ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/ 10.47459/cndcgs.2026.32**

Healthcare as a Battlefield of Hybrid Warfare

Kateřina DOSTÁLOVÁ[1*], Zdeněk JÍCHA[1], Michal MATĚJKA[1], Lukáš MIKLAS[1], Jana HUDZIETZOVÁ[1], Leoš NAVRÁTIL[1], Jan KOLOUCH[2]

[1]*Department of Health Sciences and Civil Protection, Faculty of Biomedical Engineering, Czech Technical University in Prague, Nam. Sitna 3105, Kladno, Czech Republic2*
[2]Department of Law and Cybersecurity, AMBIS, Lindnerova 575/1, Prague, Czech Republic

*Correspondence: *katerina.dostalova@fbmi.cvut.cz*

Abstract

The article analyzes the healthcare sector as a strategic target in hybrid conflicts, with a focus on cyber threats. Based on OSINT and a comparative analysis of incidents, it identifies typical attack patterns, their operational impacts, and systemic vulnerabilities in healthcare systems. The findings demonstrate that cyber incidents disrupt healthcare delivery and have broader security implications. The study emphasizes the need to integrate cybersecurity, crisis management, and the protection of sensitive patient data.

KEYWORDS: *cyber security; healthcare systems; hybrid threats; Ukraine conflict; patient data; critical infrastructure; military personnel; resilience; health law*

Citation: Dostálová, K.; Jícha, Z.; Matějka, M.; Miklas, L.; Hudzietzová, J.; Navrátil, L.; Kolouch, J. Healthcare as a Battlefield of Hybrid Warfare. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959. https://doi.org/ 10.47459/cndcgs.2026.32

1. Introduction

The security environment in Europe and globally has undergone a fundamental transformation in recent years. Modern conflicts are no longer waged exclusively through conventional military operations, but increasingly combine military means with cyber, information, economic, and legal tools. This type of conflict is referred to in the academic literature as hybrid warfare, which is characterized by the coordinated use of diverse tools with the aim of weakening the adversary while simultaneously blurring the line between peace and armed conflict [1]. Hybrid strategies often target the vulnerabilities of open societies and infrastructure, the disruption of which can have significant social, economic, and political impacts [2].

One of the key features of the current security environment is the growing importance of civilian critical infrastructure as a potential target of conflict. Modern societies are heavily dependent on complex and interconnected systems providing essential services such as energy, transportation, communications, and healthcare. Disruption of these systems can lead to extensive secondary impacts that go beyond the purely technical level of the incident and can destabilize the functioning of society as a whole [3]. For this reason, the protection of critical infrastructure is becoming one of the key elements of both national and international security policy.

In light of the above, healthcare systems represent an exceptionally sensitive and strategically significant sector. Healthcare facilities combine several factors that make them attractive targets in hybrid conflicts. Above all, they are institutions that enjoy a high level of public trust and, at the same time, constitute infrastructure whose uninterrupted operation is essential for protecting the lives and health of the population – not only within the given state. Any disruption to healthcare services can have immediate humanitarian and psychological consequences and significantly impact the public's perception of security [4].

Due to the growing digitization of healthcare, healthcare systems are increasingly dependent not only on digital technologies (hospital information systems, telemedicine platforms, or networked medical devices) but also on the data itself (e.g., electronic health records). This technological transformation brings significant benefits in terms of the quality and accessibility of healthcare, but at the same time expands the potential attack surface for cyberattacks [5].

Peer-review under responsibility of General Jonas Žemaitis Military Academy of Lithuania and University of Defence, Czech Republic

Healthcare institutions process and store large volumes of highly sensitive data that may have not only economic value but, in certain geopolitical contexts, also intelligence value. Information about the health status of members of the armed forces, critical infrastructure workers, or public officials can be used to gain strategic advantages or as a tool for coercion [6].

The significance of these threats is also confirmed by empirical data from recent years. Cyberattacks on healthcare institutions are among the fastest-growing categories of security incidents in the critical infrastructure sector. Particular attention has been drawn, for example, to attacks on hospitals during the COVID-19 pandemic or during the armed conflict in Ukraine, where healthcare institutions have repeatedly been the target of both physical and cyberattacks [7]. According to analyses by international organizations, these incidents often result in the paralysis of hospital information systems, the limitation of diagnostic services, and the necessity of switching to manual operating mode [8].

The increasing frequency of these incidents is leading the professional community and policymakers to reevaluate the role of healthcare in the security environment. Healthcare can no longer be viewed merely as a sector providing a public service, but increasingly as part of a broader system of national resilience and critical infrastructure protection [3]. Attacks on healthcare systems can serve several strategic functions in hybrid conflicts-ranging from directly disrupting healthcare delivery to destabilizing society and obtaining sensitive information.

The aim of this article is to analyze the role of healthcare systems in the context of hybrid conflicts based on a comparative analysis of selected cyber incidents and to examine the security, organizational, and legal implications of cyber threats targeting healthcare infrastructure. The study focuses primarily on the question of to what extent healthcare can be understood as an operational domain of hybrid warfare and identifies key factors influencing the resilience of healthcare systems to these threats.

2. Hybrid Threats, Operations, Strategies, and Hybrid Warfare

Hybrid threats should be understood not only as a set of cross-domain tools, but also as a process that unfolds over time and can gradually escalate from subtle activities to more overt forms of coercion [9]. In this regard, a practical analytical framework is provided by a conceptual model developed by the European Commission's Joint Research Centre (JRC) in collaboration with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), which structures hybrid activity through the pillars of actors, their strategic objectives, domains, tools, and phases of action. The framework aims, among other things, to capture the "time variable" and enable an understanding of how an actor combines tools to influence the target state and achieve strategic objectives [9, 10].

The model explicitly distinguishes the "PHASES" section and identifies three consecutive phases:

- priming;
- destabilization through operations and campaigns;
- coercion through hybrid warfare [9].

This framework supports an analytical understanding of hybrid operations as a gradual escalation from a preparatory and formative period ("priming"), through a destabilization phase carried out via operations and campaigns, to a coercion phase carried out through hybrid warfare [9]. From the perspective of security studies, the main benefit of this approach lies in its ability to link observed phenomena (e.g., information from various domains) to a hypothesis regarding the current phase of hybrid activity, thereby refining decision-making regarding an adequate response and the prioritization of measures [10].

Early detection plays a key role in the realm of hybrid threats or warfare, as it enables the identification of coordinated hostile activities at an early stage, when they occur below the threshold of open armed conflict and are deliberately disguised as ordinary political, economic, or social phenomena. Hybrid operations (e.g., disinformation, cyberattacks, economic coercion, or institutional infiltration) are so effective precisely because of their gradual nature, ambiguity, and difficulty in attribution; Early identification of warning indicators therefore enables the state to strengthen its resilience, take preventive measures, and prevent escalation before systemic damage is caused. Both NATO and the European Union emphasize that the ability to share information, build situational awareness, and integrate civilian and military intelligence is a fundamental prerequisite for an effective response to hybrid threats and, at the same time, an important deterrent, as it reduces the success of an adversary's strategy based on surprise and the exploitation of societal vulnerabilities [9, 10, 11].

Over the past two decades, the concept of hybrid warfare has become one of the key terms in the field of security studies. Although there is no single, universally accepted definition, most of the scholarly literature agrees that hybrid warfare represents a strategy that combines conventional military means with a wide range of non-military tools, including cyber operations, information campaigns, economic pressure, and political or legal action [1]. The aim of these activities is to weaken the adversary through the systematic exploitation of its structural vulnerabilities, often without the need for open armed conflict.

Hybrid strategies are characterized by a high degree of complexity and flexibility in the tools employed. Actors engaged in hybrid operations utilize a combination of state and non-state means, with individual operations potentially unfolding simultaneously across multiple domains: military, informational, economic, and cyber [12]. This multidimensional nature of hybrid operations significantly complicates their detection, attribution, and subsequent

response by the targeted state. It is precisely the difficulty of unequivocally identifying the perpetrator of an attack that makes hybrid strategies an effective tool of geopolitical rivalry.

