

NATIONAL SECURITY
НАЦИОНАЛНА СИГУРНОСТ

**HEALTHCARE POLICY AND NATIONAL SECURITY RISK SCENARIOS
AND SYSTEMIC TRANSITIONS**

Gerhard Degen

University of Library Studies and Information Technologies

<https://doi.org/10.70300/SQTW3028>

Abstract: *The article analyzes potential relationships between healthcare and national security. Disruptive events (e.g., pandemics, increasing antibiotic resistance, or technical failures) can exceed the available range of action in healthcare and become a matter of national security. Conceptually, national security is not an isolated issue, but rather the result of the interaction of institutional protective mechanisms. The analysis shows that disruptions in the health sector can also have a significant impact on economic performance, social stability, and the government's ability to act. The analysis shows that sudden risks or slowly developing risk scenarios can result abruptly or gradually in the transition from a health policy challenge to a security policy problem. Finally, the article calls for comprehensive strategies. Ultimately, healthcare should be understood as an integral part of modern security architectures.*

Keywords: *Health Care; National Security; trigger mechanisms; transition; risk scenarios*

INTRODUCTION

Health risks, whether pandemic or technological in nature, are no longer just clinically relevant, but can (under certain conditions) become a matter of national security. This essay examines how to understand the interface between health systems and national security, when a health problem becomes a security issue, and how and by what mechanisms this transition takes place. Political leaders are becoming increasingly aware of the links between a functioning healthcare system and national security considerations, as well as the relevance of thematic interactions. For them, this leads to the conclusion that the stability of a society and thus of a state structure, along with external security, also depends on a functioning medical infrastructure. Health risks have many different origins and can include epidemics, biological hazards, and other crises. A threat to public health could subsequently have a lasting disruptive effect on the functioning of economic, social, or even governmental structures. Conceptually, national security is ensured through the interaction of institutions and measures. It is therefore not an autonomous, isolated concept, but rather depends in practice on concrete protective mechanisms that can be provided by areas such as defense policy, security agencies, intelligence services, legislation, international cooperation, and crisis management.

This article shows how critical medical infrastructure, human resources, and information security, as part of these protective mechanisms, can have a direct impact on the national security situation. The evaluation of future scenarios shows an increase in this interdependence, as rapid global technology-driven progress, globalization, digitalization, demographic change, and new biotechnological applications will challenge the vulnerability limits of healthcare systems. This gives grounds for the demand for integrated strategies that strengthen security and health aspects with a view to creating a resilient external image of society. In summary, the discussion makes it clear that health and safety are interlinked and that integrated strategic considerations are necessary to maintain the resilience of society as a collective.

RESEARCH METHODOLOGY

In order to introduce a methodological approach to support this thesis the inclusion of domains as health-science, security-policy and governance perspectives must be considered.

The thematic content needs to be deepened through a comprehensive search of literature sources and contemporary developments as well as reports from institutions such as the WHO,

OECD, CSIS and national security agencies. In addition, an analysis needs to be applied conceptually. The purpose was to capture central concepts such as interdependence, transition thresholds, trigger mechanisms and resilience. Various scenarios served as the basis for comparative analyses (COVID-19 pandemic, cyberattacks on health systems, antibiotic resistance). The aim of the comparisons was to identify patterns of transition from health policy challenges to national security issues. Thus, the methodology used can make a significant contribution to the identification of mechanisms, processes and decision-making logics. Methodologically, a qualitative evaluation was applied. In the first step, comparative content analysis (qualitative content analysis) of representative sources was carried out.

Orientation in the selection supported causal relationships that pointed to a direct or indirect connection between health care risks and security policy implications. In a second step, characteristic case studies are examined from the perspective of process tracing. The aim is to make temporal sequences, decision-making logic and threshold crossings comprehensible. This can illustrate a transition from health challenges to the area of responsibility of national security structures. In addition, a phase or threshold model (based on heuristics) is recommended for future deepening. This is not intended to define fixed limit values, but more to describe transitional phases. These phases characterize a state in which medical, technological and political systems come under pressure at the same time.

