdulwahhab, 2020, p. 4).

2.1.1. Domestic Regulation of Cyberspace

Cyberspace has introduced complex security challenges, compelling states to regulate and manage the ownership and use of digital technology domestically, while also seeking cooperative mechanisms at the international level. Such

[1] CyberOne, "Cybersecurity Awareness," https://cyberone.coly (accessed November 11, 2013, at 22:45)

measures are essential to restore sovereign authority in a digital environment often violated by both state and non-state actors.

States have implemented domestic internet controls through various means. One method is comprehensive infrastructure regulation, grounded in the premise that internet proliferation depends on physical tools. Governments that control these tools can regulate online activity. This has led to the development of hierarchical networks that allow governments to manage digital gateways. Another approach is content regulation through software controls, often referred to as "software barriers," which enhance the ability to govern both routers and end-user access. (Timothy S. Wu, 1997, PCS1–652.).

China exemplifies this regulatory capacity through mechanisms such as the "Great Firewall," which restricts access to numerous foreign websites and monitors data traffic. Similarly, North Korea employs cyber opacity as a form of internal control. (Saad Murrah Zine Al-Abidin, 2022, p. 705)د .

International cyber governance remains difficult due to the absence of mutual trust and the prioritization of national over collective cybersecurity interests. This fragmentation has hindered cooperative regulation. In response, the Carnegie Endowment for International Peace proposed a 2020 strategy for enhancing global financial cybersecurity. Although centered on financial systems, the strategy underscores the necessity of joint international efforts to address global cyber threats and build digital sovereignty. (Nelson Arthur and Tim Morrow2021, p. 26)

Cyber warfare has become an instrumental tool in international relations, offering a low-cost method for harming adversaries by disrupting or infiltrating websites and critical digital infrastructure. (Khalid Walid Mahmoud, 2013, p. 116)

These invisible, undeclared wars produce significant long-term consequences for diplomatic relations. (Sarah Abdelaziz, p. 16)

One major outcome is the use of cyberattacks as a strategic means of enhancing international status, enabling medium and small states to assert greater influence. Cyber warfare has also catalyzed the diffusion of power across global politics and introduced new arms races, with cybersecurity now integral to national defense strategies. Diplomatic tensions often escalate due to cyber intrusions into domestic affairs, complicating the application of international law.

For instance, NATO's 1999 cyber operations against Yugoslavia illustrated the emerging use of moderate-intensity cyber warfare as a tool of modern conflict. (Orian Bieber, 2000, p. 124)

2.2. Cybersecurity Challenges and Objectives

Cybersecurity faces numerous evolving challenges due to the emergence of digital crimes that threaten the informational, cultural, and economic assets of individuals, organizations, and nations. As such, effective cybersecurity requires comprehensive political will and the development of integrated, achievable strategies. These must focus on infrastructure development, digital services enhancement, and cross-disciplinary solutions incorporating legal, educational, technical, and administrative dimensions.

Efforts must also address the human, legal, and economic aspects of cybersecurity to foster trust and support sustainable digital development. (Muslim Tiras Ibrahim, "Cybercrimes and Their Impact on Cybersecurity 2021, p. 81) The digital divide—both economic and social—demands a multifaceted, not merely technical, approach.

Cybersecurity also responds to the evolving nature of cyberterrorism, which—like cybercrime and cyber espionage—poses extensive and sophisticated threats, with all actors capable of launching offensive operations. (Shawn Henry and Aaron F. Brantly, 2018, p. 49)

2.2.1. Legal Limitations and Security Challenges in Cybersecurity

The United Nations Charter prohibits the use of force among member states, as outlined in Article 2(4), which forbids threats or actions against the territorial integrity or political independence of any state. However, the emergence of cyber power—referred to in the media as electronic or cyber force—raises new questions. Does cyber aggression qualify as a use of military force subject to the sanctions outlined in Chapter VII of the Charter, or is it a separate form of assault altogether? [1]

Cyberattacks, whether military or non-military, inflict harm on individuals and states. International law has addressed such matters in the context of human rights protection during both international and non-international armed conflicts. The Geneva Conventions emphasize the protection of civilians during wartime, yet rapid technological ad-

[1] Article 2(4), *Charter of the United Nations*.

vancements call for reassessment of these laws to reflect the evolving nature of warfare, including the increased threat posed by cyberattacks, which may cause collateral damage surpassing that of conventional weapons. (Ihab Khalifa, 2019)

Article 36 of Additional Protocol I to the 1977 Geneva Conventions requires parties to verify whether new weapons or methods of warfare comply with international law. This is particularly relevant in today's technological era, where rapid innovation may reshape the framework of international legal norms[1].

