Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Exploring the dynamics between artificial intelligence and cybersecurity in Healthcare

António Tavares [a], Pedro Sousa [b]*, Rita Proença [c]

[a] *Professor, Universidade Lusófona – CUP, Porto, Portugal*

[b] *IT Director, Santa Casa da Misericórdia do Porto, Portugal*

[c] *PhD, Santa Casa da Misericórdia do Porto, Portugal*

[a] *Email: tavares.aml@gmail.com*

[b] *Email: pedro.sousa@scmp.pt*

[c] *Email: rita.proenca@scmp.pt*

Abstract

Technology changed the world over the past decades, reinventing the way we work, communicate, and live. In the healthcare sector, it has contributed to driving innovations in the diagnosis process, treatment, data management, and information access. However, this transformation has been accompanied by an increasing dependence on digital systems and connectivity. Nowadays, concepts such as artificial intelligence and cybersecurity are widely recognized, but organizations just became aware of the benefits and risks involved. In fact, the nature of their relationship it is still under discussion.

The central objective of this study is to explore the dynamics of this relationship in healthcare, taken as a sector undergoing constant technological evolution. We propose a dual approach, encompassing both strategic and operational perspectives, which can support the management of this complex interaction, balancing security and innovation.

Keywords: *cybersecurity; artificial intelligence; ambidexterity; security awareness; cyberattacks; healthcare sector*

Citation: A. Tavares, P. Sousa, and R. Proenca, "Exploring the dynamics between artificial intelligence and cybersecurity in Healthcare", *ARIS2-Journal*, vol. 4, no. 1, pp. 20–34, Apr. 2024.

DOI: https://doi.org/10.56394/aris2.v4i1.44

---

* Corresponding author. Email address: pedro.sousa@scmp.pt

1. Introduction

Joseph Schumpeter, in 1942, developed the theory of "creative destruction," suggesting that economic cycles operate in long waves of innovation. Since the first wave in 1785, with the industrial revolution, we have witnessed a series of revolutions such as steam engines, the automotive industry, electronic components, aviation, and personal computing. Since the mid-20th century, in the context of the so-called Fourth Industrial Revolution, with the advent of the internet, virtual and physical systems of manufacturing changed how we communicate and how markets operate. All revolutions create benefits, opportunities and new paths, but also uncertainties and challenges. Artificial Intelligence made significant advances from 2000 onwards, fostering a digital era. Nevertheless, all artificial intelligence models meet cybersecurity, given potential attacks. As the technological revolution gained momentum, especially with computational capabilities and the expansion of the internet, cybersecurity continued to evolve, becoming increasingly crucial for the survival and sustainability of organizations.

The term cybersecurity refers to the set of technologies and processes to protect and defend information assets, networks, devices, and data from potential digital attacks, damage, or unauthorized access [1-2]. The challenges posed to cybersecurity are becoming more complex, as the number of devices connected to the Internet, around 15.1 billion in 2023, could almost exponentially increase to over 29 billion devices by 2030 [3]. Clearly, the larger the number of digital assets, the more information generated, and undoubtedly, the higher the vulnerabilities and the level of risk. Therefore, considering the rapid technological evolution we are witnessing, it becomes increasingly necessary to ensure the implementation of dynamic, cyclical, and adaptable cybersecurity processes and practices to defend assets. Cybersecurity emerges as a topic of significant importance in the healthcare sector, where all generated information, of immense sensitivity, needs protection against cyber threats. The growing complexity and continuous evolution of cybersecurity in this sector also make it the target of higher levels of concern. Hospitals need to be increasingly prepared to handle the daily challenges of cyber threats, invest in the empowerment of their technicians, train and raise awareness among their teams, and equip themselves with technology, processes, and procedures to respond to incidents that may arise.

The increasing digitization of the healthcare sector not only optimizes processes but also exposes organizations to constantly evolving cyber threats. The use of medical devices has resulted in a larger volume of information, much of which is critical and sensitive; examples include electronic medical records, diagnostic information, personal identification, payment, access credentials to application systems, among others. This volume of information has two aspects: one that is essential to ensure the functioning of hospitals and another that is valuable

to hackers, as it can enable identity theft, financial fraud, black market sales, access to critical systems, and mainly serve as a basis for extortion and ransomware crimes. Furthermore, the digitization of processes in the healthcare sector amplifies dependence on digital infrastructures, making organizations more vulnerable to threats. The complexity of interconnected medical systems requires the implementation of robust security measures, such as data encryption, access management and control, among others. Thus, the need to protect sensitive data and the pressure to maintain service continuity in critical situations pose unique challenges to organizations operating in the healthcare sector.

In turn, artificial intelligence, playing a transformative role in healthcare, can be defined as a set of machines capable of performing cognitive processes similar to humans, such as learning, understanding, reasoning, and interaction. In relation to cybersecurity, as the practice to protect the availability, integrity, and confidentiality of information and information systems, artificial intelligence is used to enhance data analysis and behavior patterns to prevent attacks and detect threats. In this context, this article aims to explore the relationship between cybersecurity and artificial intelligence from a theoretical perspective and complement this relationship with a more practical and management-oriented approach, incorporating the practice of cybersecurity risk management. The article is organized as follows: the first part presents a brief literature review of cybersecurity and artificial intelligence, addressing the main challenges for the healthcare sector. In the second part, a dual approach to the dynamics between artificial intelligence and cybersecurity is presented, working on both the strategic and operational perspectives in a logic of complementarity. Finally, the main conclusions are provided.

