SWP

SWP Comment

NO. 35 AUGUST 2026

Cybersecurity in the Healthcare Sector

An Integrated Approach to National, European and Global Resilience

Michael Bayerlein, Annegret Bendiek, Jonas Hemmelskamp and Maik von der Forst

The healthcare sector worldwide is facing an increasing threat from cyberattacks. Between 2022 and 2025, the European Repository of Cyber Incidents (EuRepoC) recorded a total of 351 significant attacks on healthcare facilities. These data provide initial insights into the impact of cyberattacks on healthcare systems and sectors, and the crisis management that follows. They also highlight that such attacks pose a threat to public health and national security. The data analysis shows that national critical sectors and the European and international levels must be interlinked. The National Security Council could do so by developing an integrated national and international situational assessments based on interdisciplinary analyses. Only such an approach can systematically identify threats, derive effective measures from them and comprehensively protect the healthcare sector.

The ongoing digitalisation of medical infrastructure and its supply chains increases the efficiency and quality of healthcare provision on the one hand, but also substantially expands the attack surface on the other. Cyberattacks on the healthcare sector not only endanger national security but also have the potential to disrupt medical service delivery worldwide.

In recent years, cyberattacks targeting the healthcare sector, including hospitals and other healthcare organisations, have become a serious challenge for national security and societies across the globe. According to the EuRepoC open-source securitydatabase, the healthcare sector is one of the most severely affected sectors, with 351 significant cyberattacks recorded worldwide between 2022 and 2025 alone.

In the healthcare sector, cyberattacks take the form of ransomware attacks, data theft or targeted disruption of hospital IT systems. In the worst case, these attacks can significantly disrupt patient care. Their consequences are potentially life-threatening, as treatment processes may be interrupted, diagnoses delayed or medical equipment rendered inoperable. Furthermore, attacks on healthcare data, such as electronic health records, undermine public confidence in state institutions.

The cyberattack on the medical billing service provider Unimed in May 2026 — during which data relating to more than 100,000 privately insured patients at German university hospitals were stolen — is a striking example. The cyberattack targeting the US medical device manufacturer

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Stryker in mid-March 2026 demonstrated how the boundaries between national, European and international policies, as well as between different policy areas, are increasingly becoming blurred: A global network outage paralysed the company's operations worldwide. The attack temporarily disrupted the supply of surgical consumables and personalised implants, forcing the postponement of operations across the globe. In Cork, Ireland, alone, more than 4,000 employees were temporarily unable to carry out their work. The Iranian hacker group Handala claimed responsibility for this "wiper" attack, which deleted the company's data. According to the group, the attack was intended as a retaliation for a missile strike on 28 February 2026, in which an Iranian school was hit and at least 175 people were killed. This example illustrates how quickly individual cyber incidents can take on international dimensions and become linked to offline conflicts.

Despite efforts to build resilience across societies, the healthcare sector lacks two key elements across all policy levels: first, the systematic involvement of international actors in exchanging information; and second, a mechanism of coordination to enable this. In other words, it is not enough merely to report cyber security incidents and record them in a situational assessment. Instead, there is a need for structured monitoring of the impacts of cyberattacks on the healthcare sector on the international level.

Only then can the information necessary for national and local crisis management in hospitals be made available. Consequently, focusing exclusively on national security — and thus on national and intra-EU structures and competences — falls short, as it neglects global synergies that are essential for effective health-crisis management.

European and national policy initiatives

In recent years, both the EU and the German federal government have placed the protection of critical infrastructure at the centre of many initiatives. In Germany, the Federal Office for Information Security (BSI) plays a central role in protecting the national healthcare system against cyber threats. In view of advancing digitalisation and a rising number of attacks on hospitals, medical practices and care facilities, the BSI offers comprehensive support, standards and recommendations for action. The BSI has called on healthcare organisations in Germany to strengthen their security measures and backup systems. In doing so, it works closely with the European Union Agency for Cybersecurity (ENISA) and collects reports of serious cyber incidents. Operators of critical infrastructure are obliged to report such incidents under the second EU Network and Information Security (NIS-2) Directive. Where this occurs, it may be possible to attribute responsibility and initiate criminal proceedings or even diplomatic responses against the attackers.

