# CYBER DEFENCE STRATEGIES IN THE HEALTHCARE SECTOR: DETERRENCE, RESILIENCE, AND CRITICAL INFRASTRUCTURE PROTECTION

*Claudia LASCATEU, PhD*

*Cyber Security Superior Manager, Cyber Security National Directorate, Bucharest*

*Mihai CONSTANTINESCU, PhD Candidate*

*Cyber Security Superior Manager, Cyber Security National Directorate, Bucharest*

DOI: 10.55535/RMT.2024.4.18

*The integration of robust cybersecurity tools and technologies within healthcare institutions is a critical strategy for strengthening national security and enhancing deterrence, particularly within NATO framework. This article highlights the strategic importance in mitigating targeted cyber threats.*

*Critical tools for real-time threat detection, establishing secure network perimeters, and comprehensive network security are discussed for their efficacy in pre-empting and responding to sophisticated cyber-attacks. Additionally, the strategic outsourcing of cybersecurity services to specialized third-party providers is explored, demonstrating the enhanced defence mechanisms achieved through leveraging external expertise and advanced technologies.*

*The article underscores the necessity of a multi-faceted cybersecurity approach, analysing the strategy and policy applied to the unique demands of the healthcare sector. By enhancing the cybersecurity posture of healthcare institutions, this research posits a significant increase in national preparedness against targeted cyber threats.*

*Keywords: national security; cyber security; healthcare system; advanced technologies; NATO;*





## INTRODUCTION

Increasing reliance on digital technologies in critical sectors such as healthcare has brought to the fore the importance of robust cyber security as a pillar of national security. In an interconnected world, cyber threats targeting medical infrastructure have become a major concern, not only for public health systems, but also for national defence mechanisms. This growing vulnerability has required the integration of sophisticated cyber security measures aimed at reducing the risks associated with cyber attacks, especially those orchestrated by state and non-state actors.

This article aims to analyse the role of advanced cyber security solutions in strengthening national security in the health sector, with a particular focus on Romania's strategic approach, highlighted in the *Cyber Security Strategy* adopted by GD no. 1321/2021. In a broader geopolitical context, these measures align with NATO's defensive framework, which prioritizes infrastructure interoperability and resilience in the face of complex cyber threats.

The detailed exploration of technologies such as artificial intelligence (AI) for threat detection, endpoint protection and advanced data encryption demonstrate how these solutions not only ensure the confidentiality, integrity and availability of sensitive health data, but also contribute to threat deterrence. This is consistent with NATO's collective defence posture, which recognizes that disruption of critical health systems could have knock-on effects on national stability and international security. Moreover, through the lens of the Tallinn Manual 2.0 and International Humanitarian Law (IHL), the protection of medical infrastructures during cyber conflicts becomes a legal obligation, emphasizing the need for advanced defensive capabilities.

By adopting a multi-faceted approach to cyber security, Romania aims to strengthen its resilience in the face of increasingly sophisticated cyber threats, thus strengthening the security architecture not only at the national level, but also among NATO allies. This article highlights the imperative to combine technological innovation with strategic collaboration, both nationally and internationally, to protect healthcare infrastructures from sophisticated cyber attacks, thereby ensuring national security and public safety. Through an analysis of existing policies,

legal frameworks and advanced technologies, this study provides insights into the future of cyber defence in the healthcare sector as a central element in national and international security.

## THE ROLE OF MEDICAL INFRASTRUCTURE IN NATIONAL SECURITY AND WITHIN NATO

The health system, through its accelerated digitization, has become an integral part of the national critical infrastructure, necessary to ensure public security and social stability. Within Romania's *Cyber Security Strategy*, protecting these infrastructures is essential for national security and defence against cyber attacks.

NATO recognizes the importance of critical infrastructures in maintaining national and regional stability. An attack on health systems not only affects the delivery of essential services, but creates vulnerabilities that can be exploited for political and military destabilization purposes.

The national cyber security system provides for the protection of the health sector by implementing specific measures, such as vulnerability assessment, incident prevention and rapid intervention in the event of cyber attacks.

### *Medical Infrastructure and National Security*

The health system, through accelerated digitization, has become an integral part of the national critical infrastructure. The importance of medical infrastructure goes beyond public health, having a direct impact on national security and social stability. The protection of the medical infrastructure against cyber attacks is essential not only for the continuity of services, but also for preventing the exploitation of vulnerabilities by state or non-state actors, including in conflict situations.