2. Theoretical Background

2.1 Cybersecurity

The concepts of Cybersecurity and Information Security are often used interchangeably, but they are not the same: while Information Security is intended to protect information assets against unauthorized access in a broader sense, Cybersecurity ensures the protection of information and communication networks against attacks or threats that may arise from the network or cyberspace [4:18]. On the other hand, cybercrime involves criminal activities that use information technology as a means to commit offenses. Both Information Security and Cybersecurity are widely connected to the concepts of confidentiality, integrity, and availability, or the CIA triad, referring to the key elements of information security:

- Confidentiality: assurance that information is accessible only to those authorized to view it;
- Integrity: assurance that information has not been altered by unauthorized individuals and remains accurate and reliable;
- Availability: assurance that information is available when needed.

The origin of the CIA triad is intertwined with studies in military security, initially stemming from the "RAND report R-609, Security Controls Systems" [5] and the 1972 "Computer Security Technology Planning" by the U.S. Air Force [6]. The primary goal of these studies was to ensure the protection of military or governmental information [7], [8]. Simultaneously, the scientific community began delving into the security domain, especially following the seminal article by Saltzer and Schroeder advocating that the primary objective of security should be

the protection of information housed in the computer, not the computer itself [9]. According to Ham [10] the triad still faces an issue – it has a binary measure (true or false), which is counterproductive for risk management methodology that also analyzes the context. Additionally, the triad was established at a time when the internet did not yet exist, so considering the significant changes in context, a reevaluation of this approach is deemed necessary [10]. Over time, other concepts such as authenticity, non-repudiation, specification correctness, responsibility, integrity of individuals, trust, ethics, and identity management have been introduced, all somehow interconnected with the initial dimensions of the CIA triad [8].

In the not-so-distant past, cybersecurity primarily involved ensuring the presence of updated antivirus software and that user accounts had passwords. However, user awareness was crucial, emphasizing the avoidance of interactions with suspicious emails, which were often vehicles for phishing attempts. Currently, threat detection has become more sophisticated, with measures providing greater protection for user accounts, such as two-factor authentication (MFA), and more robust measures safeguarding networks. Alongside progress in security, threats evolve efficiently and covertly, establishing a paradigm of continuous evolution and adaptation.

Healthcare organizations are more vulnerable to these changes for two main reasons [11]. Firstly, the evolution of security systems does not keep pace with the speed at which new technologies emerge and are implemented. Secondly, in the case of the United States, policies are being defined to promote increased technology utilization. However, as a result, healthcare organizations are becoming increasingly dependent on networks and directing budgets toward new projects, leaving little room to invest in security programs [11]. In this line of reasoning, and in order to address the challenges related to the access and sharing of electronic health data, the European Commission has proposed the EHDS (European Health Data Space). This framework consists of common procedures and practices and a governance framework with the aim of establishing a shared space where individuals can control their clinical information. The EHDS intends to facilitate the sharing of clinical information among Member States, support research and development, and ultimately build a digital space where health data can be used and shared in compliance with security standards [39]. Therefore, it is essential to delve into the concept of threats – actions carried out by individuals, groups, or countries in the digital environment with the goal of compromising, disrupting, or gaining unauthorized access to computer systems, networks, or electronic devices.

Cyber- attacks can be subdivided into two categories: active or passive. In an active attack, the attacker attempts to alter or destroy the normal operation of the system or network, while in a passive attack, attackers try to use or gain information from the system without affecting the system's resources [12]. In terms of threat categories, there are several, including ransomware, denial-of-service (DoS) / distributed denial-of-service (DDoS) attacks, phishing, vulnerability exploitation, man-in-the-middle attacks, social engineering, among others. The following stand out:

- Ransomware: A type of malware that encrypts files on a system, preventing the user from accessing their own data. Cybercriminals then demand payment of a ransom, usually in cryptocurrencies, to provide the key and restore access to the files. An example is the attack on Hospital Garcia da Orta in Portugal in 2022, which resulted in the cancellation of appointments, surgeries, and exams, and required the manual recording of all

information.

- Phishing: An attack technique that involves attempting to deceive users into revealing confidential information, such as passwords, credit card information, or login details. This is often done through fraudulent messages, emails, fake websites, or other online communication forms that impersonate trusted sources. An example is Kaleida Health, one of the largest healthcare providers in the U.S., which was attacked multiple times in 2017, with attackers gaining access to personal information and clinical records.
- Distributed Denial-of-Service (DDoS) Attacks: Refers to a malicious attempt to overload an online service, network, or system, making it inaccessible to users. The main objective is to overwhelm the target system's resources, such as bandwidth, processing capacity, or connections, leading to service disruption. In 2022, the Killnet group (pro-Russia hackers) attacked a set of hospitals and healthcare centers in the U.S., following this type of threat.
- Man-in-the-Middle (MITM) Attacks: Attacks in which an intruder intercepts or manipulates communication between two parties without their knowledge. The attacker can read, alter, or inject new data into the communication. This can occur in public or private networks, and MITM attacks can take various forms, such as intercepting wireless communications, DNS spoofing attacks (modifying the source or destination address and redirecting traffic to malicious sites), among others.
- Network Vulnerability Attacks: Exploitation of security flaws in network systems. These vulnerabilities may allow attackers to gain unauthorized access to systems, execute malicious code, modify configurations, or perform other harmful activities.