At the EU level, the Critical Entities Resilience (CER) Directive and the NIS-2 Directive, together with the corresponding national implementing legislation — Germany's KRITIS Framework Act and the National IT Security Act — aim to enhance the resilience of critical infrastructure, including the healthcare sector. CER and NIS-2 adopt an all-hazards approach. Whereas CER addresses physical and digital threats, NIS-2 focuses on cybersecurity and extends reporting obligations for, among others, healthcare facilities to ward off cyberattacks. In addition, the EU Preparedness Union Strategy has been implemented, with the aim of promoting a holistic approach to crisis preparedness. This strategy encompasses early detection, prevention of and response to threats such as cyberattacks and pandemics. The EU Action Plan on Cybersecurity in Healthcare envisages measures such as the establishment of an EU-wide support centre for hospitals and "response playbooks".

To counter cybersecurity risks in the healthcare sector more effectively at the national level, and to better prepare Germany's healthcare system for war and disasters, the former German Minister of Health Nina Warken has announced a

dedicated Healthcare Security Act. It is intended to complement the cross-sectoral KRITIS legislation mentioned above. Key aspects of the planned act are to strengthen the resilience of the healthcare sector comprehensively and to promote closer cooperation with security authorities and the Bundeswehr. The National Security Strategy and the Total Defence Action Plan also aim at interlinking societal resilience and civil-military cooperation. However, it is not clear how this can be implemented in concrete terms across the healthcare sector and at various policy levels. Building resilience and enhancing preparedness are key challenges, as is evident from the debate on reforming the National Security Strategy.

Considerations regarding the protection of critical healthcare infrastructure are already conceptually being framed in conjunction with enhanced civil-military cooperation. Johannes Backus, Major General (Medical Corps) and Commander of the Bundeswehr Health Care Command, understands resilience as the interaction of all relevant operational, administrative and supply stakeholders, as well as coordination between the state and the population. However, the implementation of these considerations in practice often fails due to departmental boundaries and the lack of top-down coordination by the National Security Council.

While national measures within the envisaged framework of comprehensive defence are important, European and international cooperation in protecting critical healthcare infrastructure is often overlooked. Cyber threats, however, are not constrained by national borders and can only be effectively countered through cross-border and cross-agency coordination involving European and international partners. Although the EU Preparedness Union Strategy must be implemented at the national level, the European and international dimensions should be factored into national-level approaches to the healthcare sector, for example through the systematic exchange of information.

Data status based on EuRepoC

Cyberattacks on the healthcare sector are not only a threat to national security but, first and foremost, to (global) public health. An analysis of 351 significant cyberattacks targeting the healthcare sector between 2022 and 2025 reveals a nuanced picture: The attacks can be classified into six categories, or clusters (C0—C5), based on their intensity, attack pattern, attribution and political responses. These differ significantly in their operational consequences for the functioning of the affected healthcare facility or facilities, at both the national and international levels.

Categories C2 and C5, which together account for 174 cases and are therefore the most frequent, aim at data theft. Whereas the motivation for C5 attacks is usually unknown, C2 attacks are carried out by criminally motivated actors who use ransomware to encrypt data and subsequently extort the targeted organisation. Despite their frequency, these incidents have little impact on operational care processes.

In contrast, the 137 attacks in categories C0, C1 and C4 have disruptive effects and cause medium- to long-term outages of operational systems, ranging from a few days (45 cases) to weeks (92 cases). These operational disruptions tend to last longer in the healthcare sector than in other sectors. Attacks in category C0 lead to long-term system outages without resulting in public attribution of the attacker. Incidents in categories C1 and C4 again involve the use of ransomware, which results in extortion (C1) or triggers a long-term disruption (C4). The 40 attacks in category C3 can be described as low-intensity espionage, with only a few attributable to a state actor.

It is interesting to note that even attacks by ransomware groups in the healthcare sector are aimed less at encryption than at the exfiltration of patient data (82 cases), and in some instances, solely at the latter. These personal data are often more sensitive than data stolen from other sectors and lend themselves particularly well to blackmailing healthcare organisations by threat-

ening their publication. The ransomware model usually involves double extortion, meaning that the perpetrators steal data and encrypt the systems to extort payment twice — in exchange for non-disclosure of the data and for decryption. If the ransom is not paid, the data are usually published.

Although the authorities frequently launch investigations in such cases, in the majority of disruptive incidents there is neither attribution of responsibility nor any political or further legal consequences. This is problematic given the impact that these attacks can have, not only on information systems but also on public health. Considering this evidence, it is insufficient to view ransomware groups solely as a security threat: Disruptive attacks on healthcare facilities that affect their operational processes systematically undermine public health.