According to Romania's *Cyber Security Strategy*, critical infrastructures, including the health sector, are essential for national security, requiring specialized cyber protection measures. In this context, compliance with International Humanitarian Law (IHL) and the Tallinn Manual 2.0 is crucial to addressing cyber attacks on critical infrastructure in a manner compatible with international law.

### *Protection of Medical Infrastructures within NATO and According to International Humanitarian Law*

NATO recognizes the protection of critical infrastructures as essential to maintaining national and regional stability. Cyber-attacks on medical systems are considered a significant threat, having the potential to destabilize not only the provision of essential services, but also the political and military balance in a NATO member state.





According to Tallinn Manual 2.0, medical infrastructures are explicitly protected against cyber attacks in conflict situations. The manual states that attacks on medical IT systems are prohibited, as they are not legitimate military targets and are protected by the **principle of distinction**. Thus, the intentional destruction or disruption of medical services, whether by cyber or physical means, can be considered a violation of International Humanitarian Law.

Article 99 of the Tallinn Manual 2.0 emphasizes that medical facilities and other infrastructures providing care are protected from being legitimate targets in cyber armed conflicts, and states have an obligation to take appropriate measures to protect these targets against cyber attacks.

### *National Cyber Security System and Health Sector Protection*

Romania, through the national cyber security system, implements concrete measures to protect critical infrastructures, including the health sector. These measures are aligned with international humanitarian law and the principles enunciated in the Tallinn Manual 2.0, which considers that medical infrastructures must be protected both in peacetime and during armed cyber conflicts.

According to Tallinn Manual 2.0, Romania must adopt preventive measures, such as:

- Assessing the cyber vulnerabilities of medical infrastructures and improving security to prevent large-scale cyber attacks.
- Preventing incidents by implementing advanced security solutions such as intrusion detection (IDS/IPS), data encryption and real-time system monitoring.
- Rapid intervention in case of cyber attacks by specialized teams, according to the provisions of IHL and Tallinn Manual 2.0, which emphasizes the need for a coordinated and proportionate response in the event of an attack.

### *Impact on National and Regional Security under International Humanitarian Law and Tallinn Manual 2.0*

Cyber attacks on medical infrastructure can seriously disrupt the functioning of the health system, but also have a significant impact on the supply chain of the medical sector, which can cause serious consequences for national and regional security. In this context, IHL and Tallinn Manual 2.0 provide a solid framework for protecting not only medical infrastructures, but also systems associated with the cyber supply chain. In accordance with the **principle of proportionality** in the law of armed conflict, states must refrain from attacks that may cause disproportionate

damage to civilian infrastructure, including medical infrastructure. Tallinn Manual 2.0 reinforces these principles, highlighting that any attack on a hospital or medical IT system can constitute a serious violation of IHL.

The medical supply chain comprises a complex network of systems that include the production, storage and distribution of medicines, medical equipment and other critical materials required for the efficient operation of health services. In the digital age, this network relies heavily on IT infrastructures for order management, shipping and inventory monitoring. According to Tallinn Manual 2.0, a cyber attack on health infrastructure can severely affect the supply chain, with major side effects such as shortages of essential medical equipment or medicines for the population.

Article 70 of the Tallinn Manual 2.0 states that cyber attacks must be directed only at military targets and cannot include medical facilities or their associated IT systems. In addition, medical infrastructures must be **protected against indirect attacks or the collateral effects of cyber operations.**

Cyber attacks that disrupt the medical supply chain can have devastating consequences for the health system and national security. During the COVID-19 pandemic, we witnessed the vulnerabilities of supply chains, where any delay in the delivery of medical equipment or essential medicines had a direct impact on public health. In a cyber conflict, disrupting these chains can be used as a destabilizing tactic, leading to a health and social crisis of major proportions.

International Humanitarian Law provides for the protection not only of medical infrastructures, but also of the critical networks that support these infrastructures. Tallinn Manual 2.0 extends this protection to digital networks that manage the logistics and supply of medical resources, emphasizing that attacks on these networks are a violation of the IHL's Principle of Proportionality. A cyber attack affecting a hospital's supply chain, blocking the supply of essential equipment or medicine, could cause a disproportionate effect on the civilian population and could be considered a war crime.

