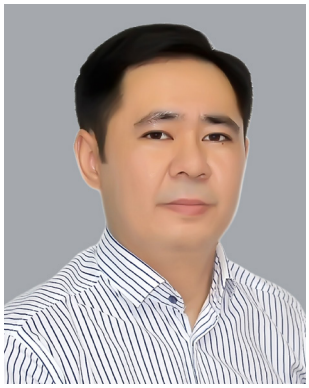
DOI: 10.51634/2307-5201_2024_2_6
УДК 341.1/8
ГРНТИ 10.87

GLOBAL HEALTH SECURITY IN THE AGE OF TRANSNATIONAL MALICIOUS CYBER OPERATIONS: A TAXONOMIC ANALYSIS OF NON-STATE AND STATE-BACKED CYBER THREATS



ZH. TEMIRBEKOV,
PhD in Jurisprudence
(Maqsut Narikbayev University),
LLM in International Law
(University of Reading),
Teaching Professor,
Maqsut Narikbayev University
(Astana, Republic of Kazakhstan)
e-mail: zh_temirbekov@kazguu.kz

The paper emphasises the critical nature of the cybersecurity threats to the global healthcare sector. The examination of quantitative and qualitative research results from official reports, bulletins, and journals is combined in the study to demonstrate the scope and impact of non-state and state-backed malicious cyber operations directed at healthcare systems. In today's digital age, cyber operations against the healthcare sector are increasing in rate and becoming more sophisticated. Therefore, the paper is *relevant*. The paper's *subject* is analysing the nature, scope, and consequences of malicious cyber activity; it examines how it can impact healthcare systems, patient privacy, and public health. By analysing recent incidents, conducting a taxonomic analysis, and proposing some general strategies to enhance healthcare protection in the face of cybersecurity threats, the paper sheds light on the critically important issue of cybersecurity threats in the healthcare sector, which is the *purpose* of the paper. The study's *novelty* is that this paper offers a taxonomic analysis of cybersecurity threats that provides a structured framework to understand the threats and propose some general suggestions to enhance the protection of the global healthcare sector.

Brief conclusions: 1) State-backed malicious cyber operations can significantly compromise the quality of healthcare and patient safety; 2) Decision-making centers in the healthcare sector are recommended to pay attention to the need to modernize cybersecurity policies since, as studies show, more and more healthcare organisations are becoming victims of transnational malicious cyber operations.

Keywords: malicious cyber operations, data privacy, right to health, global health, healthcare, cyber-attack resilience, healthcare infrastructure, cybersecurity, cyber threat taxonomy

Introduction

In the healthcare sector, which has become one of the prime targets for non-state and state-backed cyber operations, the evolving landscape of cybersecurity threats presents unprecedented challenges. This article aims to introduce the critical issue of malicious cyber activities directed at healthcare organisations and discuss the nature, scope, and impact of these threats. The article examines the general consequences of such attacks on the integrity of healthcare systems, patient privacy, and public health. An analysis of some recent incidents and their impact on healthcare infrastructures sheds light on the urgent need for robust cybersecurity measures to protect healthcare infrastructures against sophisticated cyber threats.

Basic Provisions
Materials and Methods

This study adopts a mixed-methods approach to examine the scope and impact of non-state and state-backed malicious cyber operations on global healthcare systems. It examines the results of quantitative and qualitative data analyses and case studies. Part of studying the results of existing quantitative analyses is assessing the frequency, nature, and outcomes of cyber operations targeting healthcare organisations worldwide. Qualitative data is collected from official reports and journals and, *inter alia*, was used to assess the threat of malicious cyber operations against the healthcare sector.

Results

1. *Malicious cyber operations and their impact on healthcare: some flagrant cases*

As former FBI Director Robert Mueller has noted, 'there are only two types of companies: those that have been hacked and those that will be' [30]. Over the past decade, cybersecurity attacks have steadily increased in the healthcare sector [10, p. 17]. In 2016, Hollywood Presbyterian Medical Centre suffered a ransomware attack that impaired access to medical records and equipment for ten days until the hospital paid the ransom (approximately $17,000) [51]. A website selling personal information about children vaccinated in China's hospitals was revealed in the same year – unauthorised access and malicious insiders working with cyber attackers led to the acquisition of this data, including home address and parent contact information [13]. Furthermore, it was reported in 2018 that Singapore's Prime Minister's medical information and that of 1.5 million other patients had been stolen [47, p. 2]. A phishing attack was detected on March 20th, 2020, targeting the World Health Organization (WHO) – a malicious website was launched to copy WHO's internal email system to steal passwords [37].

One group of writers correctly argues that among the most dangerous types of cyberattacks are those perpetrated by state actors across national boundaries [47, p. 3]. The advantages of territorial sovereignty (monopoly for jurisdiction, for example) and considerable financial and human potential make states dangerous actors in global cyberspace. Combining a sense of impunity and great power may lead to sad consequences. Indeed, state organs or state-backed hacker groups are responsible for the most devastating transnational malicious cyber operations in the last ten years.

