

Cyberattacks: Emerging Impacts and Criminal Liability of Perpetrators

الهجمات الإلكترونية: الآثار الناشئة والمسؤولية الجنائية للمرتكبين

Youssef Boukir

Researcher at the Laboratory of Political Studies and Public Law, Faculty of Legal,
Economic and Social Sciences, Sidi Mohamed Ben Abdellah University, Fez, (Morocco)

boukiryoussef587@gmail.com

ORCID: <https://orcid.org/0009-0009-4829-9041>

Majda Bouchafra

PhD in Private Law, Faculty of Legal Sciences in the Interior and Social, Sidi Mohamed
Ben Abdellah University of Fez, (Morocco)

majda.bouchafra@usmba.ac.ma

DOI: <https://doi.org/10.70411/MJLS.4.2.2026393>

تاريخ القبول: 2026-05-28

تاريخ المراجعة: 2026-05-28

تاريخ الاستلام: 2026-04-13

Abstract

The study seeks to identify and explore a very important topic: “Cyberattacks: Emerging Impacts and Criminal Liability of Perpetrators,” since such attacks pose a serious threat to humanity, particularly when they target the critical infrastructure of states.

Cyberattacks can cause tremendous human suffering in times of armed conflict by targeting infrastructure deemed necessary for the civilian population’s survival. Therefore, using a descriptive-analytical approach and an inductive approach, the study presents several observations, including the risks and impacts on civilians.

Today, with the rise of cyberattacks as a new form of warfare conducted, unlike traditional wars, in the distinct environment of cyberspace, jurists and legal experts are compelled to develop and apply clear legal frameworks. This is essential to prevent unrestricted use of these powerful tools and to ensure accountability in their deployment.

Undeniably, the seriousness of cyberattacks is heightened by the difficulty of identifying perpetrators and their origins. Therefore, it is crucial to shed light on this form of warfare—cyberattacks—with a primary focus on holding accountable those responsible for international crimes committed through such means and advancing the cause of international criminal justice.

Keywords: cyberattacks, cyberspace, international humanitarian law, international criminal liability.

الملخص

تسعى الدراسة إلى محاولة الوقوف عند موضوع على قدر كبير من الأهمية ويتعلق الأمر بـ "الهجمات السيبرانية - الآثار الناشئة والمسؤولية الجنائية عن مرتكبيها"، فالهجمات السيبرانية تشكل تهديدا حقيقيا للإنسانية خاصة حينما يتعلق الأمر باستهداف البنية التحتية الحرجة للدول.

تتسبب أحيانا الهجمات السيبرانية في درجة هائلة من المعاناة الإنسانية زمن النزاع المسلح من خلال استهداف البنية التحتية اللازمة لبقاء السكان المدنيين، لهذا، وبعد استعانتنا بالمنهج الوصفي التحليلي والمنهج الاستقرائي، فقد توصلت الدراسة إلى العديد من الملاحظات بما في ذلك المخاطر والآثار التي قد تعجز بالمدنيين.

اليوم، وأمام تزايد الهجمات السيبرانية، باعتبارها نمطا جديدا من الحروب تخاض في بيئة جديدة " الفضاء السيبراني" تختلف عن الحروب التقليدية، ذلك الذي يفرض على الفقهاء والخبراء القانونيين إخضاع هذه الابتكارات لقواعد قانونية واضحة حتى لا يترك للإنسان الحبل على الغارب في استخدام هذه الأسلحة كيفما شاء.

ولا مناص من القول، أن ما يزيد من خطورة الهجمات السيبرانية هو صعوبة تحديد هوية مرتكبيها ومكان انطلاقها، لهذا كان لا بد من تسليط الضوء عند هذا النوع من الحروب " الهجمات السيبرانية"، مع الوقوف بالأساس عند متابعة مرتكبي الجرائم الدولية التي تعتمد على الهجمات السيبرانية وتحقيق العدالة الجنائية الدولية.

الكلمات المفتاحية: الهجمات السيبرانية، الفضاء السيبراني، القانون الدولي الإنساني، المسؤولية الدولية الجنائية.

