ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.33**

Resilience of Military Healthcare in Contemporary Armed Conflicts: Process, Data and Cybersecurity Challenges

Zdeněk JÍCHA [1] Jan KOLOUCH [1] Lukáš MIKLAS [1*], Martin ŠANDA [2]

[1] Department of Health Care Disciplines and Population Protection, Faculty of Biomedical Engineering, Czech Technical University in Prague, Nam. Sitna 3105, Kladno, Czech Republic
[2] Institute of System Engineering and Informatics, Faculty of Economics and Administration, University of Pardubice, Studentská 95, 532 10, Pardubice, Czech Republic

*Correspondence: * lukas.miklas@fbmi.cvut.cz*

Abstract

This paper analyzes the resilience of healthcare systems in the context of armed conflicts and hybrid threats, focusing on the role of healthcare data and process management. Based on a mixed-methods approach combining qualitative and quantitative research, it identifies key systemic vulnerabilities, particularly in the areas of data sharing and coordination. The results highlight the need for healthcare organizations to prepare for operations in the event of digital infrastructure disruptions and emphasize the importance of the ability to transition to alternative modes of operation as a key element of resilience.

KEY WORDS: *health system resilience; cybersecurity; data protection; healthcare data; armed conflict; war in Ukraine; military medicine; crisis management*

Citation: Jícha, Z.; Kolouch, J.; Miklas, L.; Šanda, M. Resilience of Military Healthcare in Contemporary Armed Conflicts: Process, Data, and Cybersecurity Challenges. 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.2026.33

1. Introduction

Current armed conflicts are characterized by the growing complexity of the operational environment, in which traditional kinetic operations are increasingly combined with cyber activities, information operations, and other forms of hybrid warfare. These changes fundamentally affect the functioning of healthcare systems, which are a key element in supporting military operations and protecting the civilian population. Healthcare resilience is therefore becoming a significant factor in a state's ability to respond to crises and high-intensity conflicts. In professional literature, resilience is understood as a system's ability to absorb disruptions, adapt to changing conditions, and maintain its key functions even in an environment of long-term uncertainty and multiple threats [1, 6, 7, 8].

Experience from recent armed conflicts, particularly the war in Ukraine, shows that healthcare infrastructure is increasingly becoming a direct or indirect target of military and hybrid operations. Attacks on healthcare facilities, logistics, or information systems can severely disrupt the provision of healthcare and affect not only the health of the population but also the overall stability of society [2]. According to data from the World Health Organization, several thousand attacks on healthcare facilities, medical personnel, and infrastructure have been recorded since the start of the Russian invasion of Ukraine [3]. These incidents confirm that healthcare represents not only a humanitarian but also a strategic dimension of modern conflicts.

In addition to physical attacks, cyberattacks are becoming increasingly significant, as they can disrupt the operations of healthcare facilities by targeting hospital information systems, electronic health records, or communication infrastructure. Cyberattacks on the healthcare sector have significant impacts because modern healthcare systems are heavily reliant on information and communication technologies and the immediate availability of data, not only from diagnostic devices [4]. Failure of these technologies can lead to limited diagnostics, delayed treatment, or the need to switch to improvised manual procedures. These situations demonstrate that disruptions to information systems have a direct impact on clinical decision-making, care coordination, and the continuity of healthcare services [9, 10]. The

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

quality of process management and healthcare data governance plays a significant role in the resilience of healthcare systems. Shortcomings in these areas can lead to a gradual erosion of the system's ability to respond to crisis situations, particularly as a result of fragmented responsibilities, limited coordination, or poor data quality [5, 9, 11]. The aim of this article is to analyze the role of process and data factors in shaping the resilience of military healthcare in contemporary armed conflicts. The focus is on identifying vulnerabilities in the areas of healthcare data management, process organization, and cybersecurity, which can serve as early indicators of a loss of system resilience. The study is based on an interdisciplinary approach combining insights from security studies, healthcare management, and cybersecurity, viewing military healthcare as part of the broader resilience of the state and society in a conflict environment [8, 12].

2. Theoretical Framework for the Resilience of Health Care Systems in Armed Conflicts

The concept of health system resilience has become one of the key analytical frameworks in recent years for assessing the healthcare system's ability to respond to crisis situations. In this context, resilience is typically defined as the ability of a health system to absorb shocks, adapt to changing conditions, and simultaneously maintain the essential functions of healthcare delivery [1]. In a broader theoretical sense, however, resilience cannot be reduced to a mere ability to return to the original state but must be understood as a dynamic property of the system that enables it to function even under conditions of prolonged disruption and uncertainty [6, 8].

A key factor is the ability to manage the interdependence of actors, coordinate decision-making across different levels of the system, and maintain the operational capacity of institutions even when normal functioning is disrupted. In a conflict environment, therefore, it is not only physical resources that prove crucial, but also the institutional structure of the system, particularly the centralization of funding, the capacity for strategic procurement of services, and a functional infrastructure of health information systems [13, 14]. The importance of health system resilience has been clearly demonstrated during recent global crises, including the COVID-19 pandemic and current armed conflicts. Analyses show that systems with high-quality data structures and effective coordination are better able to respond to emergencies and minimize their impacts [15]. Conversely, systems with fragmented data management or insufficient coordination exhibit a higher degree of vulnerability [7, 10].

Review studies focusing on hospital resilience show that a hospital's resilience cannot be assessed solely based on the condition of the building or its technology. It is the result of the interplay between so-called "hard resilience" (infrastructure and technical facilities) and "soft resilience," which encompasses personnel, logistics, communication, and information systems, and the organization's ability to maintain the provision of critical services during a crisis [16, 17]. The resilience of healthcare systems in armed conflict environments represents a specific dimension. In these situations, healthcare operates at the intersection of civilian infrastructure and military operational support, creating specific organizational and security requirements. Military healthcare must be capable of providing care under conditions of limited resources, disrupted infrastructure, and high operational uncertainty, while simultaneously ensuring coordination between military and civilian structures [18].