Below the key aspects of a state-backed transnational malicious cyber operation carried out on Anthem Corporation in 2015 will be described. Also, it will briefly discuss two state-backed malicious cyber operations from 2017 that, *inter alia*, hit the healthcare sector in the territory of the UK and Ukraine—WannaCry and NotPetya, respectively.

***

Anthem, one of the largest health insurance providers in the United States (US), announced an important data breach in February 2015 [1]. In a statement released by Anthem, the company said the breach was caused by a 'very sophisticated external hacking attack' [50, p. 1]. Notwithstanding that Anthem Inc. 'demonstrated sound cybersecurity policies and procedures that limited the impact of the breach'[15, p. 81], a report on Anthem's website indicated that the company discovered that large amounts of consumer information were being accessed by unauthorised parties, including names of members, member health identification numbers, date of birth, social security numbers, addresses, telephone numbers, email addresses, employee information and income information [7].

According to prosecutors, the hackers breached Anthem's computer network without authorisation by using spear phishing attacks to gain access to the network. They used sophisticated techniques to penetrate the company's computer network without its permission [27]. Even though the hackers 'patiently waited months' to steal the data, they were still successful [27]. It appears that the Anthem cyberattack was executed by or through the Chinese government, which would make it an appropriate candidate to be classified as a 'nation-state' attack [49].

In May 2017 various companies, including FedEx, Renault, Telefonica and Deutsche Bahn, were affected by the WannaCry ransomware. However, England's National Health Service (NHS) was the hardest hit [39]. The malware encrypted all computer data, locked the operating system, and demanded a ransom in Bitcoin [52]. Despite NHS 'was not the specific target' of the malware [21], as a result of the WannaCry attack, there was a postponement of many surgical procedures; an estimated 20,000 appointments were cancelled; it affected the activity of GP surgeries, dental practices, and pharmacies; some patients were unable to be treated by five emergency departments, and they were diverted to other facilities; the incident affected 80 out of 236 NHS trusts and 603 NHS organisations [26]. The United Kingdom's National Cyber Security Centre (NCSC) speculated that the operation was launched by the hacker group 'Lazarus', which is believed to be affiliated with the North Korean government [31].

According to the findings of a group of researchers, all NHS trusts' activity went down over the WannaCry week for all functionality. Infected trusts experienced 50% more daily cancellations than unaffected trusts after the beginning of the attack. During WannaCry attack week, Accident and Emergency Department attendance dropped by 6% daily. The lesser activity at the affected trusts was worth £5.9 million economically that week. Despite all this, the authors cannot determine the true impact of the attack on complications, care procedures, or patient outcomes. At the same time, no trust significantly differed in the death rate from the baseline week. Also, according to the authors, finding the 'kill switch' on the same day as the attack reduced WannaCry's potential effect on health services [17].

In June 2017 in Ukraine, the NotPetya attack hit at least four hospitals and two airports in Kyiv, six power companies, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, practically every Ukrainian governmental agency, National Bank of Ukraine, Chernobyl Nuclear Power Plant's monitoring system, and at least 300 companies. One senior Ukrainian government official estimated that 10 per cent of all computers in the country were wiped out [19].

The president of the Boris Clinic group of Kyiv hospitals, Mikhail Radutskiy, recalled that, in addition to cancelling all upcoming appointments, the GPS used to locate ambulances at the hospitals had failed as a result of the NotPetya attack. Although IT administrators are able to retrieve a copy of all their systems from three days earlier, all tests performed since then, such as blood tests, MRIs, and CAT scans, would have to be repeated [18].

The consequences of the NotPetya attack were global. As the US State Department stated, NotPetya damaged the computers of hospitals and other medical facilities in the Heritage Valley Health System in western Pennsylvania, a large U.S. pharmaceutical manufacturer, and other US private sector entities [46]. In total, the NotPetya attack caused worldwide damage for 10 billion US dollars [48]. However, there is no information about physical harm or injury to individuals [38].

It is believed that the Russian government was behind the NotPetya cyber operation. For instance, the NotPetya attack against Ukraine has been reported by the Ukrainian government to have been carried out by Russian security services in an attempt to destroy important data [45]. It has been reported that the Russian military carried out the NotPetya attack 'almost certainly' [36]. A reward of up to $10 million has been offered by the US in exchange for information concerning six people described as Russian military intelligence officers who had allegedly carried out the NotPetya attack [35].