According to the report from the European Union Agency for Cybersecurity (ENISA) in 2023, 31.32% of attacks are ransomware, followed by 21.4% for DDoS, and 20.09% correspond to threats against data. The most attacked sector is the public administration (19%), followed by individuals (11%) and the healthcare sector (8%) [13]. In Portugal, data from the National Cybersecurity Center (CNCS) for 2022 states that 11% of notifications received are from the healthcare sector, with a 74% increase in incidents compared to 2021. While confidentiality is the most compromised principle in incidents, the main origin of data breaches was ransomware, followed by human error and application failures [14].

In the current context of technological innovation and the increasing likelihood of threats, it becomes even more crucial for organizations to incorporate risk management practices and tools. These risks, referred to as cyber risks, involve the probability of financial losses, damage to reputation, operational disruption, or other negative impacts resulting from cyber threats. They can also be defined as operational risks whose consequences affect the CIA triad for information or information systems [15]. In the "Global Risks 2023" report by the World Economic Forum [16], the risk of cybercrime and cybersecurity is ranked eighth in both short and long-term perspectives. This places it in a list led by crises in the cost of living, climate change, among other factors. In terms of impact, it surpasses crises such as unemployment, deterioration of mental health, or terrorist attacks. It is indeed an area that demands attention and development and is applicable to all sectors, with healthcare being no exception. The evolution of the COVID-19 pandemic has demonstrated the interdependence between health risks and cybersecurity risks. The rapid adoption of new digital technologies, while creating significant value and enabling a stronger innovation process, has also paved the way for the collection and sharing of more personal information,

infrastructure, and supply chain data [17].

The information generated by the healthcare sector is valuable, encompassing personal information, financial data, and more, making it a prime target for attackers [11], [18]. In this context, the level of connectivity and complexity of hospital infrastructure is so vast that it enables attackers to exploit vulnerabilities at many entry points [19], [20]. The compromise of this data carries high consequences, potentially resulting in financial losses, identity theft, damage to systems and infrastructure, reputational loss, business disruption, and negative impacts on the diagnosis and treatment processes for patients, as attackers may manipulate or destroy essential clinical information. According to Pointer [21], there are over 1 billion health records of patients available on the dark web (a part of the online content not indexed by conventional search engines and generally not accessible through standard browsers), and more records are being added every day.

In the face of this exponential increase in threats, artificial intelligence can play a significant role in enhancing the protection and security of healthcare data. The ability of artificial intelligence to detect suspicious activities, prevent cyber-attacks, and strengthen defenses against vulnerabilities is transforming cybersecurity from manual and routine work to an automated and streamlined process.

2.2 Artificial Intelligence

The Father of Artificial Intelligence is often considered to be John McCarthy. In 1955, during the Dartmouth Conference, the author introduced the term "artificial intelligence," which became central to describing this field of study and research aimed at creating machines capable of performing tasks. Also noteworthy is Alan Turing, who addressed the concept in the paper "Computing Machinery and Intelligence" (1950), where he proposed what became known as the "Turing Test." This approach sought to determine if a machine could exhibit intelligent behavior indistinguishable from human behavior. In the 1970s, expert systems emerged at Stanford University, such as Dendral (a system for molecular structure analysis) and MYCIN (for medical diagnosis, particularly in identifying and treating bacterial infections). A widely known example is Deep Blue, the artificial intelligence system that defeated the world chess champion, Garry Kasparov, in 1997.

The inherent nature of the concept of artificial intelligence is challenging to define, but generally, it can be described as a set of algorithms and systems capable of performing tasks that would typically require human intelligence, such as learning, reasoning, and language understanding. It is assumed that human intelligence can be accurately described and, therefore, can be replicated through machines [22], [23], [24]. Some artificial intelligence techniques include Machine Learning, Deep Learning, Natural Language Processing, Computer Vision, among others. One of the most important pillars is Machine Learning, which focuses on developing algorithms and models that enable systems to learn from a very large set of data. Unlike in the past when machines were programmed to perform a specific task, Machine Learning (ML) systems use data to train, learn, and perform tasks without direct human intervention. Another crucial concept is Deep Learning (DL), which employs deep neural networks to carry out complex learning and pattern recognition tasks. The difference between the two is that while ML is a broader approach and sometimes requires manual extraction of relevant features from the data,

DL specifically focuses on the use of deep neural networks and is autonomous in learning [25].

Currently, the term "artificial intelligence" has permeated across all sectors, research areas, and themes; opinions are divided regarding the risks, how it is implemented, the need for regulation, and the limits of its use. However, it is unanimous that artificial intelligence has come to change the world at an exponential rate, marking the present as the fourth industrial revolution characterized as a set of technologies that are blurring the boundaries between the physical, digital, and biological worlds. Therefore, the fundamental question that must be addressed is how to better prepare organizations to harness its benefits [16].