In this context, it is useful to distinguish between resilience, adaptability, and transformability, which reflect a system's ability to withstand disruptions, adjust its functioning, and, if necessary, fundamentally change its structure [6, 8].

Experience from contemporary conflicts confirms that healthcare systems are exposed to a wide range of threats and attacks that go beyond traditional military operations. In addition to direct attacks on healthcare facilities, indirect forms of disruption are also emerging, such as cyberattacks, disruptions to supply chains, or information operations [19]. From a resilience perspective, it is crucial to note that system failure does not necessarily take the form of a sudden collapse but can arise gradually because of the accumulation of partial disruptions and the exceeding of critical thresholds [7, 11].

In this context, the concept of healthcare resilience is gaining increasing prominence; it encompasses not only material and human resources but also the quality of process management and healthcare data governance [5]. Process fragmentation, limited interoperability, or poor data quality can represent critical points of vulnerability that manifest themselves before technical infrastructure failures [9, 20]. A decline in the resilience of the healthcare system may not manifest as a visible collapse of infrastructure, but can be identified through deteriorating coordination, an increase in improvised procedures, or limited data availability. These manifestations can be understood as early indicators of a decline in systemic resilience [21, 17]. Current research, therefore, focuses on analyzing process and data factors as key determinants of healthcare system resilience. In the context of armed conflict, healthcare resilience is not merely a matter of organizational performance but a component of the broader resilience of the state and society [12].

3. Cybersecurity and Healthcare Data in a War Zone

The digitization of healthcare systems over the past two decades has fundamentally transformed the delivery of healthcare, the management of healthcare organizations, and the coordination of medical operations. Modern hospitals today rely on extensive digital infrastructure, including hospital information systems, electronic health records, diagnostic technologies, logistics systems, and telemedicine platforms. These systems enable more efficient healthcare processes, but at the same time create new security risks that can be exploited in cyber or hybrid operations [22]. As the degree of

digitization increases, not only does the technological complexity of healthcare organizations increase, but also their dependence on the reliable functioning of information and communication systems [23]. The digitization of healthcare processes thus represents not only a technological change but also a key factor influencing the various dimensions of healthcare resilience, particularly in the areas of data flows (including the archiving of healthcare data), process management, and institutional coordination.

From an analytical perspective, the digitization of healthcare creates a specific type of systemic vulnerability that stems not only from the possibility of technical failure but also from disruptions in the links between data, decision-making, and the delivery of healthcare. The healthcare sector is a frequent target of cyberattacks aimed at critical infrastructure, primarily due to the high value of healthcare data, the technological heterogeneity of systems, and the need for continuous operation. An outage of information systems can have immediate impacts on the delivery of care, which increases attackers' motivation to use healthcare as a tool for coercion or destabilization [4]. Disruption of healthcare information systems not only threatens data confidentiality but also directly impacts the continuity of clinical, laboratory, and logistical processes [9]. Of particular significance in this context are ransomware attacks, which in recent years have been the dominant form of cyber incidents in healthcare. These attacks involve encrypting hospital data or blocking information systems to extort a ransom payment [25]. Analyses of cyber incidents show that ransomware attacks can lead to the temporary closure of hospitals, the referral of patients to other healthcare facilities, or restrictions on diagnostic and surgical procedures [24]. A study published in the BMJ journal warns that such incidents can lead to increased patient mortality if there is a significant disruption in healthcare delivery [26]. At the same time, empirical studies of specific incidents show that large-scale cyberattacks can lead to a complete failure of hospital information systems and a shift to manual operating modes, including paper documentation, improvised communication channels, and restrictions on scheduled procedures, which have a direct impact on both the volume and quality of care provided [27].

In addition to "destructive" attacks such as ransomware or "double extortion ransomware," there are other cyberattacks that demonstrate that the weakening of the healthcare system need not take the form of a sudden collapse, but can instead manifest as a gradual degradation of operations, in which limitations on the availability of data and information systems impact diagnostics, clinical decision-making, care coordination, and the organization of healthcare staff's daily work. Experience from similar incidents also confirms that a key component of healthcare organizations' resilience is not only attack prevention but also the existence of functional business continuity plans, alternative workflows, and sufficient local decision-making autonomy during periods of digital system outages [7, 27, 28]. An important part of ensuring cybersecurity in a healthcare facility is also the preparation and testing of a disaster recovery plan.

Furthermore, cyberattacks on the healthcare sector are increasingly taking place within the context of broader geopolitical conflicts. The conflict in Ukraine has shown that cyber operations can be used in parallel with kinetic military operations as part of hybrid strategies. Such attacks on government institutions, energy infrastructure, or healthcare systems can disrupt a state's ability to provide essential services and contribute to the destabilization of society [29]. In the case of healthcare, this is not merely a problem for individual facilities but a disruption of the entire system's functionality [13, 14, 30]. In addition to direct attacks on healthcare organizations, the potential compromise and extraction of healthcare data also pose a significant risk. Electronic health records contain sensitive information about individuals' health status, which may have not only economic value on the black market but also strategic value in the context of intelligence operations. Information regarding the health status of military personnel, members of security forces, critical infrastructure workers, or politicians of a given state could potentially be misused for targeted intelligence operations or psychological influence [31]. From the perspective of healthcare operations, however, it is not only the protection of the confidentiality of this data that is crucial, but also the preservation of its availability, integrity, and timely usability, as a failure of these functions can directly disrupt diagnosis, treatment decisions, and care coordination [23, 27, 32].