2. *An understanding of healthcare cyber security risks*

Overview

The abovementioned examples are only a small part of malicious cyber operations against healthcare organisations. By way of illustration, of the 4026 Patient Health Information breaches that affected 303,284,800 people in the United States from January 1, 2011, to December 31, 2021 – 43% were primarily hacking/IT related [44, p. 180]. During the year 2021, there were 5,212 confirmed data breaches due to malicious cyber operations worldwide, of which 571 were in the healthcare sector [11]. At the same time, 75% of all data breaches in Europe are unreported [8].

Cashwell observes that there are two types of vulnerable objects in the healthcare sector: (i) computer networks and electronic equipment; (ii) infrastructure essential to anticipating, preparing for, responding to, and minimising public health emergencies (power grid or telecommunication infrastructure, for example) [9, p. 29].

Harkins and Freed's work shows that personal health information is an ideal target for ransom demands due to its fluid nature. They also argue that healthcare organisations are ill-prepared to counter cyber-attacks, which makes them attractive targets [20].

Thus, there are two reasons why the healthcare sector may be attractive to cyber adversaries. It is a rich source of valuable data and a soft target that makes it a tempting target for cyberattacks [24].

Valuable data includes clinical personal health information, personally identifiable information, and research intellectual property. For example, a credit card number or social security number can be sold for between $1 and $15 on the dark web, whereas personal medical information can be sold for as much as $60 [28]. The reason for such a high price for personal medical information may be that it cannot be reset, and one's records may contain enough information to open a bank account, obtain a loan, or get a passport [24].

The healthcare sector may be a soft target because of cybersecurity weaknesses (it was explored, for example, in the works of Mattei [25], Mrcela and Vuletic [29], Thamer and Alubady [43]), including the particularities of data usage by personnel. For instance, openness and sharing of healthcare information are essential [4, p. 3]. This is why the health information systems in almost every department in a hospital store personally identifiable information and protected health information. Electronic health records, e-prescribing software, remote patient monitoring, dietitian information systems, and laboratory information systems are used by all healthcare providers (including physicians, physician assistants, nurses, pharmacists, and physical therapists) [3, p. 2]. As a result, the wide access to healthcare information increases the risk of violation of its integrity or confidentiality.

Cyber threats to the healthcare sector

The relevant literature analysis indicates that malicious cyber operations against the healthcare sector may be classified based on their form, aims, location of the breached information, types of cyber adversaries, and motivations.

The authors of examined papers [4, 32, 22, 5, 47] generally distinguish seven forms of malicious cyber operations against the healthcare sector:

- Malware or malicious software. Several types of malicious software are designed to cause harm to a computer system or compromise it without the user's consent. Malware is spread physically by using an external drive or online by using emails posing as 'phishing' attacks. These programs perform several functions, such as altering, damaging, spying, or deleting user information. Some common malware is known as worms, bots, viruses, trojans, spyware, adware, backdoors, ransomware, and rootkits. Among the mentioned malware, a ransomware attack is probably the most popular form among cyber adversaries. A ransomware malicious program prevents users from using their operational systems until they pay a fee to the attacker [16]. Cyber adversaries use ransomware to encrypt vital data in order to prevent an organisation from accessing that data. Access is granted (not in all cases) only after the attackers receive payment for the ransom.
- Denial-of-Service (Dos) or Distributed-Denial-of-Service (DDoS) attack. The attack occurs when a cyber adversary actor floods a network with traffic to the point that the network cannot react and is, therefore, unable to be accessed. Medical teams are often unable to retrieve or send patient data due to DoS events, which are usually intended to damage the hospital's reputation or make the hospital's services unavailable to patients. The most famous example of a DDoS attack is the 2007 attack against the Estonian critical infrastructure, which resulted in almost total unavailability of online public services.
- Man-in-the-middle. As a result of this attack, an unauthorised party can insert itself into the middle of communication transmission by exploiting a vulnerability in the target party's net-

work connection. Information being exchanged can be intercepted, stolen, or altered by the attacker before it reaches the receiving end of the communication.

- SQL attack. An attack consisting of a sequence of character inputs is designed to target a particular vulnerability in a system, resulting in the destabilisation or inaccessibility of system functions and potentially the exposure of data. This form of attack is generally conducted on internet servers or database systems.
- Spoofing occurs when hackers manipulate a medical device to receive an external signal, enabling them to access or manipulate data, system settings, and other system components. Sometimes, it is not difficult and requires no special equipment. However, it may be especially dangerous for some types of devices on the Internet of Medical Things (pacemakers, for example).
- Drone-specific attack. At first, a drone flies over a healthcare facility. Then, as part of drone attacks, users are generally required to disconnect from the network to perform re-authentication. After that, the drone creates a new one, which appears to be a legitimate access point on the healthcare organisation's network. Deceived personnel of a healthcare organisation log into it. The personnel provide their login information on an infected page before proceeding to the internal (as they think) of a healthcare organisation's network. The hackers use this method to steal the logins and passwords of the personnel from the internal network of a healthcare organisation.
- Web-based attacks. These attacks attract hackers because they exploit various systems, provide malicious URLs and scripts, or even download malware content in order to exploit the various systems. In addition to affecting accessibility, web-based attacks can compromise data integrity and confidentiality. The most common Web-based attacks are form jacking, malicious browser extensions, and malicious software downloads via online software.