Comprehensive consideration and thematic limitation: The angles of consideration for further development are complexity, the chronological sequence of events, the transition into the domain of “national security”, the possibilities for preventive and predictive measures, and support through monitoring. A differentiated presentation of the measures at the individual and societal levels could complement the picture. As already mentioned, future challenges to healthcare can be complex and exceed the capabilities of conventional medical care. Such risk scenarios can therefore be multidimensional rather than purely medical in nature. This means that in certain scenarios, normal infrastructure and conventional healthcare routines may not be sufficient to meet the requirements in a timely and sustainable manner.

RESULTS

A closer look at complex risk scenarios reveals the following picture: Infectious diseases can reach pandemic proportions and lead to the rapid spread of viruses that are resistant to known therapeutic measures. Healthcare systems can become overwhelmed (e.g., COVID-19) with shortages of resources in terms of materials and staff (McCoy, et al. 2023, p. 1). In general, researchers expect the emergence of multi-resistant pathogens with significant antibiotic resistance. This would mean that standardized therapies would not be applicable, resulting in increased mortality rates and structural overload (He, et al. 2021, p. 2). Environmental and technological risks are increasingly becoming an issue. Climate-related changes (heat, flooding, strong winds) have a negative impact on infrastructure (drinking water, energy, communications, transport links, critical resources and storage, healthcare facilities). A combination of heat waves and power outages, for example, can immediately lead to critical supply problems. Active external influence is once again a geopolitical issue due to experiences from conflicts (Ukraine) (Kutcher & Borisch 2025, pp. 473–478): cybercrime and hacker attacks aimed at disrupting hospital operations, interrupting supply chains and procurement logistics (e.g., vaccines), or causing the collapse of medical care in general. Ultimately, the spread of pathogens (biological warfare) is also one of the risk scenarios. In addition to medical care, security and surveillance facilities are also challenged in general. The latter raises the follow-up question of when the invisible line between medical and national security is generally crossed.

At what point are national security interests affected? As mentioned at the outset, national security interests generally concern the stability of the state. This includes also functionality, and protectability. The population and critical infrastructure are the subject of the protective function.

There are now various indicators triggering intervention by security authorities: When many human lives are directly at risk, examples include pandemics, large-scale food or drinking wa-

ter contamination, or threats to hospitals, energy supplies, and critical infrastructure. Externally caused intentional threats such as bioterrorism or cyberattacks on medical facilities (Kutcher & Borisch 2025, pp. 473–478).

In summary, it is clear that complex risk scenarios can quickly exceed the capabilities of healthcare systems, as these operate from a purely medical perspective. When medical capabilities are exceeded, national interests are immediately endangered. This situation arises when a crisis scenario threatens the population on a large scale, endangering available infrastructure or public order. By definition, national security measures are activated when risks exceed defined limits and additional measures are necessary.

Interface, transition stages, and trigger mechanisms

A deeper exploration of the topic of healthcare systems and national security leads to keywords such as interface, transition stages, and trigger mechanisms. The increasing interconnectedness of healthcare and security reflects the search for applicable methods to manage relevant risks. Politicians are responsible for making decisions or take action to predict, prevent or solve these problems.

Knowing these thresholds is an essential point for further consideration. Whether these boundaries can be identified as specific points, interfaces, or phases which can be limited in time is at the core of further elaboration. Practical examples may serve to illustrate the theoretical assumptions in the last part of the essay. By 2025, modern healthcare systems should no longer be measured solely by the number of hospitals and beds. A well-functioning healthcare system that is tailored to needs is no longer limited to treatments and therapies. Clinical units are only one dimension of a close-knit care network that is ideally supported by continuous monitoring. Needs-based systems are dynamic systems and are by no means limited to clinical units. Dynamics can affect several directions of development, and healthcare geared towards this can (under certain conditions) also become part of and a matter of national security.