NATO has recognized the **vulnerability of cyber supply chains** and established measures to protect critical infrastructures that support medical supply and logistics in the event of conflict. As part of cyber defence strategies, NATO promotes the sharing of information between member states to identify and prevent vulnerabilities in supply chains. In addition, NATO encourages collaboration between the public and private sectors to secure these critical networks.

Romania, as a NATO member, is obliged to adopt measures for the protection of the medical supply chain and the infrastructures that support the supply of essential





resources. In the context of a cyber threat, protecting these networks is essential to ensure the continuity of medical services and prevent a major public health crisis.

Under International Humanitarian Law and the provisions of the Tallinn Manual 2.0, states have an obligation to take proactive measures to protect critical infrastructures, including medical supply chains, against cyber-attacks (Article 99, the Tallinn Manual 2.0).

### *International Humanitarian Law and Tallinn Manual 2.0*

Cyber attacks are recognized as modern forms of conflict and the Tallinn Manual 2.0 provides an essential legal framework for addressing them under the Law of Armed Conflict. Medical infrastructures, especially digitized ones, are protected not only by the traditional norms of IHL, but also by the new interpretations and guidelines provided by Tallinn Manual 2.0, which states that cyber attacks on medical infrastructures are prohibited, regardless of the form of the conflict.

*

Medical infrastructure is a critical pillar of national and international security, and its protection against cyber attacks is regulated by both International Humanitarian Law and the Tallinn Manual 2.0. These legal frameworks provide explicit protection to medical facilities, prohibiting any cyber attack that could disrupt their operation.

Romania, in collaboration with NATO and aligned with the provisions of Tallinn Manual 2.0, has the responsibility to implement proactive measures to protect medical infrastructures against cyber attacks. Cyber security measures and national strategies must be consistent with the provisions of IHL and Tallinn Manual 2.0 to ensure compliance with international obligations and protect these critical infrastructures during cyber conflicts.

## CYBER THREATS AND THE NEED FOR AN INTEGRATED APPROACH

Romania, as part of a region increasingly exposed to large-scale cyber attacks, developed the *Cyber Security Strategy* in 2022 to protect critical infrastructures, such as the health sector, from cyber threats from state and non-state actors. This chapter analyses the need for an integrated approach to the protection of the health sector in the light of relevant international regulations and frameworks, including the NIS2 Directive, International Humanitarian Law, Tallinn Manual 2.0, Cyber Security Law no. 58/2023, and the measures included in the Inventory report.

### *Cyber Threats and the Relevance of the NIS2 Directive*

The NIS2 Directive (Network and Information Security Directive), adopted at the level of the European Union, represents an essential legislative framework for the protection of critical infrastructures, including the health sector, against cyber threats. The directive focuses on the confidentiality, integrity and availability of data, aiming to improve the security and resilience of critical infrastructures at national and European level.

In the context of NIS2, the health sector is defined as an essential infrastructure, and Romania, as an EU member state, must implement robust cyber security measures to align with European requirements. They include:

- Regular security audits to assess cyber risks.
- Rapid response measures in case of cyber security incidents.
- Advanced cyber attack detection and prevention systems.

NIS2 requires the implementation of advanced technological solutions such as artificial intelligence and blockchain to ensure the security of medical data and critical health infrastructures.

### *Cyber Security Law no. 58/2023 and Its Application in the Health sector*

Cyber security law no. 58/2023 provides a national legislative framework that aligns with the requirements of the NIS2 Directive and establishes clear obligations for the protection of critical infrastructures, including those in the health sector. This law introduces strict data protection and security incident management measures, requiring entities in the healthcare sector to implement technical and organizational security measures to prevent and promptly respond to cyber attacks.

Law no. 58/2023 requires:

- Mandatory reporting of cyber incidents affecting critical infrastructures, including healthcare IT systems.
- Sharing information between the public and private sectors to quickly identify and neutralize cyber threats.

This law joins other international regulations, such as the Tallinn Manual 2.0 and IHL, to ensure the protection of medical infrastructure against cyber attacks in accordance with international security standards.