In the healthcare sector, the contribution of artificial intelligence is immeasurable, presenting possibilities, for example, in the diagnosis, early detection of diseases, customization of treatments, improvement of operational efficiency in hospitals and health centers, research and development, or the creation of simulations for healthcare professional training. According to Secinaro *et al.* [26] artificial intelligence in healthcare has four dominant areas: predictive medicine, patient data and diagnosis, clinical decision-making process, and healthcare service management. In the case of healthcare service management, it includes the possibility for healthcare professionals and managers to stay updated in terms of research and development, contribute to more efficient logistic systems, train and empower employees, and handle the volume of available information [26]. Regarding diagnostic practices, ML systems can support the decision-making process – an example is a study that introduced a large number of mammograms into an artificial intelligence system to support breast cancer diagnosis. The results show a reduction of 5.7% in the U.S. and 1.2% in the U.K. in false positives and 9.4% in the U.S. and 2.7% in the U.K. [27], [28]. Another study compares artificial intelligence in the analysis of prostate cancer diagnosis through magnetic resonance imaging, and the results do not find sufficient evidence but emphasize the need for access to larger and more diverse databases to progress more rapidly in this area [29]. In the area of diagnosis, although DL algorithms show significant potential, there is still not enough knowledge about the accuracy level in diagnosis. For example, a study evaluating the accuracy in nearly 12,000 studies found that in the case of glaucoma studies, seventeen studies reported diagnostic accuracy for suspected glaucoma in retinal photographs and a set of one hundred and fifteen studies with 244 separate patients reported accuracy with DL for respiratory disease [30].

It is also important to consider the potential contribution of artificial intelligence to the process of optimizing drug doses and regularly monitoring the concentration of these drugs in the body. An example is the CURATE.AI system, a platform that dynamically optimizes chemotherapy doses based on individual patient data, with the goal of maximizing treatment effectiveness while minimizing side effects [28].

In parallel with technological advancements, macroeconomic conditions and the aging of the global population are also pushing healthcare systems to provide more innovative, personalized, and patient-centric solutions. Artificial intelligence systems enable virtual medical consultations, remote patient monitoring, and the implementation of applications that can triage patients. To address the needs of an aging population, there are already systems aimed at promoting autonomy (medication management and fall detection), preventing situations of isolation and mental health issues, and monitoring chronic diseases. However, although artificial intelligence is indeed a transformative tool, it also presents significant challenges in terms of ethics, privacy, data security, transparency, equity, competition with potential impacts on the job market. When exploring the potential of

machine learning (ML), it's crucial to remember that the quality, reliability, and effectiveness of these models are linked to the quality of the data they were trained on. In other words, there is a possibility that models are being constructed based on incorrect, discriminatory, or biased information. A notable example is a 2017 study on three commercial gender classification systems (IBM, Microsoft, and Face+++) that found an error rate of 34.7% for Black women and 0.8% for White men. These results illustrate that ML algorithms can discriminate based on factors such as race or gender [31]. The UNESCO report [32] also highlights gender bias in artificial intelligence databases, raising concerns about ensuring the non-dissemination of gender discrimination. Another challenge of artificial intelligence is the issue of transparency—many artificial intelligence algorithms, especially in deep learning (DL), act as black boxes, making interpretation difficult and raising questions about full trust. For example, in healthcare, how do doctors explain the reasons behind a particular diagnosis to patients? [33].

Regarding data security and protection, the challenges are substantial. The use of sensitive data to train artificial intelligence models implies safeguarding this information, ensuring compliance with data protection regulations, and investing in cybersecurity. However, the relationship between these two concepts is not without tensions or paradoxes. It operates in a constant dynamic state, under continuous pressure for security systems to keep pace with technological advancements and ensure the security levels demanded by data and systems.

3. Integrating AI and Cybersecurity: Strategic and Operational Perspectives

The technological evolution of the last 20 years has changed the way we work and communicate, bringing numerous advantages such as increased operational efficiency, democratization of access to information, a boost in innovation and the development of new products/services, advancements in medicine, economic growth, and the protection of people and data, among others. However, it also presents challenges. The growing complexity of networks can provide more opportunities for cyber-attacks, cyber espionage activities, may widen digital inequalities, and increases society's dependence on technology, making any failure potentially have serious impacts on services.

On the one hand, artificial intelligence serves as a shield for organizations, supporting monitoring processes, real-time analysis of large volumes of data, and defense against cybersecurity incidents. On the other hand, it is a sword, as attackers also use artificial intelligence to refine their processes. This duality is well-known—the importance of technological innovation and the need to ensure the security of assets against cyber threats. However, this complementary and inseparable relationship also poses challenges. Organizations must strike a balance between promoting technological advancements and adopting artificial intelligence without compromising the integrity and protection of data—thus promoting sustainable evolution.

Applying this line of reasoning to the healthcare sector is particularly important. Firstly, because the type of information collected and shared is very sensitive and, consequently, highly valuable. While sharing information among healthcare professionals has numerous benefits, it also places greater demands on organizations to ensure the protection of this information. Secondly, innovation in the sector has yielded more precise diagnoses, personalized treatments, and improvements in care delivery, but it is crucial to implement security practices to ensure the reliability of these technological advancements. Thirdly, remote monitoring solutions enable patient tracking but also increase privacy risks. In any of these situations, technological dependence is so significant that

a failure in an emergency situation can have impacts on human life.

This relationship cannot be addressed solely through a strategic lens; it is essential to cascade it into operational aspects, emphasizing immediate action and fostering an organizational culture focused on data security.