A micro-level perspective

The six categories of attack outlined above permit indirect inferences about the on-the-ground impacts of cyberattacks. First, targets of attacks in the healthcare sector are highly diverse, ranging from hospitals, medical practices, pharmacies and medical-device manufacturers to insurance companies, emergency medical services, pharmaceutical companies and non-governmental organisations. Depending on the organisation affected, the method and route of attack (the so-called attack vector), and the scale of the attack (including the number and type of systems and facilities affected), the implications for public health can vary considerably. The criticality of a healthcare facility can be assessed through its size, care mandate, location, specialisation and the availability or absence of alternatives.

In the following, the identified cyberattack clusters (C0 — C5) are ranked in ascending order of their impact on healthcare provision:

1. Data theft/encryption (e.g. patient data, insurance numbers or bank details)
2. Disruption to IT services (e.g. website, appointment portals or communications)
3. Disruptions to operational systems and services (e.g. hospital information systems, sterilisation services, radiology or laboratory systems, blood banks).

Together with information about the affected facility or facilities and the temporal dimension, it is possible to assess the specific impacts on healthcare provision. EuRepoC data show that cyberattacks impacting diagnostic processes (e.g. laboratories or radiology) or operational processes (e.g. sterilisation, patient admissions or documentation) have serious consequences for healthcare provision. One example is the cyberattack on the Luigi Vanvitelli University Hospital in Italy in 2023, where the resulting shift to manual processes led to noticeable capacity constraints (C4).

By contrast, attacks aimed solely at stealing patient data are often associated with a loss of information or trust. In 2025, for example, sensitive data were stolen from the UK healthcare provider HCRG Care Group and partly published on the dark web (C2). In 2023, the data of more than one million patients were stolen from the medical device manufacturer Zoll (C1). Even though attacks aimed at data theft theoretically have no direct impact on the delivery of healthcare, they can also disrupt it indirectly if protective measures require systems to be disconnected from the network or certain services to be shut down. This occurred in 2025 at SimonMed, which employs 200 radiologists across 170 sites in 11 US states (C2).

Well-known criminal threat actors, such as BianLian, Medusa, BlackCat and LockBit, which openly claim responsibility, often do so in connection with ransomware attacks to extort the affected organisations. In 2023, for example, the service provider TransForm Shared Service Organization was attacked by the DAIXIN team, which indirectly affected patient care and appointment scheduling at five hospitals in the Canadian province of Ontario (C1). In 2024, the Swiss pharmaceutical company Octapharma was forced to temporarily close more than 150 plasma donation centres in the United States following an attack by the BlackSuit group (C2).

Although some attackers such as LockBit claim that they would not target the healthcare sector, the data paint a different picture. In addition to hospitals, the most frequent targets are larger medical practices and service providers such as insurance companies and medical-device companies. Even non-governmental organisations are targeted, as the case of Omni Family Health (C1) demonstrates.

Hospitals can sometimes respond quite quickly to disruptive attacks by implementing analogue contingency procedures, as examples from 2024 at Lindenbrunn Hospital in Coppenbrügge (C4) and from 2025 at Stell Hospital in France (C4) demonstrate. At the same time, these measures also entail restrictions, meaning that appointments or scheduled procedures may have to be postponed during an attack, as occurred following an attack on the hospitals in Lippstadt, Erwitte and Geseke in 2024 (C4). Whether these were purely precautionary measures cannot be determined from publicly available reports. However, when three hospitals operated by the Katholische Hospitalvereinigung Ostwestfalen gGmbH were forced to suspend emergency care services (C4) on Christmas Eve 2023, and when operations were postponed at the Wertachkliniken in Bobingen and Schwabmünchen (C4) in 2024, these actions were taken as a precaution. One thing is clear: Greater transparency regarding the threat situation enables more closely coordinated crisis and emergency management.

Additionally, when hospitals are taken out of emergency care provision because of a cyberattack, ambulances may have to be diverted. This occurred in 2023 after an attack on the US company Ardent, which operates more than 30 hospitals and had to temporarily suspend services for 10 emergency rooms (C4), and in 2024, when two hospitals in Milan were no longer served by ambulances (C4). In rural areas, such cases can entail significantly longer transport times, which can result in harm to patients.