### *The RO-CCH Report and the Implementation of Emerging Technologies*

According to the Report *Inventory of cyber security tools and technologies suitable for or dedicated to healthcare and health institutions (D4.3)* from the Romanian Cyber Care Health Project – RO-CCH (RO-CCH, 2022), funded by the European





Commission through CNECT.H – Digital Society, Trust, and Cybersecurity, Romania has started to implement a series of advanced measures to strengthen the cyber defence capacity, with a focus on the protection of critical infrastructures in the field of health. The report highlights the importance of using emerging technologies such as:

- Artificial intelligence (AI) for real-time threat detection.
- Blockchain for securing medical data and supply chains.
- Advanced encryption to protect sensitive data from unauthorized interception.

These technologies are essential to respond to complex and evolving threats from state and non-state actors. Also, the mentioned RO-CCH report recommends regular audits and the use of incident management platforms to ensure the operational continuity of medical services in the face of potential cyber attacks.

### *The Need for an Integrated Approach*

Romania, through the 2022 *Cyber Security Strategy*, is taking important steps in protecting critical infrastructures, but must continue to adopt effective measures in cooperation with its international partners, such as NATO and the European Union. Inter-agency collaboration and information sharing between the public and private sectors is crucial to creating a resilient cyber environment.

In addition, the integrated approach must also include measures to educate and raise awareness of medical and IT staff about new threats and technologies. Tallinn Manual 2.0, IHL, NIS2 and Law no. 58/2023 provide a solid framework for securing medical infrastructures, but the implementation of these regulations at national and local level is essential for the protection of the health sector against cyber threats.

*

Romania has developed a robust framework for the protection of critical infrastructures, including the health sector, through the 2022 *Cyber Security Strategy*, the NIS2 Directive, Law no. 58/2023, and the principles established in Tallinn Manual 2.0 and International Humanitarian Law. These measures are essential for ensuring the confidentiality, integrity and availability of medical data, but also for the protection of medical infrastructures against cyber attacks supported by state and non-state actors. Romania must continue to invest in advanced technologies, conduct regular security audits and strengthen international cooperation to create a resilient and secure cyber environment.

## ADVANCED CYBER SECURITY MEASURES IN THE HEALTH SECTOR AND THEIR IMPACT ON NATIONAL SECURITY AND NATO STRATEGY

Romania's *Cyber Security Strategy*, provided for in GD no. 1321/2021 and adopted in 2022, promotes the use of innovative technologies, such as artificial intelligence and behavioural analysis systems, to improve detection and response capabilities in the health sector. According to GD no. 1321/2021, it is essential that health infrastructures should be protected by advanced technological measures, such as next-generation firewalls, continuous traffic monitoring systems and data loss prevention programmes. These measures are necessary to protect patient data and prevent cyber attacks that can destabilize the medical infrastructure.

Within NATO's strategy, interoperability and infrastructure security are key priorities. The use of these technologies in Romania contributes to strengthening cyber security in the field of health and to ensuring a robust cyber defence, compatible with NATO requirements.

### *National Policies and Strategies*

Romania's *Cyber Security Strategy* constitutes the foundation of national policies in the protection of critical infrastructure, including the health sector. It promotes the use of innovative technologies to strengthen detection and response capabilities in the face of cyber threats, emphasizing the need to adopt advanced security solutions such as:

- Behavioural analytics systems, which help identify anomalous cyber activities and can detect attacks before they cause significant damage.

According to GD no. 1321/2021, health infrastructures are considered critical for national security, and their protection is essential to prevent cyber attacks that could destabilize the entire medical infrastructure. Technological measures promoted in this strategy include:

- New generation firewalls for network perimeter protection.
- Continuous traffic monitoring systems to detect suspicious activity.
- Data Loss Prevention (DLP) programmes, which protect sensitive patient data from theft or destruction.

These advanced measures help ensure the confidentiality, integrity and availability of patient data and represent an important barrier against cyber attacks aimed at destabilizing medical infrastructures.

### *Interoperability and NATO Strategies*

Within the NATO strategy, cyber security of critical infrastructures, including the health sector, is considered a **collective security priority**. Romania, as a NATO





member state, aligns its national policies with the requirements of the alliance, ensuring interoperability and the ability to react unitedly to cyber attacks. NATO emphasizes the importance of interoperability between member states' cyber systems to ensure a rapid and effective response to coordinated attacks by state and non-state actors.

Among the technological and tactical measures promoted by NATO for the protection of medical infrastructures are:

- Incident management systems (IMSs), which integrate data from various sources and help detect and manage cyber incidents.
- Advanced end-point protection solutions to ensure the security of devices connected to the network.
- Data Loss Prevention (DLP) platforms, designed to prevent the leakage of sensitive data or unauthorized access to information critical to national security and public health.