International organizations are therefore increasingly emphasizing the importance of cybersecurity in healthcare. The European Union Agency for Cybersecurity (ENISA) notes that the healthcare sector is among the most vulnerable parts of the European Union's critical infrastructure and that the number of cyber incidents targeting healthcare organizations has risen significantly in recent years [33]. Similar conclusions are drawn by analyses from Health-ISAC, which indicate that healthcare organizations are becoming an increasingly frequent target of attacks by organized cybercriminal groups and state-sponsored actors [34].

At the same time, disruptions to information systems have broader organizational impacts, such as impaired coordination among healthcare teams, limited data availability, or the emergence of ad hoc workflows. These factors can gradually weaken the institutional management mechanisms of healthcare organizations [23, 27]. Ensuring the protection of healthcare information systems, data integrity, and the ability to respond to cyber incidents is a key prerequisite for maintaining the functionality of healthcare services in crisis and armed conflict environments [5, 32].

In the context of military healthcare, these issues have even broader significance. Military healthcare information systems may be directly linked to the armed forces' logistics, operational, or evacuation systems, which increases their strategic importance. Disruption of medical data and information flows in military healthcare can slow down triage, evacuation, logistical support, and continuity of care, thereby secondarily weakening the operational capability of the broader military system [13, 30].

4. Process and data vulnerabilities in healthcare systems in armed conflict environments

In the context of current armed conflicts, the functioning of healthcare systems is affected not only by the physical destruction of infrastructure but increasingly also by disruptions to information flows, logistical processes, and the availability of healthcare data. Modern healthcare systems are based on complex digital and organizational processes, the stability of which is essential for the effective delivery of healthcare. If these processes are disrupted, the healthcare system's ability to respond to crises may gradually degrade even before a direct infrastructure failure occurs [1]. It is precisely this form of degradation that poses a key problem in terms of resilience, as the weakening of the system does not manifest itself as a single collapse, but rather as an accumulation of minor failures that gradually reduce the capacity for coordination, decision-making, and continuity of care [7, 21].

From an analytical perspective, these processes can be understood as disruptions in the links between individual components of the healthcare system, particularly between data, organizational processes, and decision-making mechanisms. In line with approaches emphasizing the multilevel nature of resilience, a system's vulnerability is not determined solely by the state of its individual elements, but primarily by the quality of their interactions [10]. Even limited disruptions in one part of the system can thus have disproportionately strong impacts on its overall functioning if they disrupt key communication and coordination links.

Current conflicts demonstrate that healthcare systems are exposed to a combination of kinetic and non-kinetic threats. The conflict in Ukraine represents a striking example of this trend. According to data from the World Health Organization, thousands of attacks on healthcare facilities, medical personnel, and healthcare logistics infrastructure occurred during the war, with the number of attacks on healthcare targets increasing by approximately one-fifth in 2025 alone [35]. These incidents include not only direct shelling or bombing of hospitals, but also disruptions to medical supply chains, blocking of medical transports, and cyberattacks targeting critical national infrastructure [2]. For the analysis of system resilience, it is essential to recognize that vulnerability arises not only at the site of a direct strike but also as a result of disruptions in the links between the healthcare, logistics, and information subsystems.

At the same time, experiences from Ukraine show that healthcare systems are highly vulnerable to disruptions in broader infrastructure, particularly energy and communication systems. Attacks on energy infrastructure have led to widespread power outages in some regions, which have significantly impacted the functioning of hospitals, diagnostic facilities, and digital healthcare systems [36]. In such situations, healthcare institutions are forced to switch to improvised operating modes, such as using paper documentation, informal communication channels, or local decision-making procedures. While these modes may allow care to continue in the short term, they also signal a weakening of the system's procedural stability and an increased reliance on staff experience and ad hoc solutions [27, 28]. In addition to physical attacks, the significance of cyber operations as part of the hybrid strategies of warring parties is also growing. Cyberattacks are capable of disrupting healthcare systems by compromising hospital information systems, manipulating medical data, or attacking healthcare technology supply chains. These activities may be aimed not only at obtaining sensitive data but also at destabilizing healthcare institutions and undermining public confidence in the healthcare system [29]. From an operational perspective, cyber disruptions typically do not occur in isolation but rather exacerbate existing procedural weaknesses in the system, such as limited interoperability, dependence on individual communication nodes, or insufficient preparedness to operate under conditions of limited data availability [23, 32]. Similar trends can also be observed in a broader geopolitical context. For example, in connection with the escalation of tensions between Iran, Israel, and the United States, security analysts point to an increased risk of cyberattacks on healthcare organizations, which can be used as a means of asymmetric action against an adversary's critical infrastructure [37]. In these scenarios, the healthcare sector is considered an attractive target because its disruption can have immediate humanitarian and political consequences. In the context of modern conflicts, healthcare thus becomes not only an object of protection but also a strategic point of pressure, the weakening of which can generate secondary effects in other parts of the security system [30].

At the same time, there has been a significant increase in cyberattacks targeting the healthcare sector, even outside direct conflict zones. According to available statistics, nearly 300 ransomware attacks on hospitals and other healthcare institutions worldwide were recorded in 2025, with hundreds more attacks targeting healthcare technology and service providers [38]. These attacks often lead to the temporary closure of healthcare facilities, the postponement of medical procedures, or the need to switch to manual operations. Experience from these incidents shows that technical system recovery alone is insufficient unless the organization also has functional business continuity plans, backup work procedures, and the ability to maintain decision-making and communication processes under conditions of limited access to digital tools [27, 28].

These experiences suggest that the vulnerability of healthcare systems is not determined solely by their physical infrastructure, but primarily by the quality of organizational processes and healthcare data management. The fragmentation of information systems, insufficient interoperability among healthcare institutions, or poor data quality can significantly impair the ability to coordinate healthcare delivery in crisis situations [22].

Process fragmentation, insufficient interoperability, and low data quality should therefore not be viewed merely as operational shortcomings but as early indicators of weakened system resilience. In a conflict environment, it is precisely these factors that determine whether the system will be able to recognize a change in the situation promptly, share relevant information, and maintain coordinated decision-making across institutions [9, 16, 27].