The significance of hybrid operations became particularly evident in connection with the conflict in Ukraine after 2014 and subsequently following the Russian invasion in 2022. Analyses by security institutions point to the systematic use of cyberattacks, disinformation campaigns, and economic pressure as part of a broader strategy to destabilize the state and its institutions [13]. In this context, it is becoming increasingly clear that modern conflicts are not limited solely to the military battlefield but also affect civilian sectors that are essential to the functioning of society.

Critical infrastructure is therefore becoming one of the most significant targets of hybrid operations. Under the current Czech legal framework, critical infrastructure is defined as an asset, facility, equipment, network, or system (or part thereof) that is essential for the provision of an essential service, where an essential service is understood to be a service necessary for maintaining the basic functions of the state, economic activities, security, public health, or the environment. A critical infrastructure entity is a provider of an essential service whose critical infrastructure is located within the territory of the Czech Republic and is included on the list of critical infrastructure entities [14]. Modern infrastructures are increasingly interconnected and digitized, which enhances their efficiency but simultaneously increases their vulnerability to cyber threats.

From the perspective of hybrid strategies, critical infrastructure represents an attractive target primarily because its disruption can trigger chain reactions in other sectors. For example, an attack on energy infrastructure can affect transportation, communications, or healthcare services. Similarly, cyberattacks on information systems can disrupt the operations of public institutions or economic structures. These secondary impacts may ultimately have greater strategic significance than the technical incident itself [15].

International organizations and national governments are therefore paying increasing attention to the protection of critical infrastructure. The European Union has adopted Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (Critical Entities Resilience Directive), which establishes a framework for strengthening the resilience of entities providing essential services and their ability to prevent, protect against, and respond to incidents, as well as to restore service provision following a disruption. The Directive also emphasizes the need for coordinated implementation alongside Directive (EU) 2022/2555 (NIS2), given the relationship between the physical and cybersecurity of critical entities, which is also relevant to threats employed in a hybrid context [3]. Similarly, NATO documents emphasize that the protection of critical infrastructure is a fundamental component of collective security and the ability of states to confront modern forms of conflict [16].

Within this framework, healthcare is gradually becoming one of the key sectors of critical infrastructure. Healthcare systems are of vital importance for the protection of public health and also play a crucial role in managing crisis situations, including pandemics or armed conflicts. As recent experiences in Ukraine and other regions demonstrate, healthcare infrastructure can be the target of both physical and cyberattacks [7]. These attacks can have not only direct humanitarian consequences but can also be part of broader strategies aimed at destabilizing society.

Furthermore, the growing digitization of healthcare systems is creating new types of vulnerabilities that can be exploited in hybrid conflicts. Hospitals are increasingly dependent on digital information systems, networked medical devices, and external IT service providers. While these factors can enhance the efficiency of healthcare, they also create potential entry points for cyberattacks [5].

Understanding the relationship between hybrid threats and critical infrastructure protection is therefore key to formulating effective security strategies and subsequently developing measures to mitigate them. In the case of healthcare, it is necessary to consider not only technical cybersecurity measures but also organizational, legal, and strategic mechanisms that can contribute to strengthening the resilience of healthcare systems against hybrid threats.

It is therefore crucial – not only for the Czech Republic – to view cyber defense as part of security, to integrate it with other areas, and to prepare for the blurred lines between different types of attacks. A nation's resilience depends not only on the military but also on the protection of networks, data, and the information space.

3. Healthcare as a Strategic Objective of Hybrid Operations

In today's security environment, healthcare systems represent one of the most vulnerable sectors of critical infrastructure. Their importance lies not only in the provision of healthcare, but also in their role in maintaining social stability and the functioning of the state during crises. At the same time, healthcare is a sector that enjoys a high level of public trust, and any disruption to it can have significant psychological and political repercussions. It is precisely these characteristics that make healthcare infrastructure an attractive target for hybrid operations [15].

The significance of these threats is also confirmed by statistics from international security organizations. Reports from the European Union Agency for Cybersecurity (ENISA) and other institutions show that healthcare has long been among the sectors with the highest number of reported cyber incidents. The most common form of attack is ransomware, which encrypts hospital data and paralyzes the information systems of healthcare facilities [17]. These attacks can cause interruptions in healthcare delivery, delays in diagnosis, or the need to switch to manual operations.

For example, one of the most well-known incidents was the 2017 WannaCry cyberattack, which significantly affected the United Kingdom's National Health Service (NHS). This attack led to widespread disruption of hospital systems, the cancellation of thousands of planned procedures, and limitations in the provision of healthcare services across

numerous healthcare facilities [18]. The incident demonstrated how substantial the impact of cyberattacks on healthcare can be, even in cases of relatively short-term disruption of IT infrastructure.

Another significant case was the ransomware attack on the Irish Health Service Executive (HSE) in 2021, which resulted in a large-scale reduction in healthcare services across the country. The attack caused a multi-day paralysis of hospital information systems and severely disrupted the provision of healthcare [19]. These incidents illustrate that healthcare can be not only a target of financially motivated cyberattacks but also a potential instrument in broader destabilization operations.

The strategic importance of healthcare as a target has become even more evident in the context of contemporary armed conflicts. The conflict in Ukraine, for instance, has shown that healthcare infrastructure may be targeted by both physical attacks and cyber operations. Analyses by international organizations document hundreds of attacks on healthcare facilities during the first years of the conflict, leading to disruptions in healthcare provision and significant humanitarian consequences [7].

In addition to the direct disruption of healthcare services, health data also represent a valuable target. Information about the health status of the population, military personnel, or workers in critical infrastructure may have considerable intelligence value. The acquisition of such data can be used for purposes such as strategic intelligence gathering, blackmail, or information operations [20]. In the context of hybrid conflicts, health data thus acquire a new security dimension that goes beyond the traditional framework of personal data protection.

Another factor increasing the vulnerability of the healthcare sector is the organizational and technological complexity of healthcare systems. Hospitals are often dependent on external IT service providers, cloud solutions, or specialized medical technologies. Insufficient network segmentation, outdated information systems, and a lack of specialized cybersecurity professionals may further increase the risk of successful cyberattacks [21].

For these reasons, healthcare is increasingly perceived as part of the broader system of national security and state resilience. The protection of healthcare infrastructure is no longer merely a matter of health policy or personal data protection but is becoming a significant component of national security strategy. Strengthening the cybersecurity of healthcare systems, protecting health data, and enhancing the organizational resilience of healthcare institutions therefore represent key factors in addressing hybrid threats in the current security environment.

3.1 The Strategic Value of Health Data in Modern Conflicts

The digitalization of healthcare increases the availability and usability of data for clinical care; at the same time, however, it enhances their significance as a strategic resource in the context of hybrid conflicts. In this regard, health data become a highly valuable target not only from the perspective of privacy protection but also in terms of national security, as the healthcare sector is closely interconnected with other critical infrastructure sectors, particularly energy, communication networks, public administration, and logistics systems [22, 23].

The intelligence value of health data lies primarily in the ability to profile population vulnerabilities, map the actual capacities of the healthcare system, and, in the case of specific groups, indirectly assess impacts on operational readiness and personnel stability. These data gain further significance when combined with other data sources, such as administrative registries, communication metadata, or open-source information, thereby increasing the risk of secondary and cascading effects [23, 26].

From a methodological perspective, it is important to note that cyber incidents in the healthcare sector often take the form of long-term, covert intrusions aimed at information gathering rather than immediate disruption or destruction. This mode of operation corresponds to the concept of persistent intelligence collection, where the full security impact may only become apparent over time [24, 26].

3.2 Ukraine: Healthcare Data Caught Between Cyber Conflict and System Overload

In the context of Russia’s aggression against Ukraine, cyber operations have long been described as part of a broader hybrid strategy, with healthcare representing one of the sensitive targets. Analytical studies emphasize that cyberattacks are primarily used for reconnaissance, intelligence gathering, and the gradual disruption of a state’s ability to function effectively, rather than for immediate operational collapse [23, 24].