This paper examines the connections and interactions between healthcare systems and national security. The question of when a situation in the healthcare sector becomes a security issue is part of the investigation. The question of how this transition manifests itself, whether through processes, mechanisms, or human intervention. From society's perspective, reliable, targeted medical care is an expression of a functioning state. Medical care is the state's responsibility for its citizens. Fair and reliable healthcare strengthens society's perception of a stable state structure and creates trust. The result is that the state's ability to perform is demonstrated. However, if this part of the infrastructure is damaged or disrupted by external influences, this can jeopardize the ability of the state and its institutions to act in several respects (World Health Organization 2025). The same institution raises the issue of "health security" to include, by definition, all activities that support the identification of a decision-making space from a broader perspective. Within this decision-making space, risks become active by definition. The overlap between health and safety aspects is already considered to be the basis for the above definitions. The World Health Organization calls for the following preventive measures in the field of health care: Preventive measures should be preventive, protective and reactive. The aim would be to avoid or reduce potential risks and consequences of foreseeable acute health hazards. This goal requires international action to reduce the spread of risks across national borders (World Health Organization 2025).

Recognizable risk scenarios in terms of content:

Some significant security risks are known. Prominent among these is the threat posed by new communicable diseases, but also already known antibiotic resistance. These without corresponding advances in developing alternative care concepts might end with considerable treatment deficits. Triggering situations can arise from biological threats, technologically supported cybercrime with attacks on healthcare structures, or simply from carelessness in the laboratory. One institute focused on these risk situations is the Center for Strategic & International Studies (CSIS). The institute has evaluated this as a field of study in research on the topic of "health security" and identified overlaps between global health issues and security aspects. The results were recommendations for preventive measures against the spread of pathogens and biological hazards and clear indica-

tions for strengthening healthcare infrastructures (CSIS 2025). At the same time, research-based literature also points out that health and security issues can no longer be viewed solely from a local perspective. The interdependencies exist on a global level. “It is necessary to identify the numerous interfaces and interactions between actors and programs in the field of health and security (McCoy et al. 2023, p. 1).

Standardization: Since 2005, the World Health Organization has been engaged in publishing global standards in the field of health and safety (WHO 2005) and, in addition, to support country-specific application (WHO 2005).

Transition process – from healthcare to national security

Thresholds and criteria are often (but presumably not always) quite recognizable: The question arises as to when healthcare leads to a shift in responsibility to the security apparatus. This moment can occur as soon as a challenge overwhelms the healthcare system’s capacity to provide care and requires additional functions, infrastructure, and central facilities and instruments. Signs of this can include:

Prominent among these are the overload or failure of essential parts of the healthcare system. Furthermore, significant economic damage can result from the disruption of healthcare facilities. Disease outbreaks and the associated loss of productivity can have a destabilizing effect. At the same time, there is a risk that military capabilities or security-related infrastructure could be compromised. In addition, the spread of pathogens could lead to international outbreaks, resulting in cross-border difficulties. The accompanying weakening of state authority would make it considerably more difficult to maintain public order.

The Process of Transition – Human Intervention or Automated Systems?

A real example given by the pandemic: a new dangerous highly transmissible virus is spreading rapidly. This crosses geographical boundaries and thus the situation can gain national security relevance within a short time. As a result, there is political pressure to make decisions, taking into account the situational risk assessment. The decision may favor the transition from health care to the issue of national security. Ideally, decision-making guidelines are prepared for support. These focus on risk classification and extent of damage, but also under what circumstances in a critical situation of health care a decision should, can, must be made proactively and promptly in the direction of further administration by the structures of the security authorities. Once preparations have been made, this can be done mainly through targeted, politically initiated frameworks and decision-making criteria (if-then criteria). In practice, when governments or international bodies officially classify a problem as a “threat to national security,” procedures and protocols come into effect. An example: A UN resolution ruled that targeted attacks on health care facilities also involve a global health and thus security risk (UN Press Releases, 2024).