3.1 Strategic Approach

According to Charles Darwin (1850), whose theory of evolution by natural selection became seminal, it is not the strongest or the most intelligent that survives, but the one that adapts best to change. One can thus look at organizations through the same lens and state that it is not the strongest or the most competitive that survives, but those that adapt better, emphasizing the importance of flexibility and the ability to adjust to the constantly changing environment. In the current context, characterized mainly by technological developments, organizations that only focus on current processes and do not prepare for transformations do not adapt and are surpassed. It is in this field that the concept of ambidexterity emerges, as the need to manage conflicting activities, such as alignment and flexibility or incremental/radical innovation.

Organizational ambidexterity can be defined as the ability of organizations to simultaneously seek incremental and radical innovation [34: 24] or the ability of an organization to be efficient and aligned while also being adaptable to changes in the external environment [35: 375]. In the context of information systems, ambidexterity is defined as the ability to innovate and explore IT resources while simultaneously ensuring their routinization and efficiency [36]. From this arises the ambidexterity of artificial intelligence, defined as the organization's ability to ensure the standardization of artificial intelligence routines and processes and, at the same time, implement new, more creative, and innovative processes [37]. Regardless of the sector or approach, ambidexterity results from a balance between activities or processes that are contradictory but complementary. It can be argued that it is not necessarily the guarantee of balance that makes organizations adapt, but rather the result of imbalances created by external changes.

Currently, organizations face the challenge of dealing with these levels of technological evolution, having to balance the management of artificial intelligence routines with the search for models capable of driving innovation. Additionally, promoting the security of their assets becomes increasingly important. Thus, the dynamics between artificial intelligence and cybersecurity translate into an interconnected model that moves and induces movement – for this, largely inspired, applying the metaphor of the operation of gears (Figure 1). From a physics standpoint, the mechanical device consists of two or more interconnected toothed wheels that transmit a rotational movement between them. Each wheel has teeth protruding from its circumference, designed in a specific way to mesh with the teeth of the other wheel, allowing efficient transfer of movement. When the two toothed wheels are in contact, the teeth of one wheel fit into the spaces between the teeth of the other wheel, and this precise fit is crucial to ensuring the efficient transmission of movement without slipping or energy loss.

When this concept is applied to the analysis of the dynamics between artificial intelligence and cybersecurity, and from the perspective of the major innovations in healthcare, it can be stated that artificial intelligence is the driving gear. It represents the driving force in the relationship, exhibiting ambidexterity between routine execution

and innovation implementation. In the case of cybersecurity, as the driven gear, it is influenced by the movement of artificial intelligence and represents the adaptation of processes and practices to ensure system protection.

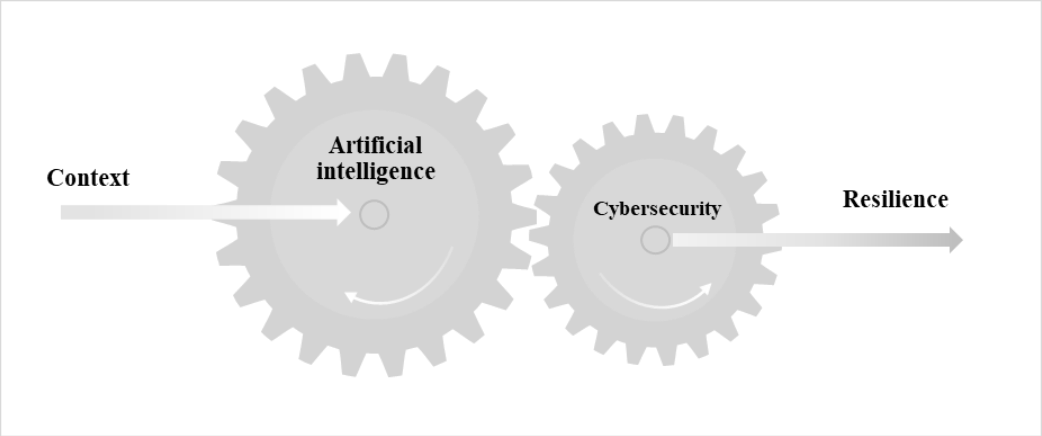

Figure 1 - Dynamics between artificial intelligence and Cybersecurity (Developed by the authors)

In practice, what happens is that when the artificial intelligence gear starts to turn, driven by the pursuit of balance between managing routines and implementing innovative models, it becomes the driving force of the dynamics. In this scenario, cybersecurity responds to the movement of artificial intelligence, continuously adapting to ensure the security of data and systems. Similar to mechanical devices, the interaction between artificial intelligence and cybersecurity is crucial to ensure efficient transfer of movement, energy, and force multiplication, essential for addressing current technological challenges and promoting secure innovations in healthcare.

The efficient and smooth operation of the system depends on regular maintenance. In other words, both artificial intelligence and cybersecurity require continuous updates and adjustments to face new threats and ensure effectiveness. Another important aspect of the system is the size of the wheels – it is considered that the size of the artificial intelligence wheel is larger, as the pace of innovation and advancement in artificial intelligence is faster or more comprehensive than the capacity of cybersecurity to adapt and protect. The larger the artificial intelligence wheel, for every complete turn it makes, the cybersecurity wheel has to complete two turns. The speed at which artificial intelligence can process large amounts of data and make complex decisions is comparable to the speed at which the driving gear transfers energy to the driven gear. This requires cybersecurity to respond faster, ensuring the protection of today's data while simultaneously adapting to the new challenges of artificial intelligence.