The main aims of malicious cyber operations against the healthcare sector may be:

- Collection of information. Personally identifiable information (PII), protected health information (PHI), and results of clinical research may be attractive for hackers seeking financial gain or motivated by political reasons;
- Attacks on databases. Managing information resources effectively and efficiently in a digital society is an essential component of decision-making and scientific research in a digital society. Medical databases contain information about electronic medical records, medical equipment, websites, and other relevant information. An attack on a database in the medical area may result in doctors being unable to retrieve patient information, which may delay treatment;
- Attacks on websites. The doctor can access patient information and provide prescriptions through a website connected to the hospital database. The website may be compromised if malicious attackers send incorrect information instead of accurate patient information. In another case, the website may crash, resulting in a delay in treatment [34];
- Attacks on operation devices. By developing technology, patients' treatment will inevitably become more accurate, which means they depend more on medical equipment such as the Internet of Medical Things (IoMT). This poses a threat to the patient's safety, as the operating devices may be vulnerable to attacks through the Internet. In some cases, such as those involving pacemakers, it can be fatal if communication is disrupted [33].

The study by a collective of authors [44] has revealed that the breached information of the US healthcare sector between January 1, 2001, to December 31, 2021, was located (from highest to lowest per cent of breaches) on:

- network servers (26 per cent, affected 227,686,822 individuals)
- email (24 per cent, affected 30,071,008 persons)
- paper/film (17 per cent, affected 5,315,442 people)
- other (11 per cent, 15,758,977 affected)
- laptop (9 per cent, 5,662,706 affected)
- desktop computer (8 per cent, 11,529,003 affected)
- electronic medical records (6 per cent, 7,260,842 affected)

As for the types of cyber adversaries who may be interested in carrying out malicious cyber operations against the healthcare sector, Bris and Asri [6], for example, divided them into five groups:

- Individuals and small groups. Profit and notoriety are their primary motivations, so they usually target targets based on opportunities and employ crude tactics;
- Political groups and paparazzi. Their motivations include hacktivism as well as political and financial gain. They are typically interested in embarrassment, discredit, blackmail or the sale of information about prominent citizens;
- Criminal organisations. In addition to financial gain, they are motivated by criminal activities such as extortion, blackmail, and coercion. It is possible that they would seek to obtain medical records about targeted individuals and threaten or harm them due to these activities. Additionally, they may benefit from the exploitation of massive amounts of untargeted electronic health records;
- Terrorists. Typically, their objective is to harm or threaten individuals. The motive behind their activities is to inspire fear and cause harm;
- Nation-states are likely to present the greatest threat to health care. Indeed, enemy nations may seek to harm or threaten individuals and obtain personal information, such as patient electronic health records, to exploit massive groups of individuals.

As one can see from the abovementioned, there may be many reasons why individuals, groups or states may decide to carry out malicious cyber operations against healthcare organisations or affiliated entities.

Nevertheless, according to the Data Breach Investigations Report in 2021, most breaches (approximately ninety per cent) were related to financial gain and in the second place (nearly 5 per cent) breaches that occurred due to political purposes [11]. According to Seebruck, cyber adversaries motivated by ideology or profit are the ones who use highly sophisticated methods [40, p. 39].

Thus, financial motivation is the main reason for most malicious cyber operations against the healthcare sector. One group of writers argued that after examining 35 articles from mid-2016–2021, they revealed that in 91% of data breaches that occurred in the healthcare sector, cyber adversaries were motivated by money [47]. Another group of authors found that during the COVID-19 outbreak, 'cybercriminals are mercilessly increasingly utilising disruptive malware against vital infrastructure and healthcare organisations because of the potential for financial gain' [2].

Aside from the financial benefits, healthcare organisations are increasingly targeted by foreign governments who undertake cyberattacks with nefarious political and disruptive goals. For example, in a report issued by the World Anti-Doping Agency (WADA), Tsar Team (APT28), a Russian cyber espionage group also known as Fancy Bear, has illegally accessed WADA's Anti-Doping Administration and Management System database through an account created for the Rio 2016 Games by the International Olympic Committee. It is believed that the group gained access to athlete data – such as medical information provided by International Sports Federations and National Anti-Doping Organizations related to the Rio Games; they then released a portion of the data into the public domain, along with a threat to release additional information [42].