Process and data weaknesses thus represent one of the first indicators of a gradual loss of systemic resilience in the healthcare system. These indicators include deteriorating quality of healthcare data, an increase in improvised work procedures, limited availability of real-time information, a decline in interoperability, and reduced confidence among healthcare personnel in information systems. These manifestations are analytically significant because they signal a weakening of the system even before a visible technical failure occurs. From a methodological perspective, they thus allow for monitoring the resilience of the healthcare system not only through the state of the infrastructure but also through the quality of process functioning and the organization's ability to work with information under conditions of disruption [9].

Identifying these factors is therefore crucial for the timely recognition of systemic risks and for designing measures aimed at strengthening the resilience of healthcare systems in the context of modern conflicts. In the case of military healthcare, this issue has much broader implications, as procedural and data weaknesses can affect not only the delivery of care itself, but also logistical support, evacuation chains, and the overall operational readiness of the armed forces [30].

5. Empirical Findings: Process and Data Factors Affecting the Resilience of Health Care Systems

The empirical findings presented in this paper are based on research conducted as part of one of the authors' dissertations [39], which focused on the security of protected individuals in healthcare settings and the protection of sensitive healthcare data during hospitalization and data transfer processes. The research combined qualitative and quantitative research methods with the aim of identifying systemic vulnerabilities affecting the resilience of healthcare processes and data protection mechanisms under real-world operational conditions. This approach made it possible to capture not only the technical aspects of information protection but also the operational and organizational contexts that determine the healthcare system's ability to function securely under conditions of heightened disruption.

The qualitative part of the research was conducted in the form of semi-structured interviews with experts in the fields of healthcare, cybersecurity, and physical security. A total of 10 interviews were conducted with respondents holding senior and executive positions (e.g., directors of healthcare facilities, physicians, cybersecurity managers, IT specialists) who had extensive experience in healthcare (approximately 15–50 years) and experience caring for vulnerable individuals. The selection also included respondents with international experience (e.g., Germany, Israel, Slovakia). The analysis showed that the protection of sensitive health information in practice depends not only on technological infrastructure but also on organizational culture, internal procedures, and the level of preparedness of healthcare personnel. The healthcare environment is thus confirmed as a complex socio-technical system in which data security is the result of the interaction between people, technologies, and organizational structures. The quantitative part of the research was conducted in the form of a questionnaire survey among healthcare personnel and persons under protection. A total of 321 healthcare workers from the Czech Republic and 95 respondents from abroad completed the questionnaire, supplemented by 616 persons under protection from the Czech Republic. The total size of the sample reached tens of thousands of respondents in the Czech Republic and abroad. Analysis of the collected data revealed significant differences between formally declared security measures and their actual application in practice, particularly in the area of health data sharing and the organizational safeguards for their protection. The results concerning the sharing of health data between institutions are particularly significant (see Fig. 1).

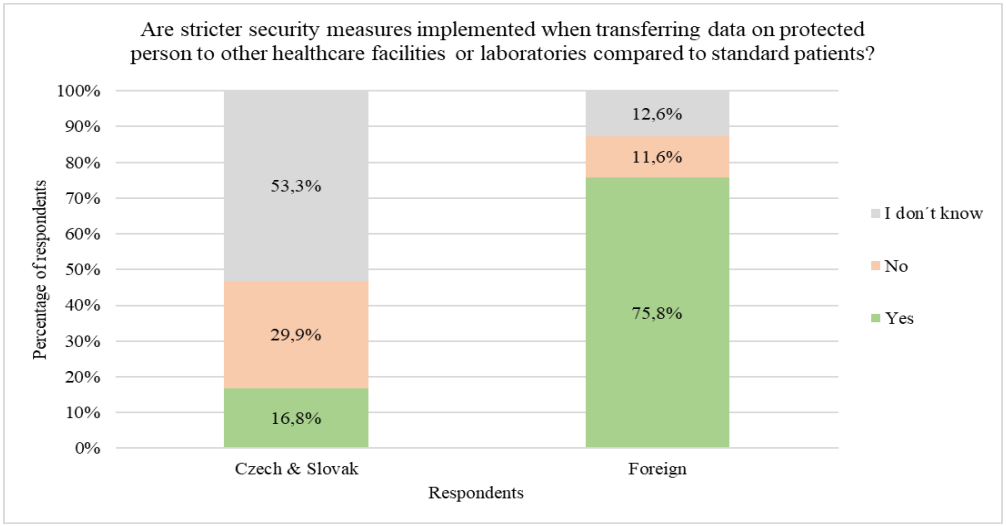

Fig. 1. Security measures for protected persons. [39]

The analysis shows that the implementation of enhanced security measures when transferring data on protected individuals between healthcare facilities or laboratories is not standard practice in the domestic context. Only a small proportion of respondents confirmed the existence of such measures, while a significant proportion stated that such

measures are not implemented or were unsure of their existence. This uncertainty points to insufficiently formalized processes, limited institutional transparency, and poor communication regarding data protection [39].

A comparison with international respondents reveals a markedly different picture. While domestic data are characterized by a high degree of uncertainty among respondents regarding the existence of security measures for data sharing, international respondents—comprising primarily healthcare professionals and senior staff from various geographic regions—significantly more often confirmed their systematic implementation. This difference can be interpreted as a manifestation of a higher degree of process standardization, institutional regulation, and technological readiness in foreign healthcare systems. At the same time, it suggests that the identified weaknesses are not an inherent characteristic of healthcare as such, but rather a consequence of specific institutional, organizational, and procedural arrangements in the given environment [39].