The absence of binding legal frameworks to govern cyberspace underscores the necessity for codified customary rules. Cybersecurity, now a strategic asset, is employed by technologically advanced states to achieve deterrence, military dominance, or strategic equilibrium. International legal scholars increasingly acknowledge that any cyberattack may constitute an act of war.[2]

Furthermore, legal advisors to the International Committee of the Red Cross stress that Article 36 imposes an obligation on states to ensure that new cyberweapons comply with humanitarian law (Mohamed Al-Majdoub, op.cit, p. 79).

Although completely halting cyberattacks may be impossible, their impact can be mitigated through modern legal frameworks and the adaptation of traditional concepts to

[1] Gilles Laurent, interview on the International Committee of the Red Cross website, 2013. Available at: https://www.icrc.org/ar/doc/resources/documents/interview/2013/06-27-cyber-warfare-ehl.htm Accessed on November 14, 2023, at 21:50.

[2] Article 36, *Additional Protocol I to the Four Geneva Conventions*.

new digital realities. The key lies in identifying the perpetrator and the intended target [1].

2.2.2. Cybersecurity Objectives

The principal aim of cybersecurity is to protect and secure data, networks, computer systems, and software from unauthorized access or cyber intrusions. It ensures the confidentiality, integrity, and availability of personal and institutional data, thus defending digital infrastructure essential for public safety and national security.

Cybersecurity also ensures the continuity of communication networks between governments and citizens, safeguarding data flow and preventing service disruptions [2].

It relies on up-to-date technical knowledge, attacker profiling, and message analysis to prevent intrusions. Encrypted communications and transactions form a critical defense layer, making it more difficult for intruders to access sensitive data—an indispensable measure for maintaining digital security[3].

[1] National Communications and Media Commission of Iraq, Cybersecurity page: www.tra.gov.ib/cybersecurity-AR, accessed November 14, 2023, at 22:00.
[2] Amir Okasha, *Electronic Warfare: The Virtual World Conflict*, available at: www.felesteen.ps/prints/news/iouusu, accessed November 14, 2023, at 22:45.
[3] Gilles Laurentop.ciy, accessed November 14, 2023, at 23:00.

Conclusion:

It has been concluded that the concept of cybersecurity has undergone substantial modification and transformation in terms of threats, effectiveness, and scope. Once confined to the domain of state and military power, cybersecurity has evolved into a comprehensive concept encompassing all areas of life, increasingly focusing on individuals and societies that have entered the digital age through the revolution in information and communication technologies.

Everyone is now connected to the network, creating a new interactive space — cyberspace — which has altered traditional understandings of international relations, such as the concepts of power, conflict, and warfare. The shift from physical to virtual conflict is clear, as wars are now conducted with ones and zeros. States are visibly moving toward the militarization of cyberspace, giving rise to new threats that are growing in scale and intensity, and that pose a serious threat to national security. This has led to the emergence of the modern concept of cybersecurity.

Findings:

1. Cybersecurity has become a critical component of national security.
2. Most states have adapted their security doctrines to address the rapidly evolving cyber threats, which now include cybercrime, cyberterrorism, and cyberwarfare as significant challenges.
3. States are making serious efforts to protect their national security due to the migration of personal and institu-

tional data into the virtual world, which exposes digital security to unprecedented risks.

4. States are operating along two main tracks:

- Technological, by developing cyber armies and establishing cybersecurity agencies.
- Legal, by enacting appropriate national and regional legislation to combat cybercrime and cyberterrorism.