Medical literature already highlighted in the early phase of the full-scale conflict that, alongside kinetic violence, a parallel cyber dimension of the conflict was unfolding, involving attempts to obtain personal and healthcare datasets. This issue is further exacerbated by the rapid digitalization of the Ukrainian healthcare system and the expansion of electronic health records, which – despite their undeniable benefits – increase the system’s attack surface [22, 25].

At the same time, the healthcare sector in Ukraine is exposed to extraordinary operational strain as a result of physical attacks on facilities and personnel. Comprehensive databases documenting attacks on healthcare facilities show that the sector has been persistently subjected to a combination of direct violence and secondary systemic effects, which disrupt the continuity of care and reduce the capacity for rapid recovery [27, 28].

From a crisis management perspective, the combination of physical destruction of infrastructure, energy outages, and cyberattacks is particularly problematic. This multi-domain stress reduces the ability of the healthcare system to detect and respond to compromises of information systems precisely at a time when its capacity is under the greatest strain [22, 24].

3.3 Israel: Targeting the Healthcare Sector, Data Breaches, and Security Implications

The Israeli security context is particularly relevant in that the healthcare sector has long been exposed to a combination of criminal and state-sponsored cyber operations, often during periods of heightened security tension. Open-source reporting repeatedly indicates that Israeli healthcare institutions are frequent targets of attacks aimed not only at disrupting operations but also at obtaining sensitive data [29, 31].

A key example is the publicly confirmed cyberattack on Ziv Medical Center, which Israeli authorities attributed to actors linked to Iran and Hezbollah. Although major operational disruption was prevented, part of the data was exfiltrated, illustrating the hybrid nature of the attack, combining elements of coercion, intelligence gathering, and psychological influence [29, 30].

Further incidents reported in 2025 demonstrate that even when attacks are successfully blocked at an early stage, there remains a tangible risk of sensitive data leakage. Investigations of these cases have highlighted that healthcare constitutes an attractive target not only due to its humanitarian sensitivity but also because of the potential for secondary impacts on public trust, legal liability, and the continuity of critical services [29, 31].

From the perspective of critical infrastructure protection, it is important to note that breaches of healthcare data may, in certain scenarios, be used to enhance the effectiveness of social engineering and targeted coercion against employees with access to sensitive systems. These findings are reflected in analyses of broader campaigns targeting the civilian sector as a means of indirectly weakening the state [30, 31].

3.4 Impacts on Critical Infrastructure: From Confidentiality to Resilience

The significance of healthcare data in hybrid conflicts cannot be reduced to a mere privacy issue. Cyber incidents in the healthcare sector typically impact three fundamental levels of security: confidentiality, integrity, and data availability. In a conflict environment, these levels further reinforce one another and can escalate into operational crises that affect not only healthcare but also other critical infrastructure sectors [22, 23].

A synthesis of findings from Ukraine and Israel shows that the healthcare sector is targeted in hybrid conflicts both for its humanitarian sensitivity and for its systemic links to the functioning of the state. For this reason, healthcare information systems should be assessed not only in terms of standard cybersecurity but also in terms of resilience, the ability to operate in degraded mode, and the rapid restoration of key functions [24, 26].

3.5 Operating Technology, Healthcare Systems

A specific area of cybersecurity in healthcare infrastructure is represented by Operational Technology (OT), i.e., systems associated with the control of physical processes and operational technologies. In the healthcare environment, these technologies are applied across a wide range of supporting and operational functions that are essential for the continuity of care delivery. In recent years, the healthcare sector has been repeatedly identified as highly exposed to cyber threats, with ransomware and attacks targeting service availability among the dominant threats [4, 33].

Another significant layer of risk in healthcare is represented by the Internet of Medical Things (IoMT), i.e., the ecosystem of network-connected medical devices and related software that transmit and process health data in both clinical and home environments. IoMT expands the organization's attack surface primarily by connecting devices with IT infrastructure (e.g., hospital networks, integration platforms) and often also with external service providers. As a result, cyber incidents may affect not only data confidentiality but also the safety and performance of medical devices. Guidance issued by the Medical Device Coordination Group (MDCG) emphasizes the need for a "secure-by-design" approach and the management of cybersecurity risks throughout the entire lifecycle of a medical device, including the definition of expectations for other stakeholders (e.g., integrators, operators) [37]. The International Medical Device Regulators Forum further frames the cybersecurity of medical devices as a shared responsibility among stakeholders and highlights the need to minimize cyber risks during the intended use of devices while ensuring the continuity of their safety and performance throughout their lifecycle [38].

From a risk perspective, a key trend is the gradual convergence of IT and OT, i.e., the increasing interconnection of operational technologies with enterprise information systems and network services. From a security standpoint, this development is significant as it expands the organization's attack surface and weakens the assumption of the "natural isolation" of OT environments, which has historically been considered a factor reducing risk. In the healthcare context, ENISA points to a systematic increase and sustained occurrence of incidents in the sector and emphasizes the need for targeted measures and support for enhancing the resilience of healthcare entities [33].

For a standardized approach to securing OT/IACS environments, the ISA/IEC 62443 framework is particularly relevant, providing a consensus-based set of requirements and processes for implementing and maintaining cybersecurity in Industrial Automation and Control Systems (IACS). These standards define both programmatic (process-oriented) requirements and technical requirements at the system and component levels and are designed as a comprehensive approach to security in environments where safety and operational reliability are closely interconnected [34, 35].

The regulatory dimension is further strengthened by the NIS2 Directive, which establishes measures aimed at achieving a high common level of cybersecurity across the EU and sets obligations, inter alia, in the areas of cyber risk

management and incident reporting for designated entities. In combination with the prioritization of healthcare as a critical sector in European security policy, this creates a requirement for demonstrable, systematic, and auditable cyber risk management, which in practice applies not only to IT systems but also to relevant components of operational technologies and their interfaces [33, 36].

For these reasons, the security of OT systems in healthcare should be assessed as an integral part of the overall risk management of healthcare infrastructure, taking into account the specific characteristics of operational technologies (in particular, requirements for availability and limited flexibility in change management), while also utilizing established frameworks and recommendations. In this regard, ENISA provides thematic guidance and support for enhancing the cybersecurity resilience of the healthcare sector, while ISA/IEC 62443 offers a structured standardization basis for defining and evaluating security requirements in OT/IACS environments [33, 34].

4. Cyberattacks on Healthcare Systems in the Context of Hybrid Warfare

4.1 Research Approach and Analytical Framework

This article is based on a qualitative research approach grounded in the analysis of open sources (Open Source Intelligence – OSINT) and a comparative analysis of selected incidents in the field of healthcare cybersecurity. OSINT represents a key methodological tool in contemporary security analysis, enabling the systematic use of publicly available information, particularly outputs from international organizations, governmental institutions, academic studies, and sector-specific security reports [39].

Within the research, documents from institutions such as ENISA, the European Commission, and other specialized organizations focused on healthcare cybersecurity were primarily analyzed. These sources provide a structured overview of threat developments, attack typologies, and their impacts on healthcare systems [17]. This approach is complemented by insights from peer-reviewed literature, which emphasizes the sociotechnical nature of vulnerabilities in healthcare, encompassing a combination of technological, organizational, and human factors [17].

The analytical framework also includes a comparative analysis of selected incidents, aimed at identifying recurring patterns of attacks, their impacts on healthcare delivery, and factors influencing the vulnerability of healthcare systems. Particular attention is paid to incidents with a direct impact on clinical operations and those occurring in the context of geopolitical tensions or armed conflicts, especially in relation to the war in Ukraine [22].

The analytical framework integrates perspectives from critical infrastructure protection, cybersecurity, and security studies focused on hybrid conflicts. This multidisciplinary approach makes it possible to understand healthcare not merely as a technological system, but as a strategically significant component of the state's security architecture.