From the perspective of a mechanical device, this dynamic is not without risks. The risk of misalignment is an example. If artificial intelligence advances rapidly in innovation, but cybersecurity cannot keep up, it can result in security risks. Another example is information overload – if artificial intelligence generates an excessive amount of data that cybersecurity cannot efficiently process, it may lead to failures in threat detection. Risks associated with managing ambidexterity are also mentioned. Regardless of the paradoxes under study, overemphasizing one of them implies risks for organizations. In the case at hand, if the organization promotes

only artificial intelligence without investing in cybersecurity, it increases vulnerabilities, facing higher risks of attacks. However, cybersecurity cannot be the ultimate goal of the process either, risking making the organization inert and less technologically advanced.

3.2 Operational Approach

From an operational standpoint, the exploration of the balance between artificial intelligence and cybersecurity can be analyzed across six dimensions, with 16 subtopics intertwining the two areas in operational terms (Figure 2). This classification is conceptual, applicable across any sector of activity, and generic enough to be shaped and adjusted to align with the context of each organization.

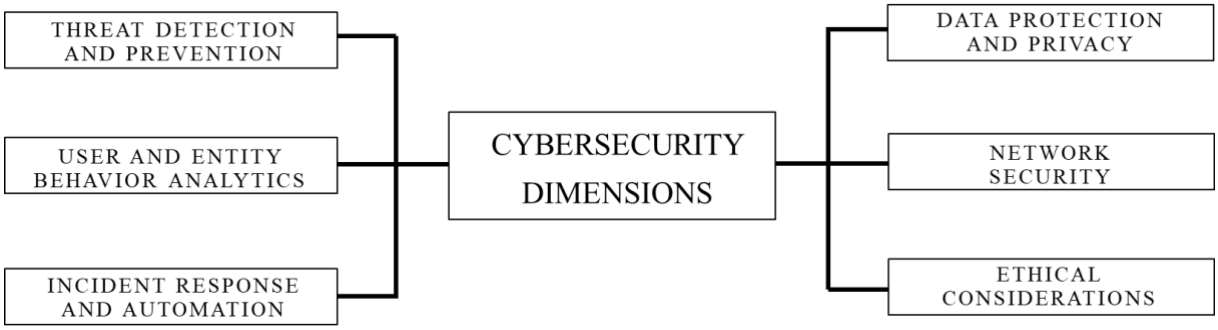

Figure 2 - Cybersecurity Dimensions (Developed by the authors)

The first dimension - *Threat detection and prevention* correspond to the set of practices and processes aimed at preventing, identifying, and/or addressing potential cybersecurity threats. These include Anomaly Detection processes, Malware Detection, and IDPS (Intrusion Detection and Prevention Systems), increasingly driven by artificial intelligence algorithms in the analysis of network traffic, malware detection, and attack prevention. While artificial intelligence support enhances the efficiency of these processes, the risks are associated with the growing sophistication of attacks. In the healthcare sector, these processes are crucial for detecting unauthorized access attempts to clinical processes and preventing ransomware attacks. The second dimension - *User and Entity Behavior Analytics* - focuses on monitoring and analyzing the behavior of users, devices, applications, and servers within a network context. This includes processes such as Behavioral Analytics, Phishing Detection, and Access Control and Authentication, supported by artificial intelligence algorithms for behavioral analysis, phishing detection, and access controls. In healthcare, these processes may involve detecting anomalous behaviors in accessing patient records and implementing preventive actions against potential internal threats.

In the case of the third dimension, *Incident Response and Automation*, it deals with the entire process of planning, coordinating, and executing responses to security incidents. This includes, for example, artificial intelligence systems that continuously monitor the network, system logs to search for anomalies, and automate incident responses. Processes such as Automated Threat Response, Security Orchestration, and Incident Response Automation are encompassed in this dimension. The ongoing evolution of artificial intelligence also introduces risks, such as rapidly spreading malware that adapts to artificial intelligence -based defenses. It is essential to recognize that a cyber-attack inevitably becomes a reality; therefore, post-incident response is crucial to ensuring the continuity of hospital operations. An effective preparation and the execution of tested procedures is essential.

It is important to have implemented procedures and security measures to safeguard data and systems, including proper backup procedures, provision of redundant equipment, and swift recovery in the event of a computer failure. The necessary investment, though challenging, is crucial, especially in ensuring system redundancy, whether hosted in the cloud or offline sites. The formation of a multidisciplinary incident response team is critical, involving top management, IT and cybersecurity teams, legal experts, and a communication team to coordinate response efforts, minimize damage, and recover in the shortest possible time frame.

The *Data Protection and Privacy* focuses on safeguarding sensitive information. artificial intelligence is applied in sub-dimensions such as encryption/tokenization, Data Loss Prevention (DLP), and compliance monitoring. These measures protect against data breaches, unauthorized access, and ensure compliance with privacy regulations. Once again, while the continuous evolution of artificial intelligence enhances security measures, risks also evolve, potentially leading to more sophisticated attacks. In the healthcare sector, examples include the application of encryption in clinical processes and monitoring compliance with industry privacy standards. In the case of Network Security, it pertains to processes involving the use of artificial intelligence for dynamic network segmentation and intrusion detection systems. Artificial intelligence adapts network structures and detects intrusions, safeguarding vulnerabilities and potential attacks, such as the man-in-the-middle. In this dimension as well, the evolution of artificial intelligence can lead to more complex attacks. Finally, ethical considerations ensure that the artificial intelligence implementation process considers aspects such as transparency, fairness, and impartiality.