Attacks that affect central systems within a hospital network or a healthcare group are particularly serious. The resulting cascading effects can compromise the systems of multiple institutions at once. One example is the attack on the Hipocrate Information System in Romania in 2024, which resulted in 25 hospitals switching to analogue methods and a further 75 facilities disconnecting from the platform as a precautionary measure (C4). Disruption affecting suppliers, emergency medical services or pharmacies can also have a significant impact on healthcare provision. This is illustrated by the outage of an emergency dispatch centre in Bolzano in 2025 (C0) and two Russian pharmacy chains that temporarily closed around 1,000 branches in 2025 (C0).

Such vulnerabilities are likely to increase in the future. In Germany, this is partly because the shift towards centre-based healthcare, including under the Hospital Care Improvement Act, entails the centralisation of information systems. Furthermore, restoring systems after a cyberattack is likely to result in longer-term restrictions on service provision. This, in turn, places an additional burden on alternative local healthcare providers. Such service restrictions caused by cyberattacks would have serious consequences in a so-called twin threat scenario, for example during a military conflict or an extreme-weather event such as a heatwave.

The clustering of the EuRepoC data and the outlined consequences of cyberattacks on healthcare provision make one point clear: Even where attack patterns are similar, attacks can have differing disruptive impacts. Overall, attacks classified in C3 and C5 have less severe impacts on healthcare provision than those classified in C0, C1 and C4, while attacks in C2 fall somewhere in between. However, attacks within a given cluster can also vary considerably, which means that each case must be assessed individually.

The potential role of WHO at the macro level

The cyberattack clusters and consequences identified at the micro level regularly have an international dimension. The attack on

Stryker simultaneously halted production sites in Cork, Tuttlingen and Mühlheim; the incident at Octapharma forced the temporary closure of more than 150 plasma donation centres; and the outage of the Hipocrate Information System affected more than 100 healthcare facilities. Cyberattacks on the healthcare sector and supply chain thus have impacts that cross national and sectoral boundaries. Systematic monitoring of these cross-border impacts and ripple effects require an institution with a global perspective and clinical expertise that can assess, in an integrated manner, the consequences of cyberattacks for healthcare provision.

The World Health Organization (WHO) is the central body responsible for coordinating global health efforts and assessing health risks. Through its Surveillance System for Attacks on Health Care (SSA), it already has an institutionally suitable model, although its current mandate is limited to kinetic (physical) attacks in humanitarian emergencies. Extending the SSA's mandate to the cyber domain would close a critical gap, as existing security-focused registries are unable to capture the specific and sometimes cross-border impacts of cyberattacks on healthcare provision; they lack the necessary specialist expertise. EuRepoC provides reliable information on attack vectors, attribution and technical intensity, but does not provide details about the impacts on healthcare provision. The Emergency Events Database (EM-DAT) and the Global Terrorism Database (GTD) do not capture digital forms of attack or the sector-specific criticality of healthcare facilities.

Since 2017, WHO's SSA has also recorded attacks that result in an obstruction to healthcare delivery. To date, however, it has been limited to kinetic attacks and to those occurring in "complex humanitarian emergencies". The crisis register of the German Working Group on Hospital Contingency Planning (DAKEP) alone covers exceptional situations, including IT incidents in hospitals. However, it only covers Germany, Austria, Switzerland and Luxembourg; moreover, incidents are reported by the institutions themselves and, in most cases, only retrospectively.

Unless cyberattacks and their consequences for healthcare are systematically recorded and assessed, patterns of impact will remain anecdotal, and the development of protection standards will continue to lack systematic evidence. Furthermore, the political accountability of states from whose territory cyberattacks originate (i.e. those that direct or at least tolerate threat actors) remains limited. Recording and publicly identifying attacks globally, and assessing their consequences for healthcare provision, is therefore not merely an analytical necessity but also a necessity for health and security policy.

WHO could bridge this existing gap, as it combines health expertise with global reach. Assessing the impact of cyberattacks on the healthcare sector from a comprehensive global perspective is particularly relevant, as concentration risks, cascading effects and twin threats identified at the micro level have cross-border implications. Through its network of regional offices, WHO has the reach required by this transnational logic of impact. Its work to protect healthcare facilities also gives it the legitimacy that is essential to a cyber-monitoring mandate. The fact that WHO now explicitly classifies cyberattacks on critical health infrastructure as attacks on health facilities underscores this reasoning.