4.2 Contemporary Typology of Cyberattacks on the Healthcare Sector

The analysis of available incidents shows that cyberattacks targeting healthcare institutions exhibit a relatively stable typology, with ransomware operations occupying a dominant position. These attacks primarily target the availability of systems and data, aiming to extort financial payments by disrupting the operations of healthcare facilities [17]. Moreover, ransomware campaigns are increasingly carried out through the ransomware-as-a-service model, which contributes to their greater accessibility and frequency [41].

A second significant category consists of attacks focused on the exfiltration of healthcare data. Healthcare databases contain highly sensitive information with not only economic but also strategic value, making them attractive targets for both criminal and state-sponsored actors [42].

In addition to these categories, there is a growing occurrence of attacks targeting healthcare infrastructure, including hospital networks, diagnostic devices, and systems managing medical technologies. The increasing digitalization and interconnectivity of healthcare devices (IoMT) create new attack vectors that can be exploited not only to obtain data but also to disrupt the provision of healthcare itself [43].

At the same time, the typology of attacks indicates that attackers do not aim solely at data compromise but seek to achieve broader operational effects, particularly the disruption of healthcare service availability and the destabilization of the healthcare system as a whole.

4.3 The Operational Impact of Cyberattacks on the Healthcare Sector

Cyberattacks on healthcare institutions have a direct impact on the provision of medical care, which represents a fundamental difference compared to most other critical infrastructure sectors. Disruptions of information systems often lead to a transition to manual operational modes, delays in diagnostics, and limitations in clinical procedures, thereby disrupting standard healthcare workflows [44].

Empirical studies show that cyber incidents can result in significant reductions in healthcare services, including declines in hospital admissions, surgical procedures, and emergency department visits. At the same time, access to electronic health records, laboratory results, and imaging data may be lost, substantially limiting the ability to deliver standard care [45].

Secondary impacts are also significant. Analyses indicate that an attack on a single healthcare facility may lead to the overloading of neighboring hospitals and disruptions in the availability of care at the regional level. Cyber incidents thus exhibit the characteristics of systemic events, with consequences comparable to other types of crises [46].

In addition to operational impacts, their clinical consequences must also be emphasized. Some studies suggest that cyber incidents may be associated with delays in treatment and, in extreme cases, even increased patient mortality, thereby elevating healthcare cybersecurity to the level of a direct threat to human life [18].

Finally, cyberattacks also have considerable psychological and societal impacts. Disruptions in the functioning of healthcare institutions may undermine public trust in the healthcare system and the state, which, in the context of hybrid conflicts, can potentially be exploited as a tool of destabilization [22].

4.4 Examples of Cyber Incidents in the Healthcare Sector

Concrete incidents provide essential insight into the real functioning of healthcare systems under conditions of cyberattack. The 2017 WannaCry ransomware attack affected the United Kingdom's NHS and led to widespread disruption of healthcare services, including the cancellation of operations and reduced availability of care [19].

Similarly, the ransomware attack on the Irish Health Service Executive (HSE) in 2021 caused a nationwide outage of information systems and a significant reduction in healthcare services at the national level [29]. These cases demonstrate that cyber incidents can take the form of systemic crises with impacts on entire healthcare systems.

Detailed analyses of specific incidents further show that a complete outage of information systems leads to an immediate decline in clinical activities and necessitates a shift to improvised procedures. The restoration of operations is gradual and depends on the prioritization of critical systems, particularly electronic health records and diagnostic modules [45].

The conflict in Ukraine has further demonstrated that healthcare institutions can be targets of both cyber and physical attacks within broader hybrid operations. Documented cases indicate that the objective of such attacks may be not only the disruption of healthcare services but also broader societal destabilization [22].

These experiences confirm that, in the current security environment, healthcare is becoming a strategic target whose disruption can generate disproportionately high impacts compared to other critical infrastructure sectors.

Table 1 shows that cyber incidents in healthcare exhibit a significant degree of structural similarity across different geographical and institutional contexts. The dominant type of attack consists of ransomware operations targeting system availability, which in all analyzed cases led to a direct disruption of healthcare delivery, regardless of the size or organization of the healthcare system [17, 46].

From the perspective of impacts, it is evident that cyber incidents in healthcare cannot be reduced to a technical issue limited to IT infrastructure. Rather, they represent events with immediate clinical and operational consequences, including the postponement of planned procedures, reduced outpatient care, overloading of other healthcare facilities, and the need to switch to manual modes of operation [18, 19, 45]. These findings confirm that the availability of digital systems is an integral component of healthcare provision itself.

Another important finding is the systemic nature of the impacts. Incidents such as the attacks on the UK NHS or the Irish HSE demonstrate that disruption of a single subsystem can lead to widespread effects across the entire healthcare system [18, 19]. Similarly, analyses from the United States confirm that cyber incidents can generate secondary effects, such as overloading of neighboring hospitals and reduced availability of care at the regional level [44, 46].

More recent incidents from 2024 also indicate a significant shift in the nature of cyber threats, particularly towards attacks targeting the healthcare supply chain. The case of the attack on Change Healthcare demonstrates that disruption of an external service provider can have systemic impacts across the entire healthcare ecosystem, including limitations in payment processes and secondary effects on the provision of care. This trend expands the traditional understanding of cyber incidents as isolated events and confirms that the vulnerability of healthcare is increasingly conditioned by its dependence on external IT and service providers [47].

From the perspective of security implications, it is also significant that some incidents exhibit characteristics of strategically motivated activities. Cases from Israel and Ukraine suggest that healthcare systems may be targeted not only by economically motivated attacks but also as part of broader hybrid operations aimed at destabilizing public services and undermining trust in state institutions [22, 29]. In this context, healthcare shifts from the role of a passive victim of cyber incidents to that of an exposed element within the broader security environment.

Across the analyzed cases, similar weaknesses and deficiencies repeatedly emerge. These include, in particular, insufficient access control management, lack of network segmentation, reliance on outdated systems, and limited preparedness for crisis scenarios. A recurring theme is also the critical importance of operational continuity, especially the ability to rapidly restore key systems such as electronic health records, laboratory systems, and imaging infrastructure [18, 45].

Table 1. Selected Cyberattacks in Healthcare

Country	Year	Healthcare Facility	Type of Attack	Affected Area	Main Impact on Operations / Care	Key Recommendations / Implications	Reference
United Kingdom	2017	National Health Service (NHS, multiple facilities)	ransomware (WannaCry)	hospital information systems	cancellation of surgeries, reduced outpatient care, disruption of service availability	network segmentation, patch management, backups, crisis planning	[19]
Ireland	2021	Health Service Executive (HSE, national network)	ransomware (Conti)	national healthcare infrastructure	nationwide IT outage, disruption of care across the country	incident management, prioritized system recovery, strengthening resilience	[29]
Israel	2023	Ziv Medical Center	attempted cyberattack (APT/state-sponsored actor)	hospital infrastructure	security incident without full outage, high risk of operational disruption	protection of hospitals as critical infrastructure, APT detection and prevention	[29]
Israel	2024	(anonymized university hospital in study)	ransomware/ IT shutdown	hospital systems (EHR, lab, imaging)	decrease in surgical procedures, ED visits, shift to manual operations	prioritized recovery of EHR and diagnostic systems, continuity testing	[45]
United States	2016–2022	multiple hospitals (study dataset)	ransomware (repeated incidents)	hospital systems + supply chain dependencies	data breaches, operational disruptions, reduced service availability	third-party risk management, reporting, systematic security measures	[46]
Ukraine	2022	healthcare facilities (multiple cases)	cyberattacks in conflict context	eHealth infrastructure	disruption of digital services, risk of data loss and reduced care	integration of cybersecurity and crisis preparedness	[22]
United States	2024	Change Healthcare (UnitedHealth Group)	ransomware (ALPHV/BlackCat)	health IT services and payment infrastructure (supply chain)	payment system outages, disruption of care across the system, secondary impacts on hospitals	supply chain management, system segmentation, ecosystem-level crisis management	[47]
United Kingdom	2024	Synnovis (NHS laboratory services)	ransomware (Qilin)	laboratory infrastructure	disruption of laboratory diagnostics, postponed procedures, reduced care	supplier protection, redundancy of laboratory services, crisis planning	[48]