Forms and dynamics of the transition from health to safety – Immediate, rapid transition: After discussing the content and possible triggers, the moment or phase of the transition should be looked at even more closely. An unexpected short-term development, such as the COVID-19 pandemic, can overwhelm health systems within a very short time. The impairment of economic life is directly affected. Another consequence can be the need to use the national resources of the national security institutions, in this example the outbreak acts as an **initial trigger** that requires immediate security policy responses.

Temporal transition: The opposite situation can occur through a slow, gradual transition. If antibiotic resistance is increasingly present due to the virus, bacteria, fungi or other threats, a creeping weakening of the supply system will occur. Often overlooked by chronic underinvestment or supply crises over long periods of time, states become vulnerable. In such cases, the transition to the security question takes place gradually. *Less recognizable, but threatening in its overall scope, as there is usually already contamination of the infrastructure area and can mutate into a crisis.*

Technology-induced scenarios: the age of digitalization has also made healthcare systems vulnerable to technology (cyber-attacks or misinformation). The initiators of such attacks have the opportunity to disrupt a state structure in its supply and social functions by non-military means.

Cyber and ransomware attacks: In addition to data protection concerns, the WHO has also

focused on the endangerment of patients' lives. Thus, the transition from health to safety problem is also in the technological-systemic area (Ghebreyesus 2024).

The transition phase: With the entry into the phase of the framework conditions and processes of safety facilities, health care becomes part of a comprehensive security concept. Once a health issue is recognized as a safety issue, specialized resources, processes, and tools expand. Health and specialist ministries are cooperating with each other, coordination resources are being mobilised, international interactions are being strengthened and crisis management structures are being activated. Health is becoming part of a broader security strategy. Viewed comprehensively, a security strategy that is pre-planned for cases of threat with the connection of health systems and the framework of national security can no longer be regarded as a theoretical side field, but as a central dimension of modern regulatory systems for states. Health as an obligation of the state is extended to a security issue. From the moment when the requirements that exceed purely medical capacity limits go beyond and reach the cornerstones of the sovereignty of the state. Triggers and threat scenarios may be manifold, but the framework and processes made in advance by the political authority are essential. There is an institutional link and instrumental expansion, in short: health systems become part of the state's safety net. The political responsibility is evident from the explanation so far. All health policy measures are by no means isolated, separate areas. Preventive provisions for crises, care concepts and all sub-areas of the state security infrastructure are affected.

Improvements and new paths: the present explanation also provides new additional options for improving existing supply facilities. These are to be predominantly cross-departmental and act as integrated AI-supported processes. Increasing the internal and external cohesion of society is a central component and the following case studies from contemporary practice show how individual situations can be considered more solution-oriented or still problematic. As far as practical evidence is available, three contemporary examples can be cited as examples on the basis of the theoretical explanations so far. In the context of health care and national security, these are as follows: pandemic Covid-19 in Western Europe, extortion and cybercrime in the UK and Ukraine. The examples are evaluated with a detailed justification and presented with extended comments on weaknesses and possible improvements.

Example 1: The Covid-19 pandemic (in Central and Western Europe)

While many countries tried to reduce acute mortality and the burden on intensive care medicine through vaccination campaigns, surveillance (including wastewater surveillance) and preventive programs, structural problems (inequality, chronic burden of disease, lack of structural investment) remained.

This means that population-based health measures have certainly strengthened national security thinking, but the impact has been significantly dampened by years of hardened structures and gaps in governance and funding (WHO European Observatory on Health Systems and Policies 2021). **There are clear demands for prevention and early detection. A recognizable vacuum exists for data integration:** One Real-time monitoring (e.g. national reporting systems, wastewater monitoring) would have enabled rapid remediation measures. There is still a lack of direct links to supporting data consolidation and the development of monitoring systems (WHO COVID-19 dashboard, 2025).