From the perspective of healthcare system resilience, this finding is crucial. Inadequately established or poorly communicated data-sharing procedures represent a critical point of vulnerability, as they undermine the system's ability to effectively share information across institutions, coordinate care, and respond to rapidly changing situations. In crisis or armed conflict environments, these processes are precisely what determine the continuity of healthcare services. These findings are also indirectly confirmed by Fig. 2, which shows the level of awareness among hospitalized protected persons.

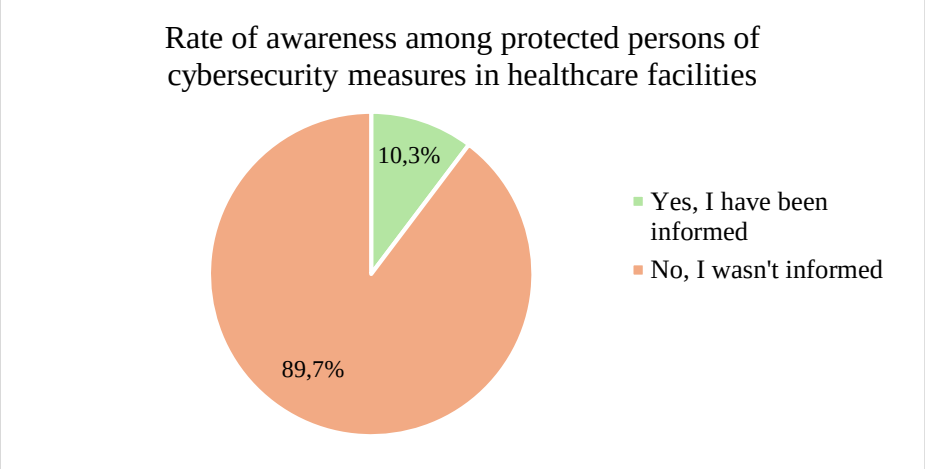

Fig. 2. Rate of awareness among protected persons of cybersecurity measures in healthcare facilities. [39]

The graph above illustrates the level of awareness among respondents with protected person status regarding cybersecurity measures in healthcare facilities. The results show that most respondents (89.7%) reported they had not been informed about these measures, while only 10.3% reported they had been informed. This significant disparity points to a major deficit in the area of patient communication and awareness. A more detailed analysis further shows that even among informed respondents, verbal communication predominated, while written information was represented only marginally. It can therefore be concluded that not only is the overall level of awareness low, but it also lacks systematicity and a standardized form, which may negatively affect patients' ability to respond appropriately in situations where the normal operation of a healthcare facility is disrupted.

Another significant finding concerns the discrepancy between formally defined procedures and their practical application. Respondents repeatedly stated that in real-world operations, improvisation and deviations from standard procedures occur, particularly in situations involving time pressure or heightened safety requirements. While these improvised procedures may temporarily enhance the system's operational capacity, in the long term, they contribute to its destabilization and reduce the predictability of processes [27, 8].

The data obtained further confirms that the management of health data and the control of information flows are among the key factors in the resilience of healthcare systems. Limited availability of relevant information, delays in its delivery, or low quality can significantly complicate clinical decision-making and care coordination, particularly in environments where healthcare organizations are integrated with security or military structures [23, 27, 32].

Empirical findings thus confirm that the resilience of healthcare systems cannot be reduced to the technological robustness of the infrastructure. Rather, it is the result of the interaction of technological, organizational, and human factors. In this context, process fragmentation, limited interoperability, unclear responsibilities, or inadequately managed data sharing represent early indicators of weakened system resilience [17, 21].

These findings support the hypothesis that monitoring processes and data factors can serve as an early warning tool for healthcare system failures, even before any visible technical disruptions occur. From this perspective, the empirical findings represent an important contribution to understanding the mechanisms of healthcare resilience in environments characterized by hybrid threats and armed conflicts.

6. Discussion – The Healthcare Sector as a Target of Hybrid Threats

The findings presented in this study show that the resilience of healthcare systems in the context of current armed conflicts cannot be reduced to technological infrastructure, but is the result of a complex interaction between organizational processes, healthcare data management, and the decision-making mechanisms of healthcare personnel. This conclusion aligns with theoretical approaches that view resilience as a property of complex socio-technical systems, whose functioning depends on the quality of the connections between individual components [6, 7, 10].

Empirical findings also show that the weakening of the healthcare system often does not manifest as a sudden collapse, but rather as a gradual degradation of its operational functioning. Limited data availability, fragmentation of responsibilities, low interoperability, or the emergence of improvised work procedures represent early signs of disruption that may precede visible technical failure. This perspective expands the traditional understanding of resilience—which focuses primarily on the absorption and adaptation to shocks—by adding the dimension of early identification of mechanisms leading to its weakening [17, 21].

At the same time, current armed conflicts confirm that the healthcare sector is becoming not only a target for protection but also a strategic objective of military and hybrid operations. Attacks on healthcare infrastructure, logistics, and information systems have direct impacts on the provision of care and simultaneously generate broader secondary effects in the form of societal destabilization and a weakening of trust in public institutions. In a conflict environment, healthcare thus represents a critical component of a state's security architecture [5, 30].

Cyber threats and attacks that strike at the very core of healthcare organizations' operations take on particular significance in this context. Disruptions to information systems not only lead to data loss but also directly impact clinical decision-making, care coordination, and the organization's ability to maintain safe operations. The concept of resilience, however, emphasizes a system's ability to absorb disruptions, adapt to the situation at hand, and simultaneously maintain its basic functions and structure. Empirical findings, obtained through semi-structured interviews analyzed using the IPA method, confirm that digital system outages lead to a shift to improvised work modes, which, while allowing for short-term maintenance of functionality, simultaneously generate significant operational and organizational complications (e.g., a shift to paper-based documentation, repeated collection of medical history data, prolonged administrative processes, and an increased risk of errors in documentation). In the long term, these modes weaken the stability, transparency, and predictability of the system, and thus its overall resilience to further disruptions [27, 28]. Cybersecurity must therefore be understood as an integral part of the healthcare system's resilience.