Introduction

From electronic medical records (EMR) to telehealth and to artificial intelligence, technological advancements are increasingly shaping the field of medicine. The number of healthcare systems going paperless continues to rise, and more services depend on the convenience and accessibility of computer systems to operate smoothly. However, with the ease of technological assistance comes the cost of increased vulnerability to malware and cyberattacks. In the context of healthcare, a cyberattack constitutes any purposeful, malicious attempt to breach healthcare data, compromise patient confidentiality, or disrupt operational systems¹.

In addition, cyberattacks target banking institutions. Perhaps the most notorious cyber incidents to date are the WannaCry and NotPetya ransomware cyberattacks. The WannaCry attack in May 2017 affected computer systems in more than 150 countries, while the NotPetya attack in June 2017 is possibly the most destructive cyberattack ever seen, with an estimated cost of US\$10 billion according to a US White House assessment. Although not aimed at the financial sector, these attacks affected banks, ATM networks, and card payment systems².

Against this backdrop, the central problem addressed in this article concerns how cyberattacks targeting critical infrastructure contribute to civilian suffering, particularly within the context of armed conflicts. This raises important legal and humanitarian questions regarding the adequacy of existing international legal frameworks.

Accordingly, this article aims to examine the impact of cyberattacks on civilians and their property, as well as to analyze the issue of criminal liability for perpetrators. To achieve this objective, the study adopts both a descriptive-analytical approach, to assess the nature and consequences of such attacks, and an inductive approach, to derive broader conclusions from relevant practices and cases.

The findings suggest that cyberattacks constitute a significant and evolving challenge, particularly when they target vital sectors such as healthcare systems and banking institutions, where their effects extend beyond material damage to encompass serious humanitarian consequences. This article is structured into two main sections: the first examines the repercussions of cyberattacks on civilians and their property, while the second explores the criminal responsibility of the perpetrators.

¹ Li Susan et al, « Cyber - attacks on hospital systems: a narrative review », the American journal of geriatric psychiatry, open science, education and practice 7, (september 2025), 31.

² Francisco José Herrera Luque y otros, « Cyber risk as a threat to financial stability », revista de estabilidad financiera, no 40, (Primavera 2021), 183.

First Part

The Impact of Cyberattacks on Civilians and their Properties

Cyberattacks have no borders, and their consequences can surpass conventional warfare. They can cause significant harm to civilians and civilian objects, for example, by targeting the healthcare sector and compromising sensitive patient data (as outlined in the first paragraph) or by gaining unauthorized access to individuals' accounts and manipulating their personal information (as outlined in the second paragraph).

First Requirement

The Impact of Cyberattacks on the Healthcare Industry

Due to technological advances, the concept of smart health has emerged, enabling wearable medical devices,³ such as blood pressure monitors and glucometers, to connect directly to smartphones. Conversely, the health sector remains the most critical target for hackers. This study will focus on two key aspects: (i) cyberattacks targeting connected medical devices; and (ii) cyberattacks targeting patients and disrupting healthcare services.

i. Cyberattacks Targeting Connected Medical Devices

Information and communications technology has transformed the healthcare sector by enhancing patient care services and enabling more accurate diagnoses through artificial intelligence. However, this digital advancement has also given rise to growing cyber threats. Healthcare systems store vast amounts of sensitive patient data, which are valuable targets for hackers. Once accessed, this information can be exploited for fraud, identity theft, or extortion, potentially leading to severe consequences and endangering human lives.⁴

The growing reliance on connected medical devices, such as heart rate monitors, significantly increases the potential risks, particularly as many of these devices lack robust

³. According to a 2018 report by the World Health Organization, the global population of older adults is projected to reach approximately 1.5 billion by 2050. Population ageing is associated with a rise in chronic diseases, leading to frequent visits to healthcare providers and a greater demand for hospitalization. The growing number of patients requiring continuous care significantly increases the cost of medical treatment. In the United States of America, for example, healthcare spending accounted for 17.9 per cent of the gross domestic product in 2017 and is projected to rise to 19.4 per cent by 2027.