With the SSA, WHO has an established platform for precisely this task of monitoring the impacts of cyberattacks on healthcare systems. The SSA serves three closely linked purposes: It raises global awareness about targeted attacks on healthcare provision; it provides a database for evidence-based prevention and protection standards; and it promotes accountability by identifying and documenting attacks on healthcare facilities as such. These three functions are as relevant to cyberattacks as they are to kinetic attacks and are vital beyond the existence of an armed conflict.

World Health Assembly resolution WHA 65.20, which sets out the SSA's mandate, employs a broad definition of attack, refer-

ring simply to "attacks". Under international humanitarian law, attacks on health infrastructure generally also include digital attacks: a cyberattack that renders a hospital inoperable is not fundamentally different in its effects from a physical attack. The necessary conceptual basis is therefore established. The mandate itself, however, remains limited to attacks in complex humanitarian emergencies. Expanding the SSA to include a cyber module that is not subject to this condition would be the logical next step towards closing the identified gap.

Recommendations for action

Cyberattacks on healthcare infrastructure pose a systemic threat to public health and national security. They are disruptive, and the data stolen are sensitive. The Stryker, Octapharma and Hipocrate cases demonstrate that their impacts propagate along complex supply chains. Cyber risks to public health should be viewed from the same perspective as systemic risks in the financial sector.

In view of the threat situation in the healthcare sector, the German federal government should address cybersecurity within the National Security Council. The Council could establish a central coordination unit staffed by representatives from the 18 critical infrastructures sectors, enabling it to serve more effectively as a link between local, European and international policy levels. Sector-specific vulnerabilities would provide the starting point for situational assessments and analyses. Unlike the BSI, which primarily receives incident reports and sets minimum technical standards, or the Federal Office of Civil Protection and Disaster Assistance (BBK), which coordinates operational crisis preparedness, this policy unit would be responsible for the analytical interpretation and expert assessment of systemic risks in each sector.

As a complementary measure, the World Health Assembly could mandate WHO to combine official reporting data and publicly available incident data with its health-sector expertise in dedicated monitoring. For example, WHO's SSA could be expanded to include a cyber module applicable beyond "complex humanitarian emergencies". The BSI, ENISA and the European Commission could share their experiences with interoperable and tiered reporting systems (DORA from the EU financial sector and NIS-2) to make their expertise applicable to cybersecurity in the healthcare sector. Scientific, interdisciplinary open-source projects such as EuRepoC could contribute expertise on methodological issues.

Structured monitoring of the health impacts of cyberattacks could produce aggregate assessments of the consequences that cyberattacks have on public health. National bodies would continue to serve as reporting hubs within their respective regulatory frameworks, while WHO would undertake the subsequent analysis of the impacts. The system of the International Atomic Energy Agency (IAEA), which is based on the confidential and anonymised transmission of incident data, could serve as a model for this reporting approach. In this context, a more in-depth analysis of the specific and systemic impacts on healthcare provision would also be possible without incurring security or reputational costs for the reporting states and institutions. At the same time, the institutions and governments acting as reporting bodies would benefit from an assessment of incidents reported at the national, European and international levels, enabling them to determine the criticality of their own healthcare sector.

Similar reporting processes have already been established in the financial sector and have been practised over many years. The approach taken by the German Central Bank could serve as a blueprint for WHO's analysis of incidents. As a specialist institution, the Bundesbank analyses the extent to which cyberattacks pose a systemic risk to the stability of the financial system. To this end, it can draw directly on reporting data and publicly available incident data, such as those provided by EuRepoC; this enables the bank to develop a broad overview of the

global cybersecurity situation in the financial sector.

Situational assessments in the field of critical infrastructure — particularly in the healthcare sector — should in future be systematised and made interoperable, both in terms of expertise and technology, to make national, European and international crisis responses more effective. Strengthening resilience in the healthcare sector against cyberattacks requires national, European and international protective measures to be conceived in a coordinated manner.

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2026C35

(English version of SWP-Aktuell 36/2026)

Dr Michael Bayerlein is a Senior Policy Analyst at the Global Health Policy Lab (GHPL). Dr habil. Annegret Bendiek is a Senior Fellow in the EU/Europe Research Division at SWP and Principal Investigator of the European Repository of Cyber Incidents (EuRepoC) research consortium. Jonas Hemmelskamp is a data scientist on the EuRepoC consortium at Heidelberg University. Dr Maik von der Forst is Deputy Head of the Crisis and Disaster Management Unit at Heidelberg University Hospital.