The collected data also underscore the role of health data as a key resource for the functioning of the system. In crises, it is not only the protection of data confidentiality that is crucial, but above all, its availability, integrity, and timely usability. Any disruption to these can directly impact the quality of clinical decision-making and the coordination of care across institutions, which allows us to view health data as critical decision-making infrastructure [23, 27, 32].

Another significant finding is the discrepancy between formally established rules and their practical implementation. In real-world operations, deviations from standardized procedures occur, particularly in situations involving time pressure or heightened security requirements. These deviations are most evident in the areas of data sharing and inter-institutional coordination and confirm that procedural improvisation represents not only an adaptive mechanism but also a potential source of systemic vulnerability.

Process and data weaknesses can thus be interpreted as early indicators of a decline in the healthcare system's resilience, allowing us to monitor the system's performance even before any visible failures occur.

Based on these findings, several specific recommendations for practice can be formulated:

1. Standardization and transparency in the sharing of health data among institutions. Empirical data show that data transfer between healthcare facilities represents a critical point of vulnerability. It is therefore essential to implement clearly defined and standardized procedures for sharing sensitive information, including a clear delineation of responsibilities and communication channels, and to ensure that healthcare personnel actually adopt them.
2. Cybersecurity must be viewed as an integral part of clinical and organizational operations. This includes regular staff training, testing of contingency scenarios (e.g., information system outages), and the implementation of effective business continuity plans that enable safe operations even when digital tools are limited.
3. Systematic monitoring of process and data indicators of resilience. Rather than assessing resilience solely based on the state of the infrastructure, it is advisable to monitor indicators such as real-time data availability, the degree of improvisation in work processes, the quality of coordination between institutions, or staff confidence in information systems. These indicators can serve as an early warning tool for system failures.

Healthcare cannot, therefore, be viewed merely as a sector providing medical care, but as an integral part of the state's broader security ecosystem. The ability to maintain continuity of care, work effectively with information, and coordinate activities among institutions is becoming one of the key prerequisites for the overall resilience of society in the context of modern conflicts. These conclusions have direct implications for the practical functioning of healthcare organizations in crisis conditions.

A significant implication of the presented findings is the need for the systematic development of crisis response processes for situations involving disruptions to the digital infrastructure of healthcare facilities. Empirical data and experiences from current conflicts, particularly in Ukraine and Israel, show that healthcare systems must be capable of functioning even under conditions of limited or completely unavailable digital support. Cyberattacks, power outages, or disruptions to communication networks can lead to situations where standard information systems become unavailable, forcing healthcare organizations to switch to alternative operating modes [2, 35, 40].

In this context, it appears that not only the development of crisis scenarios is crucial, but above all, their regular testing and practical drills. Healthcare facilities should have predefined procedures for operating under conditions of limited information system availability, including a clear definition of responsibilities, communication channels, and the prioritization of medical services. However, without systematic training in these procedures, formal plans remain difficult to apply in practice, leading to improvisation and increased operational risk. This conclusion is consistent with findings regarding the functioning of healthcare systems in conflict zones, where processes gradually degrade as a result of cumulative disruptions to infrastructure and information flows [2, 40].

Another key area is reducing the technological vulnerability of healthcare facilities through a combination of digital and non-digital backup solutions. Empirical findings and incident analyses show that complete reliance on digital systems poses a significant risk. Healthcare organizations should therefore have functional recovery plans in place that include not only the restoration of IT infrastructure but also the ability to transition to offline operations. This includes, for example, the availability of basic laboratory and diagnostic capabilities in a limited capacity, the use of analog devices, paper documentation, and alternative means of communication. Of particular importance in this regard is ensuring the continuity of laboratory processes, which are a critical element of clinical decision-making and whose failure can significantly impact the quality of care provided. The growing number of ransomware and other cyberattacks on the healthcare sector confirms that disruptions to digital systems have a direct impact on the delivery of care and the availability of healthcare services [41, 42].

The practical significance of these measures is illustrated by real-world cyber incidents in the healthcare sector. A telling example is the cyber incident at a hospital in Nymburk in 2025 [44], which led to the near-total paralysis of information systems and a switch to emergency mode. The hospital was forced to switch to paper documentation, limit patient admissions, and delegate part of its care to nearby healthcare facilities. The incident also demonstrated that a failure of digital systems can affect not only administrative and information processes but also medical devices and operational logistics themselves. Similar impacts have been observed in other cases of cyberattacks on hospitals, resulting in the postponement of procedures, the rerouting of patients, and the restriction of healthcare facility operations [42, 43].

In a broader context, it is therefore appropriate to consider the ability of healthcare organizations to switch their operations to a so-called crisis mode, which combines digital and physical elements of operations. This mode may include a transition to paper-based documentation, reducing digital dependencies, utilizing local decision-making structures, and simplifying communication mechanisms. The ability to make such a switch does not represent a return to a “less advanced” model of operation, but rather a manifestation of a higher level of systemic resilience that enables the organization to adapt to conditions of disruption. Experience from conflicts and cyber incidents shows that it is precisely this ability to adapt that determines the continuity of healthcare [35, 41].

From this perspective, the resilience of healthcare systems can be understood as the ability to flexibly combine technologically advanced and basic operational modes depending on the current situation. It is precisely this ability to transition between digital and non-digital modes of operation that represents one of the key areas for further research and practical development of healthcare systems in environments characterized by hybrid threats and armed conflicts.

7. Conclusions

The resilience of healthcare systems in the context of current crises and armed conflicts cannot be reduced to technological robustness; rather, it must be understood as the system’s ability to function adaptively even when its key components are disrupted. In this context, the preparedness of healthcare organizations for situations where digital infrastructure is paralyzed as a result of a cyberattack or an information system failure takes on particular significance.