Discussion and Conclusion

Although none of the examined in Part 1 of the Results section malicious cyber operations led to documented explicit injury or death, the negative consequences of such adverse cyber activity may be serious, even causing the death of a patient. For example, Corman has drawn attention to the fact that an ambulance traffic delay of fewer than five minutes led to four per cent more hospital deaths over the following thirty days [18, p. 214]. Furthermore, there is a lot of information in an individual's medical file, including blood type, past surgeries and diagnoses, as well as other medical information, since these records contain personal information such as names, dates of birth, insurance and health provider information, along with health and genetic information, restoring privacy or reversing psychological harm when private data is compromised cannot be achieved [3, p. 1].

Furthermore, patients can suffer permanent or temporary injuries not only as a result of direct consequences, such as failing to perform appropriate medical acts or turning off critical medical devices but their health can also be adversely affected by indirect actions aimed at disrupting medical care. For example, it is extremely likely that any alteration of a patient's health records, the compromise of medicine inventory systems, or the interruption of power supply in an operating room will dramatically impact a patient's health [6, p. 1]. Moreover, the link between malicious cyber operations and disease morbidity and mortality rates among patients has also been found in recent studies to be concerning [44, p. 3].

It should be noted that healthcare services can be categorised into two distinct categories: critical services and administrative services. The medical devices and medicine delivery systems are a part of the first ones, which ensure continuity of care. Due to the disruption of these services, patients' health may be adversely affected. The administrative services are responsible for ensuring the smooth operation of the hospital. Among these services are the systems that handle work orders, medicine inventory, prescriptions, bills, or appointments. However, the unavailability of these systems is less of a concern if the downtime is brief. In addition, it is important to remember that the reputation of the facility and the medical staff is also a non-negligible asset. Certainly, patients have to feel comfortable placing their trust in the medical staff and feel safe knowing that the facility is safe and reliable [6, p. 2].

As for the taxonomy of malicious cyber operations, a comprehensive literature review identifies a diverse and sophisticated set of cyberattacks targeting the healthcare industry. Healthcare organisations face various cybersecurity challenges because of the complexity of these threats. The generalised classification below provides a structured framework for understanding these challenges.

Forms of Malicious Cyber Operations. According to the literature review, cyber operations involve a broad range of malware infections, including ransomware attacks and more nuanced approaches like man-in-the-middle attacks and SQL injections. In 2017, when WannaCry ransomware led to a significant disruption of NHS services in England, the sophistication of these attacks highlighted how vulnerable healthcare systems are to cyber-attacks. Cybersecurity is becoming more complex as new attack vectors emerge, including drone-specific attacks and web-based threats. Comprehensive and dynamic defence strategies are required to counter these threats.

Aims of Malicious Cyber Operations. Despite the variety of forms cyberattacks take, their primary objectives remain the same. PII and PHI thefts, as well as attacks on operational devices that disrupt medical services, reveal that the motives behind these operations are a mixture of economic and political. Taking advantage of vulnerabilities in the IoMT raises significant concerns about potential catastrophic outcomes due to the intersection of technology and patient safety.

Locations of Breached Information. According to an analysis of data breaches reported by healthcare organisations in the U.S. from 2001 to 2021, the most vulnerable systems were network servers and email systems. This trend underscores the importance of implementing cybersecurity measures in healthcare as it undergoes digital transformation.

Types of Cyber Adversaries. The healthcare sector faces a wide spectrum of cyber threats, including individuals and small groups, political groups, criminal organisations, terrorist groups, and nation-states. It is important to differentiate between these types of threats so that nuanced and targeted countermeasures can be implemented in response to the unique threats posed by each type of opponent.

Motivations of Cyber Adversaries. Most data breaches committed against the healthcare sector are driven by monetary incentives, with financial gain as the principal motivation. In addition to these financial incentives, foreign governments are increasingly targeting the sector for political and disruptive purposes, posing a dual threat to national security and the economy.

The categorisation of cyber threats offers a framework for comprehending cybersecurity issues, stressing the need for strategies to combat various types of malicious cyber operations. Collaboration is essential, necessitating efforts from countries, healthcare organisations, and cybersecurity experts to exchange information and assets in order to enhance the global healthcare sector's ability to withstand cyber threats.

In conclusion, it can be claimed that the investigation into cybersecurity threats posed by non-state and state-backed actors to the global healthcare sector is critical and emphasises the importance of implementing thorough and coordinated measures to safeguard healthcare cyberspace. Instances such as the Anthem data breach and WannaCry attack underscore the susceptibility of healthcare information and the potential risks to patient well-being and public health. Protecting health systems from malicious cyber activities should be one of the key public health priorities that require proactive and collaborative approaches. By implementing cybersecurity measures and fostering partnerships, the healthcare industry can strengthen its defences against evolving cyber risks, ensuring continuous delivery of high-quality care and safeguarding public health on a global scale. Therefore, it is crucial for decision-making centres to adopt a multifaceted strategy that includes strengthened cybersecurity policies and protocols, as well as effective response mechanisms.