The identified patterns of cyber incidents presented in Table 1 can also be confirmed by empirical data from the Czech Republic. The analysis of incidents in the healthcare sector between 2019 and 2021 shows that the dominant initial attack vector was phishing, followed by the deployment of malicious code, particularly in the form of malware campaigns such as Emotet and subsequent ransomware attacks such as Ryuk. A typical example is the incident at the Benešov Hospital, where hospital information systems were extensively taken offline, forcing a transition to manual

operations and resulting in direct damages estimated in the tens of millions of Czech crowns, with total secondary costs being significantly higher. Similarly, other analyzed cases demonstrate that these attacks led to direct operational impacts, including system outages, reduced provision of healthcare services, and, in some cases, financial losses reaching up to hundreds of millions of Czech crowns [32].

These findings confirm the strong dependence of healthcare institutions on digital infrastructure, where the loss of availability of ICT systems immediately limits the ability to provide healthcare services. Czech data thus represent a micro-analytical level that confirms macro-analytical trends identified in the international context, particularly with regard to the dominance of ransomware campaigns, recurring methods of system intrusion, and the systemic nature of impacts on healthcare delivery. At the same time, the academic literature highlights that the high level of digitalization in healthcare, combined with limited system segmentation and low tolerance for outages, makes healthcare institutions structurally vulnerable to cyberattacks, which can have immediate impacts not only on operations but also on patient safety [40].

In summary, it can be concluded that the analyzed cases, summarized in Table 1 and supplemented by data from the Czech environment, do not merely illustrate individual incidents but reveal recurring patterns in both cyber threat behavior and systemic responses within the healthcare sector. These patterns confirm that healthcare cybersecurity must be understood as part of a broader framework of system resilience, encompassing not only technological measures but also organizational preparedness, crisis management, supply chain management, and the ability to operate under conditions of disruption. These findings provide a direct basis for further considerations of the legal and institutional implications discussed in the following chapter.

5. Security and Legal Implications

The increasing number of cyber incidents targeting the healthcare sector raises fundamental questions not only regarding the technical protection of healthcare systems but also concerning the legal and institutional framework for their security. In the context of hybrid threats, the protection of healthcare infrastructure becomes part of the broader national security policy and cannot be perceived merely as an issue of personal data protection or the management of healthcare information systems [17].

One of the key aspects of healthcare security is the protection of health data. Health information belongs to the most sensitive categories of personal data, as it contains detailed information about individuals' health status, diagnoses, treatment, and genetic predispositions. For this reason, its protection within the European legal framework is primarily governed by the General Data Protection Regulation (GDPR), which establishes strict rules for the processing and security of such data [49].

At the same time, it is evident that the protection of health data has, in addition to its privacy dimension, a significant security dimension. In the context of hybrid threats, health data may be used not only for financially motivated crime but also for intelligence gathering, blackmail, coercive operations, or targeted influence on decision-making processes. Particular importance is attached to data concerning individuals whose health status, movement, or operational capability may have strategic relevance for national security or for the conduct of military or security operations [50, 51].

In this context, it is appropriate to consider the category of so-called protected persons, or VIP patients. Following the definition used by Miklas and Kolouch, a protected person for the purposes of this article can be understood as an individual or group of individuals who, based on their legal status, position, or a decision by a competent authority, are provided with an increased level of protection across physical, informational, and cyber domains. This typically includes constitutional officials, publicly exposed persons, members of the armed forces, police, or other security services. Such a definition does not undermine the principle of equal access to healthcare but highlights that, for certain categories of patients, the security implications of data leakage or compromise are significantly more severe than in standard cases [52].

This leads to an important practical conclusion: hospital information systems cannot be designed solely as a universal infrastructure for the "average patient." In a high-risk security environment, healthcare institutions must take into account that certain patient groups may become targets of targeted cyberattacks precisely due to the informational value of their data. In the current global security context, this particularly concerns military personnel, members of security forces, individuals under special state protection, as well as other patients whose medical records may have operational, political, or media significance. For these groups, it is therefore appropriate to implement stricter access control regimes, more granular authorization segmentation, detailed audit trails, enhanced detection of anomalous access, and predefined crisis response procedures in the event of data compromise [51, 52].

It is precisely here that the limitations of a purely compliance-oriented approach become apparent. While the GDPR provides a robust framework for personal data protection, it does not in itself address the varying security significance of different patient categories nor the operational consequences of a cyberattack on a hospital in a crisis or conflict situation [49]. The NIS2 Directive therefore shifts the regulatory focus toward cyber risk management, accountability of organizational leadership, supply chain security, incident reporting, and the continuity of essential services, explicitly including healthcare among the regulated sectors [36]. In the Czech context, this shift has been further reflected in the new Cybersecurity Act, effective from November 1, 2025, which transposes NIS2 into national law and expands cybersecurity management requirements to relevant entities within the healthcare sector [53].

Another important dimension is represented by the European Health Data Space. The regulation on the European Health Data Space, published in 2025 and effective from March 26, 2025, establishes a new framework for access to health data, their sharing, and their secondary use within the European Union [54]. However, this increased level of interoperability and data mobility simultaneously raises the demands placed on the security architecture of the entire ecosystem. For protected persons, this means that protection cannot rely solely on general database security but must also include differentiated access control, the need-to-know principle, segmentation of sensitive cases, and predefined incident response scenarios [52, 54].

From a comparative perspective, a similar shift is observable outside Europe. In the United States, specific Healthcare and Public Health Cybersecurity Performance Goals are being developed, emphasizing the practical preparedness of hospitals, operational resilience, and the ability to respond to attacks affecting healthcare delivery [55]. The Israeli experience, in turn, demonstrates that highly digitalized healthcare systems bring significant operational advantages but also increase the strategic attractiveness of the sector as a target. Official sources from 2025 and 2026 confirm attempts to disrupt hospital operations as well as concerns regarding data breaches [56, 57]. For the European and Czech contexts, this implies that the protection of hospitals must be conceived not only as the protection of infrastructure but also as the protection of sensitive patient categories, for whom a data breach may have immediate security implications.

From this perspective, the healthcare sector becomes not only an object of protection but also an active element of the state's security architecture. The ability to identify and adequately protect high-risk patient groups represents an important component of overall system resilience, which may determine its functionality in crisis situations or during hybrid conflicts.

This reality must also be reflected in the institutional and organizational setup of the healthcare sector. Strengthening cooperation between healthcare institutions, security authorities, and specialized cybersecurity organizations is a necessary prerequisite for an effective response to incidents with potential systemic impacts. Modern cyber threats often have a transnational character, and their mitigation therefore requires a coordinated approach at both national and international levels. Organizations such as ENISA, NATO, and platforms such as Health-ISAC play a key role in this regard by facilitating the sharing of threat information and enhancing sectoral resilience [36].

In addition to legislative and institutional measures, the organizational preparedness of healthcare institutions is also crucial. Hospitals must be capable of responding to cyber incidents not only at the technological level but also through crisis management, staff training, and business continuity planning. Experience from real incidents shows that poorly prepared transitions to degraded modes of operation represent one of the main factors increasing the impact of cyberattacks on healthcare delivery [53].

Ensuring the security of healthcare in the context of hybrid threats therefore requires a comprehensive and integrated approach that combines cybersecurity, legal regulation, crisis management, and institutional cooperation. A key element of this approach is the ability of healthcare systems to maintain functionality even under conditions of disruption, including the protection of specific patient groups whose data may have significant security implications. Only a combination of these measures can contribute to the effective strengthening of the resilience of healthcare systems against current and future threats.