These measures are essential to prevent attacks such as ransomware or other types of complex attacks that target not only medical data, but also the critical functioning of healthcare IT systems. Interoperability between these systems is crucial to ensure a robust cyber defence compatible with NATO standards, thus strengthening the collective defence of critical infrastructures in the region.

### *The Impact of Advanced Measures on National and International Security*

The adoption of advanced cyber security measures in the healthcare sector has a profound impact on national and international security, contributing to the stability of critical infrastructures and defence against cyber attacks. This section analyses the implications of these measures from the perspective of cyber deterrence theory, compliance with international norms, and their role in strengthening national cyber defence capabilities, according to Romania's *Cyber Security Strategy*, Tallinn Manual 2.0 and International Humanitarian Law.

#### Impact on national security

Advanced cyber security measures have a direct impact on national security, particularly through the protection of critical healthcare infrastructure. According to cyber resilience theory, a nation's ability to withstand and rapidly respond to cyber threats ensures the continuity of essential services. Protecting IT systems that manage patient data and medical supply flows contributes to internal stability and the maintenance of public order, even in large-scale cyber-attack situations.

In accordance with Romania's *Cyber Security Strategy*, measures such as the use of artificial intelligence (AI) for incident detection and response, the implementation

of new generation firewalls and data loss prevention (DLP) systems, are key tools for preventing and managing cyber attacks on healthcare infrastructure. These technologies are essential to prevent the confidentiality, integrity and availability of medical data from being compromised and to protect the critical resources needed to operate healthcare systems.

According to the theory of proactive cyber defence, the use of technologies such as AI not only helps in real-time detection of threats, but also enables an early reaction to attacks, minimizing the impact on critical infrastructure. Implementing these measures helps ensure business continuity, a central national security objective in any cyber security crisis.

**Impact on international security and NATO cooperation**

At the international level, the integration of advanced security measures according to NATO standards contributes to the strengthening of collective security and compliance with the requirements of the cyber defence strategy of the alliance. Interoperability between national cyber systems and those of NATO allies is essential to ensure a robust and coordinated defence against cyber threats. According to collective security theory, the ability to respond quickly and effectively to cyber attacks helps deter state and non-state actors that may attempt to exploit vulnerabilities in medical infrastructures.

Technologies such as SIEM (Security Information and Event Management), advanced firewalls and end-point protection ensure the rapid detection and management of incidents, allowing Romania to act within NATO strategies and contribute to regional stability. The use of AI and behavioural analytics helps prevent sophisticated attacks and reduce response time, thereby strengthening cyber defence capability internationally.

**The deterrent effect on malicious actors**

Another key aspect of advanced cyber security measures is the deterrent effect they have on malicious actors. *Cyber deterrence theory*[1] suggests that the presence of advanced technologies, combined with the state's ability to detect and respond

[1] Deterrence theory can be examined in detail by distinguishing between two key concepts: denial deterrence and punitive deterrence. Denial deterrence involves preventing adversaries from achieving their goals by making attacks difficult or unlikely, typically through robust defensive measures such as advanced cybersecurity systems, encryption, and real-time threat detection. Punitive deterrence, in contrast, focuses on imposing significant consequences or retaliation on attackers, discouraging them from initiating attacks due to the high risks involved. In the field of cybersecurity, both strategies can be applied: denial through technical measures that make systems difficult to compromise, and punishment through legal and diplomatic measures. In the healthcare sector, punitive deterrence can take the form of legal and diplomatic responses to cyberattacks targeting healthcare infrastructure, including working with international allies to isolate malicious actors (A.N.)





quickly to attacks, creates a less favourable cyber environment for attackers. Romania, by adopting these measures, strengthens its deterrence capacity at the national and international level, making it difficult to compromise medical infrastructures.

Next-generation firewalls and DLP play a critical role in protecting healthcare infrastructures from the theft or compromise of sensitive data. According to the theory of denial deterrence, advanced cybersecurity measures increase costs and risks for attackers, thereby reducing the likelihood of successful attacks.