The ability to safely transition to alternative operating modes, including temporarily reducing digital dependencies and utilizing non-digital procedures, represents a key manifestation of systemic resilience. This does not entail a return to a less advanced model of operation, but rather an expansion of the system’s operational flexibility under conditions of disruption.Strengthening this capability through systematic preparation, standardization of crisis procedures, and their regular rehearsal is therefore an essential prerequisite for maintaining the continuity of healthcare and the functionality of healthcare systems in an environment of modern hybrid threats. This approach allows for expanding the understanding of healthcare system resilience from a reactive concept toward proactive management of systemic vulnerabilities.

References

1. **Kruk M.E., Myers M., Varpilah S.T., Dahn B.T.** What is a resilient health system? Lessons from Ebola. The Lancet, 2015, 385(9980), p. 1910–1912. Available online: https://doi.org/10.1016/S0140-6736(15)60755-3 [accessed on 20.4.2026].
2. **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(1), p. 57. Available online: https://doi.org/10.1186/s13031-023-00557-2 [accessed on 21.4.2026].
3. **World Health Organization.** Surveillance of attacks on healthcare in Ukraine. Geneva: WHO, 2024. Available online: https://www.who.int/europe/news/item/05-08-2025-2024-emergency-annual-report--who-s-health-response-in-ukraine [accessed on 22.4.2026].

4. **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. Available online: https://doi.org/10.2196/21747 [accessed on 23.4.2026].
5. **Truppa C., Yaacoub S., Valente M., Celentano G., Ragazzoni L., Saulnier D.** Health systems resilience in fragile and conflict-affected settings: a systematic scoping review. Conflict and Health, 2024, 18, p. 2. Available online: https://doi.org/10.1186/s13031-023-00560-7 [accessed on 24.4.2026].
6. **Walker B., Holling C.S., Carpenter S.R., Kinzig A.** Resilience, adaptability and transformability in social-ecological systems. Ecology and Society, 2004. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000228062200010 [accessed on 25.4.2026].
7. **Folke C.** Resilience: The emergence of a perspective for social-ecological systems analyses. Global Environmental Change, 2006. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000239752200004 [accessed on 26.4.2026].
8. **Folke C., Carpenter S.R., Walker B., Scheffer M., Chapin T., Rockström J.** Resilience Thinking: Integrating Resilience, Adaptability and Transformability. Ecology and Society, 2010. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000285917100034 [accessed on 27.4.2026].
9. **Hosseini S., Barker K., Ramirez-Marquez J.E.** A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 2016. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000365367300006 [accessed on 28.4.2026].
10. **Williams A., Whiteman G., Kennedy S.** Cross-Scale Systemic Resilience: Implications for Organization Studies. Business & Society, 2021. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000603356200005 [accessed on 20.4.2026].
11. **Brand F.S., Jax K.** Focusing the meaning(s) of resilience: resilience as a descriptive concept and a boundary object. Ecology and Society, 2007. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000247904800029 [accessed on 21.4.2026].
12. **Haavik T.K.** Societal resilience – Clarifying the concept and upscaling the scope. Safety Science, 2020. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:000582127200014 [accessed on 22.4.2026].
13. **Blanchet K., Nam S.L., Ramalingam B., Pozo-Martin F.** Governance and capacity to manage resilience of health systems: towards a new conceptual framework. International Journal of Health Policy and Management, 2017, 6(8), p. 431–435. Available online: https://doi.org/10.15171/ijhpm.2017.36 [accessed on 23.4.2026].
14. **Habicht J., Hellowell M., Kutzin J.** Sustaining progress towards universal health coverage amidst a full-scale war: learning from Ukraine. Health Policy and Planning, 2024, 39(7), p. 799–802. Available online: https://doi.org/10.1093/heapol/czae041 [accessed on 24.4.2026].
15. **El-Jardali F., Bou-Karroum L., Fadlallah R.** Emergency preparedness and health system resilience: a comprehensive approach. BMJ Global Health, 2025, 10, p. e016459. Available online: https://doi.org/10.1136/bmjgh-2024-016459 [accessed on 25.4.2026].
16. **Khalil M., Kooli C., Medjelled A., et al.** What is "hospital resilience"? A scoping review on conceptualization, operationalization, and evaluation. Frontiers in Public Health, 2022, 10, p. 1009400. Available online: https://doi.org/10.3389/fpubh.2022.1009400 [accessed on 26.4.2026].
17. **Fallah-Aliabadi S., Ostadtaghizadeh A., Ardalan A., Fatemi F., Khazai B., Mirjalili M.R.** Towards developing a model for the evaluation of hospital disaster resilience: a systematic review. BMC Health Services Research, 2020, 20(1), p. 64. Available online: https://doi.org/10.1186/s12913-020-4939-2 [accessed on 27.4.2026].
18. **NATO.** Allied Joint Doctrine for Medical Support (AJP-4.10). Brussels: NATO Standardization Office, 2019. Available online: https://www.coemed.org/files/stanags/01_AJP/AJP-4.10_EDC_V1_E_2228.pdf [accessed on 28.4.2026].
19. **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. Available online: https://doi.org/10.1111/jonm.13633 [accessed on 20.4.2026].
20. **Naderpajouh N., Matinheikki J., et al.** Resilience science: Theoretical and methodological considerations. International Journal of Project Management, 2023. Available online: https://www.webofscience.com/wos/woscc/full-record/WOS:001112361600001 [accessed on 21.4.2026].
21. **Biddle L., Wahedi K., Bozorgmehr K.** Health system resilience: a literature review of empirical research. Health Policy and Planning, 2020, 35(8), p. 1084–1109. Available online: https://doi.org/10.1093/heapol/czaa032 [accessed on 22.4.2026].
22. **Boonstra A., Versluis A., Vos J.** Implementing electronic health records in hospitals: a systematic literature review. BMC Health Services Research, 2014, 14, p. 370. Available online: https://doi.org/10.1186/1472-6963-14-370 [accessed on 23.4.2026].
23. **Argaw S.T., Troncoso-Pastoriza J.R., Lacey D., et al.** Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 2020, 20(1), p. 146. Available online: https://doi.org/10.1186/s12911-020-01161-7 [accessed on 24.4.2026].
24. **Martin G., Martin P., Hankin C., Darzi A., Kinross J.** Cybersecurity and healthcare: how safe are we? BMJ, 2017. Available online: https://doi.org/10.1136/bmj.j3179 [accessed on 25.4.2026].