-For more information, see: H. Boualfull, "The role of the Internet of Things (IOT) in performing work in the health field with reference to some countries", Journal of Financial, Accounting and Management Studies, Vol. 8, No. 3, (December 2021), at: 21 – 4 – 2026, at: 12:32.

⁴. A. Cervera García and A. Goussens, "Ciberseguridad y uso de las TIC en el sector salud", Elsevier, Vol. 56, No. 3, 2024: 3.

security features. As the healthcare sector continues to digitize, it will face a range of challenges, including data privacy and security.⁵

In addition, hospital networks are vulnerable to indirect harm caused by cyber operations, often referred to as “collateral damage”. The potential impact of such attacks can be alarming, particularly when they target critical systems responsible for the supply of medication, oxygen, or the digital infrastructure linked to the electrical power of medical devices. This threat becomes even more severe in the context of health crises or armed conflicts, where the uninterrupted functioning of these systems is vital to saving lives.⁶ In our humble opinion, while modern medical technologies offer significant benefits, they also present complex challenges, particularly in safeguarding the confidentiality and integrity of patients' personal information. Failure to address these concerns could result in serious human consequences.

ii. Cyberattacks Targeting Patients and Disrupting Healthcare Services

Hospital facilities and health insurance offices are undergoing rapid digital transformation, leading to improved service quality for patients. However, this shift often occurs with inadequate consideration of the emerging cybersecurity risks it entails. The vast amount of sensitive digital information stored within health systems, such as electronic health records, could become a strategic target for cyberattackers.

In 2020, a woman receiving treatment at a hospital in Düsseldorf, Germany, died after a cyberattack paralyzed the hospital's computer systems, preventing her from receiving timely care. Similarly, in 2023, a group of hackers used ransomware to breach the patient data systems of a hospital in Barcelona, resulting in encryption and blocking of digital medical records and sensitive information. The incident also led to the disruption of numerous medical procedures, many of which were suspected to have been deliberately targeted by the attackers.⁷

In 2019, a major cyberattack targeted several healthcare organizations in the United States of America, with an estimated financial impact of \$4 billion. That same year, another cyberattacks compromised the data of nearly one million patients at Quest Diagnostics across Brazil, the United States of America and Mexico.

⁵. Ibid, 3.

⁶. L. Gisel, T. Rodenhäuser and K. Dörmann, “Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts”, International Review of the Red Cross, No. 913, (March 2021): 293.

⁷. J. P. Jarufe Bader, “Ciberataques contra la infraestructura de salud : Experiencia internacional”, Asesoría Técnica Parlamentaria, (September 2023) : 5.

According to a 2019 study by Armis, 40% of medical institutions were affected by the 2017 ransomware attack, highlighting the widespread vulnerability of the healthcare sector to cyber threats.⁸

Second Requirement

The Impact of Cyberattacks on Banks and Financial Institutions

Attacking the websites of banks and companies is a common objective of various hackers. This often takes the form of stealing customer information and credit card data, or launching denial-of-service attacks. Notably, in late 2011, the United States of America experienced a cyberattack that disrupted access to bank accounts, causing significant operational paralysis. According to US officials, Iran was behind the attack.⁹

In a comparable case, the Thai police, in cooperation with the Federal Bureau of Investigation (FBI), arrested the 24-year-old Algerian hacker Hamza Bendelladj in January 2013. Despite his young age, he was ranked among the FBI's top 10 most wanted hackers. US authorities have charged Bendellaj with hacking into the online banking systems of over 217 banks worldwide, causing financial losses amounting to millions of dollars.¹⁰

Second Part

International Criminal Liability for Cybercrime Attacks

Cyberattacks can constitute international crimes that cause injury or death to civilians and damage civilian objects. Therefore, the perpetrators are subject to international criminal liability based on the provisions of international criminal law, as these attacks constitute violations of both international law and international humanitarian law.