**Protection of medical infrastructures according to Tallinn Manual 2.0 and International Humanitarian Law**

In the context of Tallinn Manual 2.0 and International Humanitarian Law, advanced cyber security measures ensure legal protection of medical infrastructures in the event of cyber conflicts. The advanced cyber security measures implemented in Romania ensure compliance with these international norms, reducing the risks of violating the principle of distinction. By protecting medical infrastructures from cyber attacks, Romania fulfils its international obligations and contributes to maintaining global stability and security in the face of cyber conflicts.

The advanced cyber security measures implemented in the health sector, provided for in GD no. 1321/2021 and supported by the NATO strategy, have a significant impact on national and international security. The use of state-of-the-art technologies such as AI and advanced encryption, as well as the application of national and international policies and strategies, help strengthen the resilience of critical infrastructures and protect citizens against cyber attacks.

Aligning with NATO policies, adopting the measures of the NIS2 Directive and complying with the Tallinn Manual 2.0 norms ensure a robust and integrated protection of the health sector. These measures strengthen cyber defence at the national and international level, contributing to the stability and security of the region and the protection of critical infrastructures in the face of increasingly complex threats.

## STRENGTHENING NATIONAL AND INTERNATIONAL SECURITY IN HEALTH SYSTEMS

Analysing the impact of cyber defence advanced measures on national and international security, we will highlight some of the theories applied in the health sector, such as: *"Defence in Depth", "Zero Trust", "Deterrence by Denial", "Cyber Resilience" and "Shared Responsibility".*

The mentioned theories underline the need for an integrated framework, which should include advanced technological measures, institutional cooperation and international partnerships, to ensure the effective protection of critical infrastructures. By implementing these theoretical frameworks, Romania could contribute to strengthening the national and regional security, in compliance with international norms as well as with NATO and EU standards in cyber security.

### *"Defence in Depth" Theory and Its Application in the Health Sector*

*"Defence in Depth"* theory is a key concept in cyber security and promotes the idea that effective security is based on multiple layers of defence. In the context of healthcare cyber security, this approach is applied by using a combination of technologies, procedures and organizational measures to protect critical infrastructure.

Advanced technological measures such as next-generation firewalls, data encryption and end-point protection are only one layer of this multi-level system. The implementation of data loss prevention (DLP) systems, SIEM platforms and behavioural detection solutions constitute other layers of defence, creating a resilient barrier against cyber attacks.

This theory holds that reducing reliance on a single protection mechanism and creating a multi-layered security architecture help delay and detect cyber-attacks, thereby reducing their success-associated risks. In the healthcare sector, the application of the *"Defence in Depth"* theory contributes to the protection in depth of sensitive data and critical functionalities, increasing the degree of system resilience.

### *"Zero Trust" Theory and the Protection of Medical Data*

*"Zero Trust"* theory has become a central paradigm in modern cyber security. It implies that there should be no implicit trust between different network segments or between users accessing the resources. In a *"Zero Trust"* system, access to resources is only granted based on continuous checks of identity and compliance with security policies.

In the health sector, this theory is applied by strictly controlling access to medical data and essential infrastructures. Every access is monitored and verified, eliminating the risk of an attacker gaining unauthorized access and stealing or compromising critical data. Data encryption and the use of multi-factor authentication (MFA) are central to the implementation of this theory.

Adopting the *"Zero Trust"* model in healthcare infrastructures helps create a more secure cyber environment and significantly reduces the risk of internal





or external attacks that could compromise patient data. In an international context, this model is essential to ensure interoperability and protection of sensitive data between NATO and EU partners.

### *"Deterrence by Denial" Theory and Cyber Deterrence*

*"Deterrence by Denial"* theory is an approach that focuses on preventing the success of an attack through technical and organizational measures that make attacks extremely difficult to carry out. In the case of the health sector, the application of this theory consists in the development of resilient cyber systems, so that attackers can be deterred from the start, due to the complexity and effectiveness of the security measures implemented.

Advanced cybersecurity measures such as real-time anomaly detection, continuous monitoring, and the use of automated cyber incident response solutions are all tools that contribute to *deterrence by denial*. A clear example is the deployment of AI technologies for behavioural analysis that can proactively detect and respond to attacks before they become a major threat.

In this context, the state's ability to prevent the success of cyber attacks on health infrastructures creates a deterrent shield that protects both national and international security. This theory also aligns with the *Active Defence Theory*, which involves continuous monitoring and intervention to prevent malicious activities.