25. **Kolouch J., Zahradnický T., Kučínský A.** Ransomware Attacks on Czech Hospitals at the Beginning of Covid-19 Crisis. In: Tušer I., Hošková-Mayerová Š., eds. Trends and Future Directions in Security and Emergency Management. Cham: Springer, 2022, p. 303–316. Available online: https://doi.org/10.1007/978-3-030-88907-4_18 [accessed on 26.4.2026].
26. **Ghafur S., Kristensen S., Honeyford K., Martin G., Darzi A., Aylin P.** A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digital Medicine, 2019, 2, p. 98. Available online: https://doi.org/10.1038/s41746-019-0161-6 [accessed on 27.4.2026].
27. **Abbou B., Hagens S., Van de Velde A., et al.** When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Frontiers in Digital Health, 2024, 6, p. 1317753. Available online: https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2024.1321485/full [accessed on 28.4.2026].
28. **Moore G., Connolly S., Mullen A., et al.** A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Services Research, 2023, 23(1), p. 1103. Available online: https://doi.org/10.1186/s12913-023-10165-8 [accessed on 20.4.2026].
29. **CyberPeace Institute.** Cyberattacks during the Russian invasion of Ukraine. Available online: https://cyberconflicts.cyberpeaceinstitute.org/ [accessed on 21.4.2026].
30. **Bozorgmehr K., McKee M., Rast E., Kazatchkine M., Zoidze A., Berdzuli N.** Health system response to war and displacement in Europe requires transformative actions and policies. The Lancet Regional Health – Europe, 2024, 47, p. 101122. Available online: https://doi.org/10.1016/j.lanepe.2024.101122 [accessed on 22.4.2026].
31. **ENISA.** Threat Landscape for the Health Sector. Available online: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf [accessed on 23.4.2026].
32. **Wasserman L., Wasserman Y.** Hospital cybersecurity risks and gaps: review. Frontiers in Digital Health, 2022, 4, p. 862221. Available online: https://doi.org/10.3389/fdgth.2022.862221 [accessed on 24.4.2026].
33. **European Union Agency for Cybersecurity (ENISA).** Cybersecurity of Critical Sectors: Health. Available online: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/health [accessed on 25.4.2026].
34. **Health-ISAC.** Health Sector Cyber Threat Landscape Report. Available online: https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf [accessed on 26.4.2026].
35. **World Health Organization.** Attacks on Ukraine's health care increased by 20% in 2025. Available online: https://www.who.int/news/item/23-02-2026-attacks-on-ukraine-s-health-care-increased-by-20-in-2025 [accessed on 27.4.2026].
36. **Physicians for Human Rights.** Health Care in the Dark: The Impacts of Russian Attacks on Energy in Ukraine. Available online: https://phr.org/our-work/resources/health-care-in-the-dark-attacks-on-energy-in-ukraine/ [accessed on 28.4.2026].
37. **Healthcare IT News.** Iran war prompts hospitals to prepare for cyberattacks. Available online: https://www.healthcareitnews.com/news/iran-war-prompts-us-hospitals-prep-potential-ddos-attacks [accessed on 20.4.2026].
38. **Comparitech / Industrial Cyber.** Healthcare ransomware attacks surge in 2025. Available online: https://industrialcyber.co/reports/healthcare-ransomware-attacks-surge-30-in-2025-as-cybercriminals-shift-focus-to-vendors-and-service-partners/ [accessed on 21.4.2026].
39. **Miklas L.** Bezpečnost hospitalizovaných chráněných osob. Disertační práce. České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství, 2024. Available online: https://www.fbmi.cvut.cz/sites/default/files/2024-11/Diserta%C4%8Dn%C3%AD%20pr%C3%A1ce-PhDrMiklas.pdf [accessed on 22.4.2026].
40. **Poole D.N., et al.** The effect of conflict on damage to medical facilities in Ukraine. PLOS Global Public Health, 2025. Available online: https://doi.org/10.1371/journal.pgph.0003950 [accessed on 23.4.2026].
41. **European Policy Centre.** From ransomware to statecraft: Protecting EU healthcare in the new threat landscape. Available online: https://www.epc.eu/publication/from-ransomware-to-statecraft-protecting-eu-healthcare-in-the-new-threat-landscape/ [accessed on 24.4.2026].
42. **Health-ISAC / Industrial Cyber.** Health Sector Cyber Threat Landscape Report. Available online: https://industrialcyber.co/reports/health-isacs-2025-health-sector-cyber-threat-landscape-report-warns-of-rising-ransomware-espionage-iomt-vulnerabilities/ [accessed on 25.4.2026].
43. **Ghafur S., Grass E., Jennings N.R., Darzi A.** The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health, 2019, 1(1), p. e10–e12. Available online: https://pubmed.ncbi.nlm.nih.gov/33323235/ [accessed on 26.4.2026].
44. **Vaníčková K.** Totální blackout, nefungoval ani zvonek. Hackeři nymburskou nemocnici paralyzovali. iDNES.cz, 2025. Available online: https://www.idnes.cz/zpravy/domaci/kyberutok-a-pak-blackout-ochromena-nemocnice-musela-pacienta-prevezt-jinam.A250702_101842_domaci_vank [accessed on 27.4.2026].