Ж.Р. Темірбеков, PhD in Jurisprudence, LLM in International Law, Teaching Professor Maqsut Narikbayev University (Астана қ., Қазақстан Республикасы): **Трансұлттық зиянды кибероперациялар дәуіріндегі жаһандық денсаулық қауіпсіздігі: мемлекеттік емес және мемлекеттер демеушілік ететін киберқауіптердің таксономиялық талдауы.**

Мақалада жаһандық денсаулық сақтау үшін киберқауіпсіздік қатерлерінің маңыздылығы көрсетілген. Зерттеу денсаулық сақтау жүйесіне бағытталған мемлекеттік емес және мемлекеттер демеушілік ететін зиянды кибероперациялардың ауқымы мен әсерін көрсету үшін ресми есептердің, бюллетеньдердің және журналдардың сандық және сапалық талдауын біріктіреді. Бүгінгі цифрлық заманда денсаулық сақтау саласына қарсы кибероперациялардың саны өсіп, олардың жүзеге асырылу жолдарының күрделенуі мақаланы өзекті етеді. Мақаланың пәні – зиянды кибер әрекеттің сипатын, көлемін және салдарын талдау арқылы оның денсаулық сақтау жүйелеріне, пациенттердің жеке деректерлеріне және қоғамдық денсаулыққа қалай әсер етуі мүмкін екендігін қарастыру. Соңғы оқиғаларды зерделеу, таксономиялық талдау жүргізу және киберқауіпсіздік қатерлері жағдайында денсаулық сақтауды қорғауды күшейтудің кейбір жалпы стратегияларын ұсына отырып, мақаланың мақсаты – денсаулық сақтау секторындағы киберқауіпсіздік қатерлерінің маңызды мәселесіне жарық түсіру. Зерттеудің жаңалығы – мақалада денсаулық сақтау саласына қатысты киберқауіпсіздік қатерлерінің таксономиялық талдауы ұсынылып, сол қауіптерді түсіну үшін құрылымдық негіз қалыптастырылады, сондай-ақ жаһандық денсаулық сақтаудың киберқауіпсіздігін нығайту бойынша кейбір жалпы ұсыныстар әзірленеді.

Қысқаша қорытындылар: 1) Мемлекеттер демеушілік ететін зиянды кибероперациялар денсаулық сақтау сапасы мен пациенттердің қауіпсіздігіне айтарлықтай қатер туғызуы мүмкін; 2) Денсаулық сақтау саласындағы шешім қабылдау орталықтарына киберқауіпсіздік саясатын жаңғырту қажеттілігіне назар аудару ұсынылады, өйткені зерттеулер көрсеткендей, трансұлттық зиянды кибероперациялардың құрбанына айналатын денсаулық сақтау ұйымдарының саны күннен-күнге өсіп барады.

Түйін сөздер: зиянды кибероперациялар, деректердің құпиялылығы, денсаулыққа құқық, жаһандық денсаулық сақтау, денсаулық сақтау, кибершабуылға төзімділік, денсаулық сақтау инфрақұрылымы, киберқауіпсіздік, киберқауіптердің таксономиясы

Ж.Р. Темирбеков, PhD in Jurisprudence, LLM in International Law, Teaching Professor Maqsut Narikbayev University (г. Астана, Республика Казахстан): **Глобальная безопасность здравоохранения в эпоху транснациональных вредоносных кибероперaций: таксономический анализ негосударственных и поддерживаемых государствами киберугроз.**

В статье подчеркивается опасность киберугроз для глобального здравоохранения. В исследовании объединено изучение количественных и качественных результатов исследований из официальных отчетов, бюллетеней и журналов, с целью продемонстрировать масштабы и последствия негосударственных и поддерживаемых государствами вредоносных

кибероперациий, направленных на системы здравоохранения. В современную цифровую эпоху кибероперации против сектора здравоохранения происходят все чаще и становятся все более изощренными, поэтому статья актуальна. Предмет статьи заключается в том, что анализируя природу, масштабы и последствия вредоносной киберактивности, в статье рассматривается, как такая активность может повлиять на киберсистемы здравоохранения, конфиденциальность данных пациентов и общественное здравоохранение. Анализируя недавние инциденты, проводя таксономический анализ и предлагая некоторые общие стратегии по усилению защиты здравоохранения перед лицом угроз кибербезопасности, статья проливает свет на критически важную проблему угроз кибербезопасности в секторе здравоохранения, что является целью статьи. Новизна исследования заключается в том, что в статье предлагается таксономический анализ угроз кибербезопасности для сферы здравоохранения, который обеспечивает структурированную основу для понимания таких угроз, а также формируются некоторые общие предложения по усилению киберзащиты глобального сектора здравоохранения.