From Preventive to Predictive: Monitoring and Early Warning Systems Can significantly support the lead time for countermeasures (vaccination campaigns, resource shift). This prevents the direct consequences of disruptions to critical infrastructure or detects them in advance (e.g. care, police). This would result in a clear additional safety benefit (Ghebreyesus, et al. 2022).

Resilient supply networks: Regions with robust primary care and integration models have been able to maintain care in a stable and continuous manner. In this environment, the national security impact was stronger. OECD analyses therefore recommend targeted investments in resilience (OECD Health Policy Studies 2023). It became clear that insufficient investment before the pandemic (high chronic disease burden, fragmented care) limited the effectiveness of these measures (vulnerable groups could only be addressed partially and then with increased effort). Without structural reform, vulnerability to new risks remains (OECD Health Policy Studies 2023).

Example 2: Extortion and cybercrime – the WannaCry case

Cyber-attacks on healthcare facilities not only endanger immediate patient care (surgery cancellations, transfers) but also undermine the trust of the population and could directly affect national security (disruption of critical infrastructure, diversion of state resources). The situation **WannaCry** shows how outdated IT infrastructure in combination with inadequate precautions can lead to extraordinary disruptions to health care. Currently, there are ongoing trends and a segregated complexity of such attacks. Inclusive cooperation between health care and national security is here **not particularly pronounced** (National Audit Office 2018).

Ransomware attacks could lead to the collapse of supply continuity. In the UK, gaps in legacy software led to massive disruption (surgical failures). Research shows that IT weakness weighed heavily on the NHS's operational response, which was clear evidence of negative security effects.

The lack of integration between health IT, national cyber defense and emergency planning exacerbated the consequences. The deficiency was the missing component “cooperation between health, safety and technology sectors”. (Cybersecurity & Infrastructure Security Agency 2020). **There is an ongoing trend and modern ransomware tactics:** US authorities HHS/analyses document persistently high number of attacks, double extortion (data leak + encryption) and increasing targeting of healthcare and public institutions. This makes the situation systemically exposed and dangerous. This is true as long as cyber resilience is lacking (Office of Information Security HHS 2023).

Within the framework of these obvious weaknesses, some thoughts for improvement are possible- like early warning systems through data integration and real-time monitoring: Investing in national surveillance, data sharing platforms, and standardization to improve early detection and coordinated crisis response (OECD Health Policy Studies 2023). **Building resilience for cyber situations should be a core component of resilient care. A strategic division of critical networks,** virtual or real situational task forces with protocol mandates that work with health care facilities and both local and federal agencies with a national cyber focus.

Scenario planning and cross-sectoral real-world exercises: Joint crisis simulations (health × safety × infrastructure) increase operational interoperability later in the event of an emergency (avoidance of unrealistic dry training) (Haldane, et al. 2021, pp. 964–980). **Targeted investments in primary and public health capacities** to reduce vulnerable population groups (as a long-term security gain). (OECD Health Policy Studies 2023). Finally, a summary to answer the question of the “timing and the trigger criteria” for the transition from regular operation to integration into the structures of national security: The chosen examples to answer the question are: the Covid-19 pandemic, the WannaCry case in the UK and the slow development of antibiotic resistance. The investigation is from when (point in time) and/or with which trigger criteria the transition from regular operation of health care to introduction into the structures of national security is achieved.