Since Article 5 of the Statute of the International Criminal Court defines serious crimes, including crimes against humanity, genocide, war crimes, and crimes of aggression, this research will focus on addressing a critical question: To what extent do the rules of international criminal law apply when international crimes are committed through cyberattacks in cyberspace?¹¹

⁸. CiberSeguridad Latam, "Hospitales: Uno de los principales blancos de ciberataques", 2020. Article accessed the link: <https://ciberseguridadlatam.com/hospitales-uno-de-los-principales-blancos-de-ciberataques/>, at: 21 – 05 – 2026, at: 23.21.

⁹. E. Khalifa, *Cyber Power: How Nations can Manage their International Affairs in Cyber Area*, (Al – arabi, publishing, Cairo), 2017: 288.

¹⁰. Ibid: 277.

¹¹. M. al-Samarrai, « The Role of International Law in Combating Cyber Attacks », 1st ed, (Baghdad: Al- thakera Publishing and distributors, 2024), 266.

For this purpose, Part I will explore individual international criminal responsibility for conducting cyberattacks, while Part II will examine the criminal liability of military commanders for their involvement in such attacks.

First Requirement

Individual Criminal Liability for Cyberattacks

However, as the role of individuals in certain events has evolved, international law has adapted by recognizing a limited status for individuals and non-state actors at the international level, such as armed groups involved in internal conflicts, multinational corporations, and non-state entities conducting cyberattacks. These actions violate state sovereignty and undermine national security and stability. Consequently, it has become essential to apply international legal frameworks to establish the responsibility of these actors. Cyberattacks result in significant harm to states, such as severe damage to vital facilities. These cyberattacks are carried out by natural persons, whether acting on behalf of or as agents of a state or operating independently. In either case, these individuals can be held internationally criminally responsible.¹²

Article 25 of the Statute of the International Criminal Court clearly establishes the Court's jurisdiction over natural persons, holding individuals personally responsible for crimes within its mandate. To prevent impunity, the Statute also addresses criminal participation, which includes ordering, urging, or enticing others to commit crimes under the Court's jurisdiction. Such criminal participation encompasses providing aid, incitement, or any form of assistance that facilitates the commission of an international crime. Regarding cyberattacks, Rule 84 of the Tallinn Manual 2.0 addresses individual criminal responsibility for cyber operations that may constitute war crimes or serious violations of the law of armed conflict. This is further supported by Article 85 of the Additional Protocol I of 1977 on War Crimes (Geneva Conventions) and Article 8 of the Rome Statute. These provisions recognize that acts committed by electronic means can be considered war crimes, affirming that the law of armed conflict applies to new methods and means of warfare, even those that did not exist when the law was originally drafted.¹³

¹² H.S. Al-Darmiki and W. A. Allam, "International responsibility for cyberattacks by non-state entities", University of Sharjah Journal of Law Sciences, Vol. 21, No. 4, 2024, 483.

¹³ I. El-Sayed Ahmed Ramadan, "Confronting cyber-attacks in light of the provisions of international law", Revue des Sciences Juridiques et Economiques, Vol. 1, No. 67, 2025, 1847.

Second Requirement

Individual Criminal Liability for Cyberattacks

Article 28(a) of the Rome Statute of the International Criminal Court establishes the responsibility of military commanders:¹⁴ A military commander or person effectively acting as a military commander shall be criminally responsible for crimes within the jurisdiction of the Court committed by forces under his or her effective command and control or effective authority and control, as the case may be, as a result of his or her failure to exercise control properly over such forces, where:

- i. That military commander or person either knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes; and
- ii. That military commander or person failed to take all necessary and reasonable measures within his or her power to prevent or repress their commission or to submit the matter to the competent authorities for investigation and prosecution. This article therefore establishes the responsibility of military commanders for offenses committed by forces under their effective control.¹⁵

In the context of cyber operations, Article 24 of the Tallinn Manual outlines the general principles of commanders' criminal responsibility when they order the direct execution of cyberattacks. The article further specifies a second category of liability, which applies if the military commander knew, or under the circumstances should have known, that forces under their command had committed or were about to commit an international crime. This aligns closely with the provisions set forth in Article 28 of the Rome Statute of the International Criminal Court.