5. There is a growing international consensus to curb the cyber arms race and prevent the militarization of cyberspace.
6. Cyber threats now represent a new form of non-traditional, soft threats that accompany globalization. These threats are multifaceted, targeting both states and individuals, and are designed for immediate and effective use to undermine adversarial capabilities.
7. In the case of Algeria, cyber threats are on the rise due to increased connectivity, deeper integration of individuals into the digital sphere, lack of regulatory oversight in cyberspace, and the inadequacy of domestic legislation to address the evolving and deceptive nature of these crimes. Algeria's cybersecurity is thus threatened by:

- First, breaches of data confidentiality and violations of digital privacy.
- Second, digital disinformation, including fabricated content and the chaotic dissemination of news.
- Third, though less prominent, is the threat posed by cyberterrorism.

Recommendations:

1. Given that cyber threats harm the interests and security of both individuals and states without distinction be-

tween civilian and military targets, it is imperative that states establish specialized cybersecurity bodies.
2. States should develop national cybersecurity strategies and oversee their implementation.
3. Cybersecurity governance policies, frameworks, and guidelines must be established and widely disseminated.
4. Local communities should create frameworks for managing cybersecurity risks.
5. States must work to establish centralized response mechanisms for handling cyber incidents and breaches.
6. Relevant authorities should establish national encryption standards and policies.
7. National awareness campaigns, conferences, and seminars should be held across various media platforms to raise public understanding of cybersecurity.

References

Books:

1. Ashraf Mohamed Abda, *The Security Environment of E-Government: Between Risks and Protection Requirements*, Dar Al-Kutub wa Al-Dirasat Al-Arabiya, Alexandria, Egypt, 2018.
2. Ihab Khalifa, *What Is the Position of the UN Charter on the Use of Cyber Force in International Interactions?*, Future Center for Research and Studies, Abu Dhabi, 2019.

3. Jawhar Al-Jamousi, *The Virtual and the Revolution: The Role of the Internet in the Emergence of an Arab Civil Society*, Arab Center for Research and Policy Studies, Beirut, Lebanon, 2019.
4. Hamadoun Touré, *Cybersecurity Guide for Developing Countries*, International Telecommunication Union (ITU), 2007
5. Abdel Fattah Bayoumi, *Principles of Criminal Procedures in Computer and Internet Crimes*, 1st ed., Dar Al-Kutub Al-Qanuniya, 2007.
6. Abdullah Ahmed Hilali, *The Budapest Convention on Cybercrime*, 1st ed., Dar Al-Nahda Al-Arabia, Cairo, Egypt, 2007.
7. Karim Hamid Abdulwahab, *Cybersecurity: Constraints and Challenges under International Law*, *The Social Contract Journal*, Center for Legal Research, Iraq, 2021
8. Mohamed Al-Majzoub, *The Intermediary in Public International Law*, 7th ed., Al-Halabi Legal Publications, Beirut, Lebanon, 2018.

Articles:

1. Ismail Zerrouga, *Cyberspace and the Transformation of Power and Conflict Concepts*, Vol. 10, No. 2, *Journal of Legal and Political Sciences*, Mohamed Boudiaf University, Algeria, 2019.
2. Ismail Zerrouga, *Cyberspace and the Transformation of Power and Conflict Concepts*, *Journal of Legal and Political Sciences*, El Oued University, Algeria, 2019.
3. Aws Majid Ghaleb Al-Awadi, *Cyber-Informational Foundations*, *Bayane Harvest Series*, Center for Research and Planning, Baghdad, 2016.

4. Khaled Walid Mahmoud, *Internet Attacks as the New Arena of Electronic Conflict*, No. 5, *Arab Policies Journal*, Arab Center for Research and Policy Studies, Doha, Qatar, 2013.
5. Zaghdah El-Bahi, *Cyber Deterrence: Concept, Challenges, and Requirements*, Vol. 1, Issue 1, *Journal of Political Science and Law*, Arab Democratic Center, 2017.
6. Zouaoui Lamia, Faheem Ramali, *Cyber Threats and the Digital Society's Security: Case Study of Algeria*, Vol. 12, No. 2, *Algerian Journal of Security and Development*, University of Hadj Lakhdar Batna, Algeria.
7. Sara Abdulaziz, *Cyber Warfare: Event Trends*, Issue 20, Abu Dhabi
8. Saad Murra Zain Al-Abidin, *The Impact of Sovereignty on Jurisdiction in Cybercrimes*, *International Journal of Jurisprudence, Judiciary and Legislation*, Egyptian Knowledge Bank, Egypt, 2022.
9. Suleiman Qataf, Abdel Halim Bouguerine, *Cybersecurity and Its Related Conceptual Contents*, Vol. 5, No. 2, *Journal of Academic Scientific Studies*, University of Barika, Algeria, 2022.
10. Samir Bara, *Cybersecurity in Algeria: Policies and Institutions*, Vol. 2, No. 2, *Algerian Journal of Human Security*, University of Hadj Lakhdar Batna,Algeria, 2017.
11. Abdel Azim Allah Jaafari, *The Cyber Threats Saga and Their Impact on Algerian National Security*, *African Journal of Legal and Political Studies*, Mohamed Drayah University, Adrar, Algeria, 2022.
12. Abdelghani Cherki, *Cyber Threats and the Sovereignty Dilemma: Re-reading Sovereignty and Independence*, Vol. 7,