6. Discussion

The findings of this study support the argument that, in the current security environment, healthcare can no longer be understood merely as a passive civilian sector secondarily affected by conflict, but rather as a strategically significant and at the same time highly vulnerable element of critical infrastructure. The combination of high public trust, minimal tolerance for disruptions, intensive digitalization, and the concentration of sensitive data makes healthcare a target whose disruption can generate disproportionately high operational, psychological, and political impacts [4, 39, 42].

The empirical findings presented in Chapter 3, particularly in the context of the conflict in Ukraine and the analyzed cases from Israel, further demonstrate that these impacts are not merely hypothetical but have a real operational character and may form part of broader hybrid strategies.

At the same time, the literature is relatively consistent on one key point: cyber incidents in healthcare cannot be reduced to a purely technical problem limited to IT system management. Systematic reviews and survey studies repeatedly show that vulnerabilities in healthcare organizations are sociotechnical in nature, arising at the intersection of technology, human factors, and organizational structures [39, 42]. This conclusion is also important for the interpretation of the analyzed incidents. If the problem were primarily technical, one would expect its solution to lie mainly in improved software, patch management, or network segmentation. However, available studies suggest that equally important roles are played by governance processes, staff preparedness, the quality of internal communication, and the organization's ability to operate under conditions of disruption [39, 58].

At the same time, it should be noted that part of the literature still tends to overestimate the importance of technical measures at the expense of organizational resilience. While this approach is understandable – since most incidents do indeed originate from the compromise of technical infrastructure – the decisive factor in terms of real impacts on healthcare delivery is the organization's subsequent ability to transition into a degraded mode of operation and maintain critical functions. Case studies of hospital outages show that the loss of access to electronic health records, laboratory modules, or imaging systems does not lead merely to technical inefficiency but to a direct disruption of clinical decision-

making and hospital workflows [58, 59]. This supports the argument that healthcare cybersecurity should be conceptualized more as a component of clinical continuity management rather than solely as a specialized domain of IT governance [44].

Another important issue concerns the relationship between cyber incidents and patient safety. The available literature suggests that cyberattacks can disrupt healthcare delivery, particularly due to system outages and limitations in clinical processes; however, it must also be acknowledged that the extent of these impacts is not uniformly quantified across studies, and empirical evidence of a direct effect on clinical outcomes remains limited in some cases [44, 59]. The literature increasingly includes claims that cyberattacks pose risks to morbidity and mortality, yet the level of empirical support for these claims varies across different types of studies. Commentaries, review articles, and sectoral reports often formulate this relationship in strong terms [4, 42, 44], whereas more robust quantitative evidence is still developing. It is therefore important to distinguish between generally plausible claims and directly demonstrated causal relationships. Nevertheless, more recent studies published in *JAMA* and *JAMA Network Open* already indicate that ransomware attacks are associated with measurable changes in emergency department visits, hospital admissions, regional patient redistribution, and broader technological disruptions in care delivery [44, 59, 60]. Critically speaking, it cannot yet be asserted that every cyberattack automatically leads to worsened clinical outcomes; however, it can be stated with increasing confidence that such attacks raise the likelihood of care disruption in ways that may have clinically significant consequences.

This finding is also crucial for the central argument of the article. If cyberattacks are capable of disrupting healthcare delivery not only within the targeted hospital but also in its surrounding environment, then the healthcare sector represents an attractive target from the perspective of hybrid operations. Studies from the United States indicate that the impacts of such incidents can spill over into nearby hospitals that were not the primary targets of the attack [59, 60]. These spillover effects increase the strategic value of an attack, as they enable broader destabilization with a relatively limited number of direct interventions. In this sense, healthcare differs from many other sectors: an attack on a single institution can trigger a chain reaction within a regional system of care.

Particular attention should be paid to the question of attacker motivation. The prevailing view confirms the dominance of economically motivated ransomware campaigns [4, 46], which could suggest that healthcare is primarily a target of criminal activity rather than hybrid operations. However, such a conclusion would be overly simplistic. Economic motivation does not exclude strategic effects, and evidence from Ukraine and Israel demonstrates that healthcare systems can also be targeted in the context of geopolitical tensions, state-sponsored activities, or broader destabilization strategies [22, 29]. Healthcare should therefore be understood as a sector where economic, intelligence, and strategic motivations may overlap.

This leads directly to the critical issue of healthcare data protection. The traditional European approach is primarily grounded in the framework of privacy and personal data protection. While this approach remains essential, it is no longer sufficient in light of the analyzed incidents. Healthcare data may have clear security relevance for certain groups of patients, particularly members of the armed forces, security services, protected persons, or other individuals with elevated security profiles. This raises an important limitation of current regulatory and organizational practice, which often implicitly assumes that all records require the same level of protection. While this principle of equality is justified from the perspective of the right to healthcare, it may be insufficient from a cybersecurity standpoint. Differentiated access controls, audit mechanisms, and data-handling regimes for high-risk patient groups therefore appear to be a rational extension of the general security framework [61].

Closely related to this is another key finding, namely the distinction between compliance and resilience. Many organizations may formally meet regulatory requirements without being genuinely prepared for prolonged degraded operations. Recent literature on cybersecurity interventions and preparedness in healthcare organizations emphasizes that the mere existence of security policies or technical controls does not guarantee the ability to manage incidents in clinical practice [58, 62]. A critical gap often emerges in the transition from prevention to response and recovery. In other words, a hospital may be "compliant" but not "resilient." This distinction represents one of the most important conclusions of the study. Formal compliance with regulatory requirements does not necessarily imply that a healthcare organization is capable of effectively responding to a cyber incident in real-world operational conditions.

It is important to note, however, that even the current scholarly literature does not offer a fully consolidated model of healthcare resilience in cyberspace. Case studies, review articles, and policy documents predominate; longitudinal studies, standardized comparisons, or robust evaluations of specific measures are less common [39, 58, 62]. This limits the ability to formulate universally applicable recommendations. Nevertheless, at least four relatively consistent conclusions recur in the literature:

- the need for business continuity plans,
- regular testing of degraded modes of operation,
- training of both clinical and non-clinical staff,
- strengthening management of supply chain dependencies [39, 58, 61, 63].

We consider these conclusions sufficiently substantiated for their implementation in practice.

From a broader perspective, the results suggest that in the context of hybrid threats, healthcare is shifting from the role of a "protected civilian sector" to that of a strategic node whose disruption may have a multiplicative effect on security, stability, and public trust in the state. In such conditions, healthcare no longer represents merely a vulnerable sector but rather a strategic target whose disruption can generate systemic impacts extending beyond the healthcare system

itself. This transformation has direct implications for security policy: the protection of hospitals cannot be perceived solely as a matter of healthcare governance, but as an integral component of national resilience. If healthcare systems are expected to function under conditions of geopolitical tension, their cybersecurity must be understood simultaneously as an issue of patient safety, critical infrastructure protection, and crisis management [4, 22, 63].

In summary, the main added value of this study lies in linking three dimensions that are often examined separately in the literature: cybersecurity, the operational reality of hospitals, and the hybrid security context. Their integration demonstrates that the core problem is not merely the possibility of an attack, but the fact that healthcare systems remain insufficiently prepared for its systemic and clinical consequences. This conclusion supports the need for an integrated approach that combines technological measures, legal regulation, and organizational preparedness, while also emphasizing the necessity of understanding healthcare as part of the broader security architecture of the state in the context of hybrid threats.

7. Conclusions

In the context of hybrid threats, healthcare no longer represents merely a vulnerable sector, but a strategic target whose disruption can generate systemic impacts extending beyond the healthcare system itself. The analysis of cyber incidents shows that their consequences are not limited to the technical domain, but directly affect the availability of healthcare services, the continuity of clinical processes, and, in some cases, patient safety.