Timing and triggering criteria for the transition from **regular operations** to integration into **national security structures:** In the example of Covid-19) defines the point in time when a locally limited infection situation develops into a national health crisis with the threat of overloading medical care. Trigger criteria could be an exponential increase in the number of infections beyond the capacity limits of the health system, supply bottlenecks in intensive care places, or additional support for federal authorities. **In the example of cybercrime** (e.g. WannaCry in the NHS, UK), the time as soon as digital attacks impair or paralyze the functionality of critical infrastructures in the healthcare sector (e.g. hospitals, laboratory networks, rescue coordination centers) will be impaired or paralyzed. The primary trigger criteria are the failure of central IT systems endangering patient care, broader attacks (by institutions or regions), the call for the need for national cyber defense. In the case of antibiotic resistance in a population, the point in time would be when resistance developments permanently endanger public health and security of supply and national or international spread becomes apparent. **Trigger criteria** are the detection of multidrug-resistant pathogens with a significant increase and lack of therapeutic options and the risk of system-wide failures; Use of coordinated defense strategies.

The **overall resilience** of the health system and transition to national security: If you look at the three threat scenarios **at the same time** (pandemic, cyber-attack, antibiotic resistance), **no single point in time** of transition can be clearly defined. Instead, there is a **phase-oriented transition period in which solutions are positioned**. In summary, the **transition to the national security structure** can be described as follows: either several subsystems become critical at the same time (e.g. **overload of facilities** and *failure of IT systems*) or the *self-control of health care has reached limits, or state intervention becomes necessary to ensure care and order*.

CONCLUSIONS

This paper reveals that healthcare and national security are not isolated domains. An interdependent system has emerged. Disruptive events can transcend the functional boundaries of health-care systems, thereby threatening elements of state stability. This affects public order, economic performance, and, more generally, the state's capacity to act.

A transition from a health policy challenge to a national security problem will usually not be detectable as a single event. Rather, it will arise when thresholds are exceeded, causing stress in several areas. These can simultaneously and rapidly affect healthcare, social, and political subsystems, exacerbated by technical challenges. These findings imply that national security depends not only on traditional defense mechanisms. It also needs to include the resilience of critical medical infrastructure, human resources, information systems, and preventive capacities. Mandatory are effective prevention, surveillance and early warning systems. A cross-sector coordination is an essential component. International cooperation and standardized frameworks further strengthen this resilience in an increasingly globalized risk environment.

Health care is part of a national security policy. Beyond the social and ethical-moral obligation, the strengthening of health systems is part of a strategic orientation. This strengthens social resilience and protects the long-term stability of the state.

REFERENCES

- CSIS, 2025. *A New Era in Health Security* [online]. [Viewed 29 October 2025]. Available from: <https://www.csis.org/analysis/new-era-health-security>
- CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA), 2020. *Ransomware Activity Targeting the Healthcare and Public Health Sector* [online]. [Viewed 30 October 2025]. Available from: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a>
- GHEBREYESUS, T. A., et al., 2022. WHO recommendations for resilient health systems. *Bulletin of the World Health Organization* [online]. [Viewed 03 November 2025]. Available from: <https://doi.org/10.2471/BLT.22.287843>
- GHEBREYESUS, T. A., 2024. *Threats posed by ransomware attacks against hospitals and other health-care facilities and services* [online]. [Viewed 27 September 2025]. Available from: <https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks>
- HALDANE, V., DE FOO, C., ABDALLA, S. M., et al., 2021. Health systems resilience in managing the COVID-19 pandemic: lessons from 28 countries. *Nature Medicine*, vol. 27, pp. 964–980 [online]. [Viewed 16 October 2025]. Available from: <https://doi.org/10.1038/s41591-021-01381-y>
- HE, Y., ALIYU, A., EVANS, M. and LUO, C., 2021. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *Journal of Medical Internet Research* [online], vol. 23, no. 4, e21747. [Viewed 03 November 2025]. Available from: <https://doi.org/10.2196/21747>
- KUTCHER, S. and BORISCH, B., 2025. Health and global security: challenges and considerations [online]. [Viewed 02 November 2025]. Available from: <https://doi.org/10.1057/s41271-025-00562-0>
- McCOY, D., ROBERTS, S., DAOUDI, S. and KENNEDY, J., 2023. Global health security and the health-security nexus: principles, politics and praxis. *BMJ Global Health* [online], vol. 8, no. 9, e013067. [Viewed 03 November 2025]. Available from: <https://gh.bmj.com/content/8/9/e013067>
- NATIONAL AUDIT OFFICE, 2018. *Investigation: WannaCry cyber attack and the NHS* [online]. [Viewed 01 November 2025]. Available from: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>
- OECD, 2023. *Ready for the Next Crisis? Investing in Health System Resilience*. OECD Health Policy Studies [online]. Paris: OECD Publishing. [Viewed 03 November 2025]. Available from: https://www.oecd.org/en/publications/ready-for-the-next-crisis-investing-in-health-system-resilience_1e53cf80-en.html
- OFFICE OF INFORMATION SECURITY, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, 2023.