No. 2, *Journal of Global Politics*, Mohamed Bouguerra University, Boumerdes, 2023.

13. Atiyah Idris, *The Role of Cybersecurity in Algeria's National Security System*, Vol. 1, No. 1, *Misdaqiya Journal*, University of Larbi Tebessi, Tebessa, Algeria, 2019.
14. Atiyah Idris, *Cybersecurity in the Algerian National Security Framework*, Vol. 1, No. 1, *Misdaqiya Journal*, University of Larbi Tebessi, Tebessa, Algeria, 2019.
15. Alaa Eddine Farhat, *Cyberspace: Shaping the Battlefield of the 21st Century*, Vol. 10, No. 3, *Journal of Legal and Political Sciences*, El Oued University, Algeria, 2019.
16. Ali Abdulrahim Al-Obaidi, *The Iranian Wars Anxiety and Its Impact on International Peace and Security*, *Political Issues Journal*, Al-Tahari University, Iraq, 2019.
17. Fatima Bayram, *National Sovereignty in Light of Cyberspace and Digital Transformations: China as a Model*, *Algerian Journal of Human Security*, University of Hadj Lakhdar Batna, Algeria, 2020.
18. Lamia Talha, *Cyber Threats and Crimes: Their Impact on National Security and Counter-Strategies*, *Ma'alem Journal of Legal and Political Studies*, University Center of Tindouf, Algeria, 2020
19. Mahmoud Abdulrahman Khalaf & Ahmed Abdulkarim Abdulwahab, *The Dilemma of Iraqi Cybersecurity: Between Cyber Threats and Freedoms-Restricting Legislation*, Issue 60, *Journal of Political Studies*, Al-Nahrain University, Iraq, 2020.
20. Muslim Tiras Ibrahim, *Cybercrimes and Their Impact on Cybersecurity*, Vol. 12, No. 1, *Journal of Al-Qadisiyah for Law and Political Science*, 2021.

21. Ne'ma Al-Fatlawi & Ahmed Abeet, *Cyber Attacks: Their Concept and Emerging International Responsibility in Light of Contemporary International Law*, Issue 40, *Journal of Al-Muhaqqiq Al-Hilli for Legal and Political Sciences*, University of Babylon, Iraq, 2016
22. Nelson Arthur & Tim Morrow, *Global Cyber Threat: Finance and Development*, 2021.
23. Noura Shalouch, *Electronic Piracy in Cyberspace: The Growing Threat to State Security*, Vol. 8, No. 2, *Babel Center for Human Studies Journal*, Iraq, 2018.

Foreign References:

1. HENRY, Shawn, & Aaron F. BRANTLY, *Countering the Cyber Threat*, The Cyber Defense Review by Nion, 2018.
2. [International Committee of the Red Cross], *Overview of the Geneva Conventions* – https://www.icrc.org/ar/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm
3. Olivier Kempf, *Introduction to Cyberstrategy*, Economica, Paris, 2012.
4. Orian Bieber, *Cyber Wars or a Sideshow? The Internet and the Balkan Wars*, *Current History*, Vol. 99, 2000.
5. Paulo Shakarian, Jana Shakarian, & Andrew Ruef, *Introduction to Cyber Warfare: A Multidisciplinary Approach*, Elsevier, 2013.
6. Timothy S. Wu, *The International System: Cyberspace Sovereignty? The Internet and International Law*, *Harvard Journal of Law and Technology*, 1997.