The findings of this study further confirm that vulnerabilities in healthcare systems are predominantly sociotechnical in nature. Therefore, the key factor is not only the level of technological protection, but also organizational preparedness, the ability to manage crises, and the capacity to operate effectively under conditions of disruption. From this perspective, the ability of healthcare institutions to transition into degraded modes of operation and to prioritize the recovery of critical systems appears essential.

At the same time, current regulatory frameworks – while providing an important foundation for protection – do not fully reflect the differing security relevance of various patient categories or the operational realities of healthcare institutions in crisis situations. Particular attention should therefore be paid to the protection of security-sensitive patient groups, for whom the compromise of health data may have broader security implications.

The results of the study also suggest that cyberattacks on healthcare can take the form of systemic events with regional and national impacts. This aspect reinforces the importance of healthcare as part of critical infrastructure, while also highlighting the need for its deeper integration into national security policy.

From a practical perspective, this implies the need to strengthen the resilience of healthcare systems, particularly through the integration of cybersecurity, crisis management, and business continuity planning. This requires not only the implementation of technical measures, but also systematic staff training, regular testing of crisis scenarios, and effective management of dependencies within supply chains.

From a research perspective, an important open question remains the more precise quantification of the impact of cyber incidents on clinical outcomes, as well as a deeper analysis of the relationship between cybersecurity and patient safety. These areas represent a key direction for future research and for the development of effective security policies.

Acknowledgements. This research was supported by project SGS26/176/OHK5/3T/17.

References

1. **Hoffman F.G.** Hybrid Warfare and Challenges. Joint Force Quarterly, 2009, p. 52:34–39. ISSN 1070-0692. Available online: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-52.pdf [accessed on 20.4.2026].
2. **Galeotti M.** Hybrid War or Gibridnaya Voyna? Getting Russia's Non-Linear Military Challenge Right. NATO Defense College Research Paper No. 111, 2016. Available online: https://www.iir.cz/en/hybrid-war-or-gibridnaya-voina-getting-russia-s-non-linear-military-challenge-right [accessed on 21.4.2026].
3. **European Union.** Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [accessed on 28.4.2026].
4. **Theocharidou M., Lella I. (eds.).** ENISA Threat Landscape – Health Sector. European Union Agency for Cybersecurity, 2023. Available online: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf [accessed on 22.4.2026].
5. **He Y., Aliyu A., Evans M., Luo C.** Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 2021, 23(4), p. e21747. ISSN 1438-8871. Available online: https://doi.org/10.2196/21747 [accessed on 23.4.2026].
6. **European Commission.** European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers. 2025. Available online: https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers [accessed on 28.4.2026].

7. **Barten D.G., Tin D., Granholm F., Rusnak D., Van Osch F., Ciottone G.** Attacks on Ukrainian healthcare facilities during the first year of the full-scale Russian invasion of Ukraine. Conflict and Health, 2023, 17, p. 57. ISSN 1752-1505. Available online: https://doi.org/10.1186/s13031-023-00557-2 [accessed on 24.4.2026].
8. **Wells J.S.G.** Preparing for hybrid warfare and cyberattacks on health services' digital infrastructure: What nurse managers need to know. Journal of Nursing Management, 2022, 30(6), p. 2000–2004. ISSN 1365-2834. Available online: https://doi.org/10.1111/jonm.13633 [accessed on 25.4.2026].
9. **Giannopoulos G., Smith H., Theocharidou M.** The Landscape of Hybrid Threats: A Conceptual Model (Public Version). Publications Office of the European Union / JRC & Hybrid CoE, 2021. Available online: https://www.readkong.com/page/the-landscape-of-hybrid-threats-a-conceptual-model-public-6143305 [accessed on 28.4.2026].
10. **EU-HYBNET.** Hybrid CoE and the European Commission published the Landscape of Hybrid Threats – conceptual model (Actors, Domains, Tools, Phases). Available online: https://euhybnet.eu/hybrid-coe-and-the-european-commission-published-the-landscape-of-hybrid-threats/ [accessed on 28.4.2026].
11. **European Commission (CIPR).** The conceptual framework of Hybrid Threats (JRC + Hybrid CoE): early detection, gaps in preparedness/response, whole of society approach. Available online: https://ec.europa.eu/newsroom/cipr/items/713833/en [accessed on 28.4.2026].
12. **NATO.** Hybrid Warfare: NATO's Response to a Complex Threat Environment. NATO Review. Available online: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [accessed on 26.4.2026].
13. **Council on Foreign Relations.** Cyber Operations in the Russia-Ukraine War. Available online: https://www.cfr.org/articles/tracking-cyber-operations-and-actors-russia-ukraine-war [accessed on 27.4.2026].
14. **ČESKO.** Zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury („o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře). 2025. Available online: https://www.zakonyprolidi.cz/cs/2025-266 [accessed on 28.4.2026].
15. **ENISA.** Threat Landscape 2023. European Union Agency for Cybersecurity. Available online: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf [accessed on 20.4.2026].
16. **NATO.** Baseline Requirements for National Resilience. Available online: https://www.nato.int/cps/en/natohq/topics_132722.htm [accessed on 28.4.2026].
17. **Health-ISAC.** Health Sector Cyber Threat Landscape Report. 2024. Available online: https://health-isac.org/health-isac-2024-annual-report/ [accessed on 21.4.2026].
18. **National Audit Office (UK).** Investigation: WannaCry cyber attack and the NHS. 2017. Available online: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ [accessed on 28.4.2026].
19. **Health Service Executive (Ireland).** Conti Cyber Attack on the HSE. 2021. Available online: https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf [accessed on 22.4.2026].
20. **European Commission.** European Health Data Space (EHDS). Available online: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en [accessed on 28.4.2026].
21. **Boonstra A., Versluis A., Vos J.** Implementing electronic health records in hospitals: a systematic literature review. *BMC Health Services Research*, 2014, 14:370. Available online: https://doi.org/10.1186/1472-6963-14-370 [accessed on 20.4.2026].
22. **Samarasekera U.** Cyber risks to Ukrainian and other health systems. The Lancet Digital Health, 2022. Available online: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00064-4/fulltext [accessed on 28.4.2026].
23. **Center for Strategic and International Studies (CSIS).** Cyber Operations during the Russo-Ukrainian War. 2023. Available online: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war [accessed on 24.4.2026].
24. **Kvartsina K.** Ukraine's Cyber Defense: Lessons in Resilience. German Marshall Fund, 2023 (PDF). Available online: https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf [accessed on 25.4.2026].
25. **Bronk C., Collins G., Wallach D. S.** The Ukrainian Information and Cyber War. The Cyber Defense Review, 2023 (PDF). Available online: https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Fall/CDR_V8N3_Fall_2023_03-Bronk.pdf?ver=U0B1Cl6qzBlZrFPxIjqOEg%3D%3D [accessed on 26.4.2026].
26. **Tkachuk N.** Ukraine as the Frontline of European Cyber Defence. NATO CCDCOE, Tallinn Paper No. 15, 2025 (PDF). Available online: https://ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf [accessed on 27.4.2026].
27. **Attacks on Health Care in Ukraine (joint dataset).** Available online: https://www.attacksonhealthukraine.org/ [accessed on 28.4.2026].
28. **Physicians for Human Rights.** "Brutal Milestone": 2000 Attacks on Ukraine's Hospitals, Clinicians, and Health Infrastructure. 2025. Available online: https://phr.org/news/brutal-milestone-2000-attacks-on-ukraines-hospitals-clinicians-and-health-infrastructure-since-russias-full-scale-invasion/ [accessed on 22.4.2026].
29. **Israel National Cyber Directorate.** Iran and Hezbollah behind an attempted cyber attack on an Israeli hospital (Ziv Hospital). 2023. Available online: https://www.gov.il/en/pages/ziv181223 [accessed on 23.4.2026].