4. Conclusion

Healthcare organizations do not operate in silos or islands; they increasingly function in interconnected environments, establishing growing relationships with various entities and stakeholders. This results in a significant increase in the volume of information generated and shared within a hospital, far exceeding what it was in the past. The exponential proliferation of digitally-based technologies interconnected in hospital networks also contributes to the rise in vulnerabilities. In a hospital, as in other organizations, the more equipment and information, the greater is the need for protective measures. It's noteworthy that a cyber-attack can compromise and even interrupt healthcare activities, potentially becoming life-threatening for patients. In the future, threats will not cease to exist; they will diversify and be proportional to technological evolution. Alongside reaping the benefits of artificial intelligence and innovation, organizations must ensure a proactive, adaptive, and security-centered role.

The management of cybersecurity should be viewed as a continuous activity, enabling organizations to better adapt to developments, ensuring that security solutions are not centered on a reactive response or directed at individual assets, but rather on monitoring and anticipating threats [7], [19]. The level of cybersecurity maturity in the healthcare sector is still low compared to other industries, possibly due to limited resources, lack of awareness and training for employees, or the complexity of healthcare systems [38].

The coexistence of artificial intelligence and cybersecurity is not easy; it involves trade-offs that organizations need to manage, primarily through two perspectives. First, the strategic perspective must guide the organization's future path, promoting the creation of a resilient organization capable of adapting to the current evolution by

balancing innovation and routine, accompanied by security processes and practices. Second, the operational perspective ensures that the ambidextrous management of this relationship is translated into operational processes. The relationship between artificial intelligence and cybersecurity has a dynamic nature, involving movement and the transfer of energy, elements that do not stop – especially in the context of the healthcare sector. The challenge is to maintain an ambidextrous approach that allows the organization to take advantage of the opportunities offered by artificial intelligence while actively protecting its assets.

5. References

[1] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," *Information Fusion*, vol. 97, p. 101804, 2023. [Online]. Available: https://doi.org/10.1016/j.inffus.2023.101804.

[2] D. Kim and M. G. Solomon, *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning, 2021.

[3] Statista, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030," [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. [Jan.,11, 2024].

[4] B. G. Raggad, *Information security management: Concepts and practice*. New York: CRC Press, 2010.

[5] W. H. Ware, "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security," RAND Corporation, R-609-1, 1970.

[6] J. P. Anderson, "Computer Security Technology Planning Study". U.S. Air Force. 1972.

[7] J. Van der Ham, "Towards a better understanding of 'Cybersecurity,'" *Digital Threats: Research and Practice*, vol. 2, no. 3, 2021. [Online]. Available: https://doi.org/10.1145/3442445.

[8] S. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security," *Journal of Information System Security*, 2014.

[9] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308, 1975.

[10] J. Van der Ham, "Towards a better understanding of 'Cybersecurity,'" *Digital Threats: Research and Practice*, vol. 2, no. 3, 2021. [Online]. Available: https://doi.org/10.1145/3442445.

[11] C. S. Kruse, B. Frederick, T. Jacobson and D.K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, n.º. 1, pp. 1–10, 2017. [Online]. Available: https://doi.org/10.3233/thc-161263

[12] Y. Liang, H. V. Poor, and S. Shamai, *Information theoretic security*. Now Publishers Inc, 2009.

[13] European Union Agency for Cybersecurity, "Threat Landscape 2023,".2023 [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. [Jan. 16, 2024]

[14] Centro Nacional de Cibersegurança. "Relatório Riscos e Conflitos 2022".2023. [online] Available: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf [Jan. 16, 2024]

[15] J. J. Cebula and L. R. Young, "A Taxonomy of Operational Cyber Security Risks," Carnegie Mellon University – Software Engineering Institute. 2014.

[16] World Economic Forum, "The Global Risks Report 2023," [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf. [Jan. 17, 2024].

[17] A. Garcia-Perez, J. G. Cegarra-Navarro, M.P. Sallos, E.Martineza-Caro and A.Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol. 121, 102583, 2022. [Online]. Available: https://doi.org/10.1016/j.technovation.2022.102583.

[18] S. M. Altowaijri, "An architecture to improve the security of cloud computing in the healthcare sector," in *Smart Infrastructure and Applications*, pp. 249–266, 2020.

[19] D. M. Javaid, A.Haleem,R.P. Singh and R.Suman. "Towards insighting Cybersecurity for Healthcare domains: A comprehensive review of recent practices and trends", *Cyber Security and Applications*, vol. 1(100016), 2023. [Online]. Available: https://doi.org/10.1016/j.csa.2023.100016.

[20] M. Zubair, A. Ghubaish, D. Unal, A. Al-Ali, T. Reimann, G. Alinier, M. Hammoudeh, J. Qadir, "Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System," *Sensors*, vol. 22, p. 8280, 2022. DOI: 10.3390/s22218280.

[21] I. Pointer, "The rise of telemedicine: how to mitigate potential fraud", *Computer Fraud & Security*, 2020, pp. 6–8.