Краткие выводы: 1) Вредоносные кибероперации, поддерживаемые государствами, могут оказывать существенное негативное влияние на качество здравоохранения и безопасность пациентов; 2) Центрам принятия решений в сфере здравоохранения рекомендуется обратить внимание на необходимость модернизации политики кибербезопасности, поскольку, как показывают исследования, все больше организаций здравоохранения становятся жертвами транснациональных вредоносных кибероперациий.

Ключевые слова: вредоносные кибероперации, конфиденциальность данных, право на здоровье, глобальное здравоохранение, здравоохранение, устойчивость к кибератакам, инфраструктура здравоохранения, кибербезопасность, таксономия киберугроз

References:

1. A sophisticated cyber attack resulted in unauthorized access to one of our IT systems. Here's what you need to know. Anthem. 2015. URL: https://www.anthem.com/wisconsin/statement-regarding-cyber-attack-against-anthem/ (accessed: 13.02.2024).
2. Alawida M. and others. A deeper look into cybersecurity issues in the wake of Covid-19: A survey // Journal of King Saud University. Computer and information sciences. 2022. № 10. Pp. 8176-8206.
3. Argaw S. and others. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. British Medical Journal (medical informatics and decision making). 2020. № 1. Pp. 1-146.
4. Bhosale K., Nenova M., Iliev G. A study of cyber attacks: In the healthcare sector // 2021 Sixth Junior Conference on Lighting (Lighting): IEEE, 2021. Pp. 1-6.
5. Bhuyan S. and others. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. Journal of medical systems. 2020. № 5. Pp. 98-98.
6. Bris A., Asri W. State of Cybersecurity & Cyber Threats in Healthcare Organizations. Cergy, France: ESSEC Business School, 2016.
7. California Department of Insurance: Consumer information on Anthem Blue Cross data breach // California Department of Insurance. 2015. URL: https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm (accessed: 09.02.2024).
8. Campbell N. Over 75% of Data Breaches Unreported. Cleaver Fulton Rankin. 2019. URL: https://cleaverfultonrankin.co.uk/legal-update/over-75-of-data-breaches-unreported/ (accessed: 08.02.2024).
9. Cashwell G. Cyber-vulnerabilities & Public Health Emergency Response. Journal of Health Care Law and Policy. 2018. № 1. Pp. 29-58.
10. Clarke M., Martin K. Managing cybersecurity risk in healthcare settings. Health Manage Forum. 2024. № 1. Pp. 17-20.

11. Data Breach Investigations Report: Verizon, 2022. URL: https://www.verizon.com/business/en-au/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir-industries.pdf (accessed: 5.03.2024).

12. Djenna A., Eddine D. Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure // 2018 2nd Cyber Security in Networking Conference (CSNet): IEEE, 2018. Pp. 1-4.

13. Desk D. Cyber attacks are bad for your health. Sunday business post. 2016. URL: https://www.proquest.com/newspapers/cyber-attacks-are-bad-yourhealth/docview/1904871232/se-2?accountid=13460 (accessed: 08.02.2024).

14. Dreyfuss E. As Cyberattacks Destabilize the World, the State Department Turns a Blind Eye. Wired. 2017. URL: https://www.wired.com/story/state-department-cybersecurity/ (accessed: 10.02.2024).

15. Ferrillo P. To over Disclose or Not: That Is the Question with Cybersecurity. Florida State University Business Review. 2021. № 1. Pp. 79-96.

16. Ghafur S. and others. Improving Cyber Security in the NHS. London: Imperial College London, 2019. 38 pp.

17. Ghafur S. and others. A retrospective impact analysis of the WannaCry cyberattack on the NHS // npj Digit. Med. 2019. № 1. Pp. 98.

18. Greenberg A. Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. New York: Doubleday, 2019. 348 Pp.

19. Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed: 19.02.2024).

20. Harkins M., Freed A. The Ransomware Assault on the Healthcare Sector. Journal of Law & Cyber Warfare. 2018. № 2. Pp. 148-164.

21. Investigation: WannaCry cyber attack and the NHS: UK National Audit Office, 2017. URL: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ (accessed: 5.03.2024).

22. Kandasamy K. and others. Digital Healthcare – Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. IEEE access. 2022. № 10. Pp. 12345-12364.

23. Maia E. and others. Security Challenges for the Critical Infrastructures of the Healthcare Sector // Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures / Edn. J. Soldatos, J. Philpot, G. Giunta: Now Publishers, 2020. Pp. 141-165.

24. Martin G. and others. Cybersecurity and healthcare: how safe are we? British Medical Journal (Online). 2017. № 358. PP. j3179-j3179.

25. Mattei T. Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack World Neurosurgery. 2017. № 104. Pp. 972-974.

26. Mayor S. Sixty seconds on ... the WannaCry cyberattack. British Medical Journal. 2018. № 361. Pp. k1750-k1750.

27. Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People. URL: https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including (accessed: 09.02.2024).