Therefore, holding perpetrators of cyberattacks, including leaders and heads of state, criminally responsible for actions that result in humanitarian disasters and atrocities threatening international peace and security requires the international community to act decisively. This includes establishing specialized courts to investigate such crimes and accelerating amendments to the Rome Statute of the International Criminal Court to explicitly address cyberattacks.¹⁶

¹⁴ In the context of cyberattacks, a military commander may order a subordinate to carry out cyber operations against an opposing combatant, provided that all applicable laws and norms of armed conflict are respected and strictly adhered to.

¹⁵ I. El-Sayed Ahmed Ramadan, "Confronting cyber-attacks in light of the provisions of international law", *Revue des Sciences Juridiques et Economiques*, Vol. 1, No. 67, 2025, 1849.

¹⁶ M. al-Samarrai, « The Role of International Law in Combating Cyber Attacks », 304.

Conclusion

The proliferation of cyber weapons poses a major challenge, as this new form of warfare takes place in the distinct domain of cyberspace, which is fundamentally different from the traditional physical battlefield where conventional weapons operate. Cyberattacks often impose the greatest toll on civilians, with their destructive impact sometimes equalling or even surpassing that of conventional weapons, especially when critical infrastructure such as the power plants, healthcare systems, or banking institutions of a nation are targeted.

I.Results:

1. Cyberattacks pose significant challenges to compliance with the principles and rules of international humanitarian law.
2. Cyberattacks represent a serious threat to international peace and security.
3. There is an urgent need for the international community to take decisive action towards drafting a dedicated convention prohibiting the use of cyberattacks (similar to existing international treaties banning biological and chemical weapons).
4. Promote criminal liability and enforce a zero-tolerance approach toward perpetrators of cyberattacks against civilians, whether they are individual actors or military commanders.

Conflict of Interest Statement

All authors declare that they have no conflict of interest

Reference List

❖ References in Arabic

I. Books

1. al-Samarrai, M., The Role of International Law in Combating Cyber Attacks, 1st ed., Al-Thakera Publishing & Distributors, Baghdad, 2024.
2. Khalifa, E., Cyber Power: How Nations can Manage their International Affairs in Cyber Area, Alarabi, publishing, Cairo, 2017.

II. Scientific articles

1. Al-Darmiki, H.S. and Allam, W. A., "International responsibility for cyberattacks by non-state entities", University of Sharjah Journal of Law Sciences, Vol. 21, No. 4, 2024.
2. El-Sayed Ahmed Ramadan, I., "Confronting cyber-attacks in light of the provisions of international law", Revue des Sciences Juridiques et Economiques, Vol. 1, No. 67, 2025.

❖ References in other languages:

1. Cervera García, A. and Goussens, A., "Ciberseguridad y uso de las TIC en el sector salud", Elsevier, Vol. 56, No. 3, 2024.
2. CiberSeguridad Latam, "Hospitales: Uno de los principales blancos de ciberataques", 2020: <https://ciberseguridadlatam.com/hospitales-uno-de-los-principales-blancos-de-ciberataques/> (accessed 22 March 2025).
3. Francisco José Herrera luque y otros, « Cyber risk as a threat to financial stability », revista de estabilidad financiera, núm 40, primavera 2021.
4. Gisel, L., Rodenhäuser, T. and Dörmann, K., "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts", International Review of the Red Cross, No. 913, March 2021.
5. Jarufe Bader, J.P., "Ciberataques contra la infraestructura de salud: Experiencia internacional", Asesoría Técnica Parlamentaria, September 2023.
6. Li susan et al, « Cyber - attacks on hospital systems: a narrative review », the American journal of geriatric psychiatry, open science, education and practice 7, september 2025.



This work is licensed under a

[Creative Commons Attribution NonCommercial 4.0](https://creativecommons.org/licenses/by-nc/4.0/)

[International license.](https://creativecommons.org/licenses/by-nc/4.0/)