30. **Foundation for Defense of Democracies (FDD).** Iran and Hezbollah Conduct Cyberattack on Israeli Hospital. 2023. Available online: https://www.fdd.org/analysis/2023/12/19/iran-and-hezbollah-conduct-cyberattack-on-israeli-hospital/ [accessed on 21.4.2026].
31. **Ynetnews.** Cyberattacks are surging and the health care system is still vulnerable. 2025. Available online: https://www.ynetnews.com/tech-and-digital/article/s1vcatkzbl [accessed on 20.4.2026].
32. **Kolouch J., Zahradnický T., Kučínský A.** Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. Masaryk University Journal of Law and Technology, 2021, 15(2), p. 301–341. ISSN 1802-5943. Available online: https://journals.muni.cz/mujlt/article/view/14463/12356 [accessed on 30.4.2026].
33. **ENISA.** Health – Cybersecurity of Critical Sectors (Health). European Union Agency for Cybersecurity (web). Available online: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/health [accessed on 28.4.2026].
34. **ISA.** ISA/IEC 62443 Series of Standards. International Society of Automation. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards [accessed on 25.4.2026].
35. **ISAGCA / ISA Secure.** Security of Industrial Automation and Control Systems – An Overview of ISA/IEC 62443 Standards (Quick Start Guide). Available online: https://isasecure.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf [accessed on 26.4.2026].
36. **European Union.** Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L333, 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [accessed on 28.4.2026].
37. **Medical Device Coordination Group (MDCG).** MDCG 2019-16 rev.1: Guidance on Cybersecurity for medical devices (oficiální PDF). Available online: https://health.ec.europa.eu/document/download/b23b362f-8a56-434c-922a-5b3ca4d0a7a1_en [accessed on 27.4.2026].
38. **International Medical Device Regulators Forum (IMDRF).** Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020). Available online: https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity [accessed on 23.4.2026].
39. **Ewoh P., Vartiainen T.** Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. Journal of Medical Internet Research, 2024, 26:e46904. Available online: https://doi.org/10.2196/46904 [accessed on 28.4.2026].
40. **Argaw S.T., Baskaran V., Asplund M., et al.** Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks. BMC Medical Informatics and Decision Making, 2020, 20:146. ISSN 1472-6947. Available online: https://doi.org/10.1186/s12911-020-01161-7 [accessed on 26.4.2026].
41. **Cartwright A.J.** The elephant in the room: cybersecurity in healthcareJournal of Clinical Monitoring and Computing. 2023, 27, p. 1123–1132. Available online: https://doi.org/10.1007/s10877-023-01013-5 [accessed on 20.4.2026].
42. **Wasserman L., Wasserman Y.** Hospital cybersecurity risks and gaps: review. Frontiers in Digital Health. 2022, 4:862221. Available online: https://doi.org/10.3389/fdgth.2022.862221 [accessed on 21.4.2026].
43. **Freyer O., Jahed F., Ostermann M., Rosenzweig C., Werner P., Gilbert S.** Consideration of Cybersecurity Risks in the Benefit-Risk Analysis of Medical Devices: Scoping Review. J Med Internet Res 2024;26:e65528. Available online: https://doi.org/10.2196/65528 [accessed on 22.4.2026].
44. **Dameff C.J., Tully J., Chan T.C., Castillo E.M., Savage S., Maysent P., Hemmen T.M., Clay B.J., Longhurst Ch.A.** Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA Network Open. 2023, 6(5). Available online: https://pubmed.ncbi.nlm.nih.gov/37155166/ [accessed on 23.4.2026].
45. **Abbou B., Kessel B., Ben Natan M., Gabbay-Benziv R., Dahan Shriki D., Ophir A., Goldschmid N., Klein A., Roguin A., Dudkiewicz M.** When all computers shut down: the clinical impact of a cyberattack on a general hospital. Frontiers in Digital Health. 2024, 6:1321485. Available online: https://doi.org/10.3389/fdgth.2024.1321485 [accessed on 24.4.2026].
46. **Cornejo G.M., Lee J., Russell B.** A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Health and Technology. 2024, 14, p.1059–1070. Available online: https://doi.org/10.1007/s12553-024-00890-3 [accessed on 25.4.2026].
47. **Cybersecurity and Infrastructure Security Agency (CISA).** ALPHV BlackCat Ransomware Attack on Change Healthcare (UnitedHealth Group). 2024. Available online: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a [accessed on 26.4.2026].
48. **NHS England.** Cyber incident affecting Synnovis laboratory services. 2024. Available online: https://www.england.nhs.uk/synnovis-cyber-incident/ [accessed on 28.4.2026].
49. **European Union.** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119, 2016, p. 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed on 27.4.2026].
50. **European Commission.** European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers. Brussels: European Commission, 2025. Available online: https://health.ec.europa.eu/publications/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en [accessed on 28.4.2026].

51. **ENISA.** Cybersecurity for VIPs. European Union Agency for Cybersecurity, 2023. Available online: https://www.enisa.europa.eu/publications/cybersecurity-for-vips [accessed on 28.4.2026].
52. **Miklas L., Kolouch J.** Zajištění bezpečnosti chráněných osob a ochrana jejich osobních údajů ve virtuálním prostředí zdravotnického zařízení – část I. DSM – Data Security Management, 2024, 4. ISSN 2336-6745.
53. **ČESKO.** Zákon č. 264/2025 Sb., o kybernetické bezpečnosti. Sbírka zákonů, 2025. Available online: https://www.zakonyprolidi.cz/cs/2025-264 [accessed on 28.4.2026].
54. **European Commission.** Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM 2022) 197 final, 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197 [accessed on 28.4.2026].
55. **U.S. Department of Health and Human Services.** Healthcare and Public Health Sector Cybersecurity Performance Goals. Washington, D.C.: HHS, 2025. Available online: https://www.hhs.gov/sites/default/files/fy2025-performance-plan.pdf [accessed on 20.4.2026].
56. **Israel Ministry of Health.** Digital Health Strategy. Jerusalem: Ministry of Health, Government of Israel. Available online: https://www.health.gov.il/English/Topics/DigitalHealth [accessed on 21.4.2026].
57. **Israel National Cyber Directorate.** Annual Cybersecurity Report 2024. Government of Israel, 2024. Available online: https://www.gov.il/en/departments/israel-national-cyber-directorate [accessed on 22.4.2026].
58. **Hasegawa K., O'Brien N., Prendergast M., Ajah C.A., Neves A.L., Ghafur S.** Cybersecurity Interventions in Health Care Organizations: Systematic Review. Journal of Medical Internet Research. 2024, 26:e47311. Available online: https://www.jmir.org/2024/1/e47311/ [accessed on 23.4.2026].
59. **Abouk R., Powell D.** Ransomware Attacks, ED Visits and Inpatient Admissions in Targeted and Nearby Hospitals. JAMA. 2024, 331(24), p. 2129–2131. Available online: https://doi.org/10.1001/jama.2024.7752 [accessed on 24.4.2026].
60. **Tully J.L., Sumanth Rao S., Straw I., Gabriel R.A., Longhurst Ch.A., Savage S., Voelker G.M., Dameff Ch.J.** Patient Care Technology Disruptions Associated with the Change Healthcare Cyberattack. JAMA Network Open, 2025, 8(7):e2517765. Available online: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2836824 [accessed on 25.4.2026].
61. **Kanter G.P., Rekowski J.R., Kannarkat J.T.** Lessons From the Change Healthcare Ransomware Attack. JAMA Health Forum. 2024, 5(9):e242764. Available online: https://doi.org/10.1001/jamahealthforum.2024.2764 [accessed on 26.4.2026].
62. **O'Brien N., Ghafur S., Sivaramakrishnan A., Durkin M.** Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. Digital Health. 2022, 8. Available online: https://doi.org/10.1177/20552076221104665 [accessed on 27.4.2026].
63. **Kramer D.B.** Promoting the Resilience of Health Care Information Systems. JAMA Health Forum. 2024, 5(11):e243518. Available online: https://jamanetwork.com/journals/jama-health-forum/fullarticle/2827098 [accessed on 28.4.2026].