28. Morrissey D. Malicious Actors and Medical Data: Where Are We Heading? AT&T Cybersecurity. 2020. URL: https://cybersecurity.att.com/blogs/security-essentials/malicious-actors-and-medical-data-where-are-we-heading (accessed: 08.02.2024).

29. Mrcela M., Vuletic I. Healthcare, Privacy, Big Data and Cybercrime: which one is the weakest link? // Annals of Health Law. 2018. № 2. Pp. 257 – [viii].

30. Mueller R. Director of Federal Bureau of Investigation, RSA Cyber Security Conference. URL: https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (accessed: 13.02.2024).

31. NHS cyber-attack was «launched from North Korea». BBC News. 2017. URL: https://www.bbc.com/news/technology-40297493 (accessed: 19.02.2024).

32. Niki O. and others. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. Digital health. 2022. № 8. Pp.1-3.

33. Peterson A. Connected medical devices: The Internet of things-that-could-kill-you. Washington Post. 2015. URL: https://www.washingtonpost.com/news/the-switch/wp/2015/08/03/connected-medical-devices-the-internet-of-things-that-could-kill-you/ (accessed: 25.02.2024).

34. Razaque A. and others. Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain // IEEE access. 2019. № 7. Pp. 168774-168797.

35. Reuters. U.S. offers $10 mln reward for information on Russian intelligence officers - State Dept // Reuters. 2022. https://www.reuters.com/world/us-offers-10-mln-reward-information-russian-intelligence-officers-state-dept-2022-04-26/ (accessed: 25.02.2024).

36. Russian military 'almost certainly' responsible for destructive 2017 cyber attack. Wired-Gov.2018. URL: https://www.wired-gov.net/wg/news.nsf/articles/Russian+military+almost+certainly+responsible+for+destructive+2017+cyber+attack+16022018091500?open (accessed: 25.02.2024).

37. Satter R., Stubbs J., Bing C. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike. Reuters. 2020. https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN/ (accessed: 08.02.2024).

38. Schmitt M., Biller J. The NotPetya Cyber Operation as a Case Study of International Law // Blog of the European Journal of International Law. 2017. URL: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ (accessed: 20.02.2024).

39. Schmitt M., Fahey S. WannaCry and the International Law of Cyberspace. Just Security. 2017. URL: https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/ (accessed: 10.02.2024).

40. Seebruck R. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. Digital investigation. 2015. № 14. Pp. 36-45.

41. Sengupta K. Isis carried out cyber-attack on NHS sites // Independent. 2017. URL: https://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html (accessed: 10.02.2024).

42. Compromise of the World Anti-Doping Agency // Council on Foreign Relations. 2016. URL: https://www.cfr.org/cyber-operations/compromise-world-anti-doping-agency (accessed: 10.02.2024).

43. Thamer N., Alubady R. A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research // 2021 1st Babylon International Conference on Information Technology and Science (BICITS). Babil, Iraq: IEEE, 2021. Pp. 210-216.

44. Tin D. and others. Cyberthreats: A primer for healthcare professionals. The American Journal of Emergency Medicine. № 68. 2023. Pp. 179-185.

45. Ukraine points finger at Russian security services in recent cyber attack. Reuters. 2017. URL: https://www.reuters.com/article/idUSKBN19M39P/ (accessed: 13.02.2024).

46. US offering $10 million for info on Russian military hackers accused of NotPetya attacks. The Record. 2022. URL: https://therecord.media/notpetya-reward-state-department-10-million-gru-sandworm/ (accessed: 19.02.2024).

47. Wasserman L., Wasserman Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in digital health. 2022. № 4. Pp. 1-20.

48. What is NotPetya? 5 Fast Facts. Security Encyclopedia. https://www.hypr.com/security-encyclopedia/notpetya (accessed: 19.02.2024).

49. Whittaker Z. Justice Department charges Chinese hacker for 2015 Anthem breach. Techcrunch. 2019. URL: https://techcrunch.com/2019/05/09/anthem-breach-indictment/ (accessed: 13.02.2024).

50. Wild A. The Anthem and Premera data breaches put the healthcare industry on notice: you are a target. Database and network journal. 2015. № 2. Pp. 15+.
51. Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. Los Angeles Times. 2016. URL: https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html (accessed: 08.02.2024).
52. Zetter K. What Is Ransomware? A Guide to the Latest Global Cyberattack. Wired. 2017. URL: https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ (accessed: 09.02.2024).

Для цитирования и библиографии: Temirbekov Zh. Global Health Security in the Age of Transnational Malicious Cyber Operations: A Taxonomic Analysis of Non-State and State-Backed Cyber Threats // Право и государство. № 2(103), 2024. – С. 6-17. DOI: 10.51634/2307-5201_2024_2_6

Материал поступил в редакцию 11.04.2024.