[22] J. H. Fetzer, *Artificial Intelligence: Its Scope and Limits*, (Studies in Cognitive Systems, vol. 4). Springer, 1990

[23] S. D. Tagliaferri, M.Angelova, X. Zhao, P.J.Owen, C.T. Miller, T.Wilkin and D.L.Belavy, "Artificial intelligence to improve back pain outcomes and lessons learnt from clinical classification approaches: three systematic reviews," *Npj Digital Medicine*, vol. 3, no. 1, 2020.

[24] A. J. G. de Azambuja, C.Plesker, Schützer and R.Anderl, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," *Electronics*, 12 (8):1920, 2023. [Online]. Available: https://doi.org/10.3390/electronics12081920

[25] P. Meyer, V. Noblet, C. Mazzara, and A. Lallement, "Survey on deep learning for radiotherapy," Computers in Biology and Medicine, vol. 98, pp. 126–146, Jul. 2018, [Online]. Available: https://doi.org/10.1016/j.compbiomed.2018.05.018.

[26] S. Secinaro, D. Calandra, A. Secinaro, V. Muthurangu, and P. Biancone, "The role of artificial intelligence in healthcare: a structured literature review," BMC Medical Informatics and Decision Making, vol. 21, no. 1, Apr. 2021, [Online]. Available: https://doi.org/10.1186/s12911-021-01488-9.

[27] S. M. McKinney, M. Sieniek, V. Godbole, J. Godwin, N. Antropova, H. Ashrafian, T. Back, M. Chesus, G. S. Corrado, A. Darzi, M. Etemadi, F. Garcia-Vicente, F. J. Gilbert, M. Halling-Brown, D. Hassabis, S. Jansen, A. Karthikesalingam, C. J. Kelly, D. King, J. R. Ledsam, *et al*., "International evaluation of an AI system for breast cancer screening,"*Nature*, vol. 577, no. 7788, pp. 89–94, 2020. [Online]. Available: https://doi.org/10.1038/s41586-019-1799-6.

[28] S. A. Alowais, S. S. Alghamdi, N. Alsuhebany, T. Alqahtani, A. Alshaya, S. N. Almohareb, A. Aldairem, M. Alrashed, K. B. Saleh, H. A. Badreldin, M. S. A. Yami, S. A. Harbi, A. Albekairy, "Revolutionizing healthcare: the role of artificial intelligence in clinical practice," *BMC Medical Education*, vol. 23, no. 1, 2023. [Online]. Available: https://doi.org/10.1186/s12909-023-04698-z.

[29] T. Syer, P. Mehta, M. Antonelli, S. Mallett, D. Atkinson, S. Ourselin, S. Punwani, "Artificial Intelligence Compared to Radiologists for the Initial Diagnosis of Prostate Cancer on Magnetic Resonance Imaging: A

Systematic Review and Recommendations for Future Studies," *Cancers*, vol. 13, p. 3318, 2021. [Online]. Available: https://doi.org/10.3390/cancers13133318.

[30] R. Aggarwal, V. Sounderajah, G. Martin, D. S. W. Ting, A. Karthikesalingam, D. King, H. Ashrafian, A. Darzi, "Diagnostic accuracy of deep learning in medical imaging: a systematic review and meta-analysis," *Npj Digital Medicine*, vol. 4, no. 1, 2021. [Online]. Available: https://doi.org/10.1038/s41746-021-00438-z.

[31] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *PMLR*, Conference on Fairness, Accountability, and Transparency, pp. 77–91, 2018.

[32] UNESCO, EQUALS Skills Coalition, M. West, R. Kraut, and Ei Chew Han, "I'd blush if I could: closing gender divides in digital skills through education" (Document code: GEN/2019/EQUALS/1 REV.5). [Online]. Available: https://doi.org/10.54675/RAPC9356.

[33] T. H. Davenport and R. Kalakota, "The potential for artificial intelligence in healthcare," *Future Healthcare Journal*, vol. 6, no. 2, pp. 94–98, 2019. [Online]. Available: https://doi.org/10.7861/futurehosp.6-2-94.

[34] M. L. Tushman and C. A. O'Reilly, "Ambidextrous Organizations: Managing Evolutionary and Revolutionary Change," *California Management Review*, vol. 38, no. 4, pp. 8–29, 1996.

[35] S. Raisch and J. Birkinshaw, "Organizational Ambidexterity: Antecedents, Outcomes, and Moderators," *Journal of Management*, vol. 34, no. 3, pp. 375–409, 2008.

[36] R. Van de Wetering, P. Mikalef, and D. Dennehy, "Artificial Intelligence Ambidexterity, Adaptive Transformation Capability, and Their Impact on Performance Under Tumultuous Times," in *Proceedings of PACIS 2022, 2022.* [Online]. Available: https://aisel.aisnet.org/pacis2022/153

[37] R. Van de Wetering, "The impact of artificial intelligence ambidexterity and strategic flexibility on operational ambidexterity" (2022). *PACIS 2022 Proceedings*, p. 153. [Online]. Available: https://aisel.aisnet.org/pacis2022/153

[38] A. Kolade, T. Onunka, C. Daraojimba, N. Eyo-Udo, O. Onunka, A. Omotosho, C. Okafor, "Mitigating Cybersecurity Risks in the U.S. Healthcare Sector," *International Journal of Research and Scientific Innovation (IJRSI).* pp. 177–194, 2023. [Online]. Available: 10.51244/IJRSI.2023.10918.

[39] European Commission, "European Health Union: A European Health Data Space for people and science," [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711. Accessed: Jan. 26, 2024.