2022 Healthcare Cybersecurity Year in Review and a 2023 Look-Ahead [online]. [Viewed 27 October 2025]. Available from: <https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf>

UNITED NATIONS, 2024. *Ransomware Attacks on Healthcare Sector “Pose a Direct and Systemic Risk to Global Public Health and Security”*, *Executive Tells Security Council* [online]. [Viewed 21 September 2025]. Available from: <https://press.un.org/en/2024/sc15891.doc.htm>

WORLD HEALTH ORGANIZATION (WHO), 2005. *International Health Regulations (IHR)* [online]. [Viewed 18 October 2025]. Available from: <https://www.who.int/health-topics/international-health-regulations>

WORLD HEALTH ORGANIZATION (WHO), 2025a. *COVID-19 Dashboard: WHO Health Emergencies Programme* [online]. [Viewed 03 November 2025]. Available from: <https://data.who.int/dashboards/covid19/summary>

WORLD HEALTH ORGANIZATION (WHO), 2025b. *Health Security* [online]. [Viewed 03 November 2025]. Available from: <https://www.who.int/health-topics/health-security>

WORLD HEALTH ORGANIZATION (WHO), 2025c. *National Action Plan for Health Security (NAPHS)* [online]. [Viewed 18 October 2025]. Available from: <https://www.who.int/emergencies/operations/international-health-regulations-monitoring-evaluation-framework/national-action-plan-for-health-security>

WORLD HEALTH ORGANIZATION EUROPEAN OBSERVATORY ON HEALTH SYSTEMS AND POLICIES, 2021. *Health Systems Resilience During COVID-19: Lessons for Building Back Better* [online]. [Viewed 02 November 2025]. Available from: <https://eurohealthobservatory.who.int/publications/i/health-systems-resilience-during-covid-19-lessons-for-building-back-better>

ЗДРАВНА ПОЛИТИКА И НАЦИОНАЛНА СИГУРНОСТ. РИСКОВИ СЦЕНАРИИ И СИСТЕМНИ ПРЕХОДИ

Резюме: Статията анализира потенциални връзки между здравеопазването и националната сигурност. Разрушителни събития (например пандемии, нарастваща антибиотична резистентност или технически повреди) могат да надхвърлят наличния обхват на действия в здравеопазването и да станат въпрос на национална сигурност. Концептуално, националната сигурност не е изолиран въпрос, а по-скоро резултат от взаимодействието на институционалните защитни механизми. Анализът показва, че смущенията в здравния сектор могат също да имат значително въздействие върху икономическото представяне, социалната стабилност и способността на правителството да действа. Анализът показва, че внезапни рискове или бавно развиващи се рискови сценарии могат да доведат внезапно или постепенно до преход от предизвикателство на здравната политика към проблем със сигурността. Накрая статията призовава за цялостни стратегии. В крайна сметка здравеопазването трябва да се разбира като неразделна част от съвременните архитектури за сигурност.

Ключови думи: здравеопазване; национална сигурност; механизми на задействане; преход, рискови сценарии

Герхард Деген, докторант
Университет по библиотекознание и информационни технологии
София, България
E-mail: g@gdegen.at