### *"Cyber Resilience Theory" and the Importance of Recovery Capabilities*

*"Cyber Resilience"* theory is central to understanding the impact of advanced cyber security measures on national and international security. Cyber resilience refers to the ability of a critical infrastructure to detect, withstand and quickly recover from a cyber attack, ensuring the continuity of essential operations.

In the healthcare sector, it means that not only prevention and detection measures are important, but also the ability of systems to return to a normal operational state after a cyber incident. Implementing disaster recovery plans (DRPs) and backup systems is central to this theory, complementing advanced cyber security strategies.

Resilience capabilities are critical in international collaboration, as cyber attacks can simultaneously affect infrastructure in multiple countries. Romania's ability to collaborate effectively with its NATO and EU partners to ensure the operational continuity of health infrastructures is a central pillar in its cyber security strategy.

### *"Shared Responsibility" Theory and the Collaboration between the State and the Private Sector*

Another relevant theoretical framework for analysing the impact of advanced cyber security measures is the *"Shared Responsibility"* theory. It suggests that the cyber security of critical infrastructures such as the health sector cannot be ensured by the state alone, but requires close collaboration between the public and private sectors.

In this context, the state creates the legislative framework and the basic infrastructure for cybersecurity, but private entities – such as healthcare providers and technology companies – play a crucial role in implementing and maintaining security measures. This partnership between the state and the private sector is essential to ensure the continuity and resilience of the medical infrastructure against cyber threats.

Law no. 58/2023 imposes this principle by requiring entities that operate critical infrastructures to collaborate with national authorities to protect their systems, in accordance with international requirements.

## CONCLUSIONS

As cyber attacks become more sophisticated and frequent, future research directions in cyber security for critical infrastructures, including the healthcare sector, should explore several key areas to support the continued evolution of protection and defence measures.

By implementing Romania's *Cyber Security Strategy* and adopting a position consistent with NATO standards and the requirements of the NIS2 Directive, Romania is strengthening its cyber defence capabilities. These measures not only protect critical health infrastructures against cyber attacks, but also create a significant deterrent effect on state and non-state actors who would attempt to exploit digital vulnerabilities.

At the same time, the application of the principles of International Humanitarian Law and the norms of Tallinn Manual 2.0 underlines the need to protect medical infrastructures in the context of cyber conflicts, ensuring Romania's compliance with international legislation on the protection of civilians and essential infrastructures. This legal framework provides a solid basis for the protection of critical health infrastructures and contributes to maintaining national and regional stability.

In conclusion, we consider that advanced cyber security in the health sector is an indispensable component of national and international security, and the application of innovative technologies, along with compliance with international





norms, is an effective strategy for protection against cyber threats. By collaborating with international partners and implementing robust security measures, Romania strengthens its leadership position in regional cyber security and contributes to the collective resilience of NATO and the European Union. This holistic approach ensures the protection of citizens and critical infrastructure in the face of the complex challenges of modern cyberspace.

## BIBLIOGRAPHY:


1. *International Humanitarian Law and Civil Infrastructure Protection,* https://www.icrc.org/en/document, retrieved on 12 June 2024.
2. *EU Cyber Resilience Act*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52022PC0454, retrieved on 23 May 2024.
3. Hotărârea de Guvern/Government Decision no. 1.321 on 30 December 2021, to adopt *Strategia de securitate cibernetică a României pentru perioada 2022-2027/ Romania's Cyber Security Strategy* and its implementation plan, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128, retrieved on 13 August 2024.
4. *Inventory of cyber security tools and technologies suitable for or dedicated to healthcare and health institutions (D4.3) "Romanian Cyber Care Health – RO-CCH"*, RO-CCH - DIGITAL-2022-CYBER-02, https://dnsc.ro/pagini/proiect-ro-cch, retrieved on 22 May 2024.
5. *Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative/Law no. 58/2023 regarding cyber security and defence*, https://legislatie.just.ro/Public/DetaliiDocument/265677, retrieved on 2 June 2024.
6. *NATO's Concept for Deterrence and Defence*, https://www.nato.int/docu/review/articles/2021, retrieved on 22 may 2024.
7. *NATO Cyber Defence Policy*, https://www.nato.int/cps/en/natolive/topics_78170.htm., retrieved on 22 June 2024.
8. RO-CCH (2022), https://dnsc.ro/pagini/proiect-ro-cch, retrieved on 14 June 2024.
9. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, https://ccdcoe.org/research/tallinn-manual, retrieved on 23 May 2024.