Politécnica

Revista Científica

Nº 30 Dezembro de 2023

BIBLIOMETRIC ANALYSIS ON CYBERSPACE SECURITY – NIS DIRECTIVES

BIBLIOMETRIC STUDY ON THE DEVELOPMENT AND IMPLEMENTATION OF CYBERSECURITY IN AUTONOMOUS VEHICLES

BIBLIOMETRIC STUDY ON THE IMPORTANCE OF ENDPOINT SECURITY IN COMPANIES

UM CISNE NEGRO NA SOCIEDADE DA PÓS-NORMALIDADE E PÓS-VERDADE. AS IMPLICAÇÕES DA COVID-19 NA BUSCA DA VERDADE

ISPGAYA
instituto superior politécnico

CENTRO DE INVESTIGAÇÃO E DESENVOLVIMENTO DO ISPGAYA

Ficha Técnica

Administração
Redação
Sede do Editor
Instituto Superior Politécnico Gaya
Avenida dos Descobrimentos, 333
4400-103 Vila Nova de Gaia
www.ispgaya.pt

Propriedade Instituto Superior Politécnico Gaya

NIPC 501962433
Contato Tel. 22 374 57 30/3 Fax 22 374 57 39
ISSN 0874-8799

Registo DGCS nº 123623

Depósito Legal 153750/00

DOI 10.58086/cxw5-g269
Frequência Anual
nº Vol. XXX - Dezembro de 2023

Estatuto Editorial: https://comum.rcaap.pt/retrieve/95533/Estatuto%20editorial%202020%20Timbrado.pdf

Índice

p.

Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/625w-1k44

Editorial

A *ratio* tecnológica…

Num mundo transformado numa "aldeia global", cruzamo-nos em qualquer rua, de qualquer sítio, com o transeunte, com pessoas que caminham sós, com auscultadores nos ouvidos, e vão fazendo diferentes expressões faciais, alegres ou sorumbáticas. Certamente que vão a ouvir algo que os alegra ou entristece e transmitem-no involuntariamente. Mas vão a ouvir…

Graças à comunicação, o homem consegue desenvolver-se e desenvolver o mundo, construir e apreciar mensagens que transmitem o seu pensamento, os seus sentimentos, emoções e ações e, em simultâneo, torna-o capaz de compreender os outros. As mãos e os olhos são entendidos como o fundamento sensorial de referência. Em contrapartida, vivemos numa época em que algumas pessoas, não sei se muitas, atribuem menos importância ao livro que acabam de comprar que ao relógio digital que lhes é enviado como brinde dessa compra…

Mas, com expressões faciais alegres ou sorumbáticas, vão a ouvir e ouvir é uma das capacidades do homem e de muitos animais. O ouvido é um dos cinco sentidos que permite captar as sensações que chegam do mundo exterior. Através do ouvido apercebemo-nos de sinais sonoros, que podem ser suaves, brandos, fortes ou ásperos.

Cruzamo-nos, também, com gente a caminhar só, embora a olhar para o telemóvel. Do mesmo modo fazem expressões faciais que exteriorizam perante o infinito. A alegria ou a admiração para o que estão a olhar.

Mas olhar não é ver e ouvir não é escutar ou, se quisermos, não é saber ouvir. O homem passa a maior parte do tempo a ouvir. Com frequência ouve, mas não escuta, isto é, não se preocupa em atender aos sons que o cercam. O ouvido contacta com ruídos e em muitos casos nem sequer se sente perturbado. Infelizmente, muitas vezes, a continuidade e intensidade de tais ruídos conduzem a uma progressiva perda da capacidade auditiva. Essa dificuldade de audição torna-se negativa para a compreensão daquilo que escuta[1].

[1] Moreira, V.; Pimenta, H. (1994) Encontro Literário, Porto Editora, p. 27

https://doi.org/10.58086/625w-1k44

Não discuto a lógica do uso correto de cada um dos equipamentos, de som ou de imagem, enquanto se caminha, mas ambos os passeantes usam tecnologias que agora estão generalizadas e, elas mesmo, são incentivadoras do incremento do seu uso, mesmo que correndo o risco de atropelamento ao passar distraído numa passadeira.

Atualmente, como sempre aconteceu, na comunicação oral é necessário que o destinatário seja capaz de saber escutar e ouvir bem, tanto mais que descodificar uma mensagem não é apenas ouvi-la e, por vezes, ser capaz de reproduzi-la na íntegra. Isso pode ser apenas resultado de uma boa capacidade de compreensão genérica. Para que o ato de escuta resulte em pleno é necessário ter atenção, concentração, motivação, sentido crítico, interesse pelo que se ouve e, porque não, uma certa sedução.

A comunicação unilateral implica a atuação de um emissor, enquanto o recetor é passivo. É o exemplo daqueles com quem me cruzo no passeio e apenas emitem expressões faciais difusas. Em contrapartida, a comunicação bilateral exige reciprocidade entre emissor e recetor, que se vêm na necessidade de alternarem os papeis. A isto chama-se “conversar”.

A minha experiência, ao ter-me potenciado o contacto com colegas, professores e estudantes, mostrou-me poder ser a escola, o dia a dia na universidade, um espaço de festa e de suor, de alegria e de rigor, de valores humanos plasmados em direitos e em deveres, um espaço e um tempo de realismo e de sonho, de ventura e de aventura, um espaço fértil de relação de comunicação mutuamente clarificada e assumida, ganhando uma dimensão que está para além das mecanicistas interações da *ratio* tecnológica.

Este é um desafio de crescimento, de maturação da maturidade, que o ensino superior aconselha e que aqui incentivamos.

Vale a pena pensar nisto…

Lino Tavares Dias

Janeiro 2024

Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/625w-1k44

BIBLIOMETRIC ANALYSIS ON CYBERSPACE SECURITY - NIS DIRECTIVES

Cláudia Borgguen[1]

José Morais[2]

Mário Lousã[3]

Abstract

The impact of security in cyberspace has been increasing, motivating companies to reconsider their security strategies. In addition, people from various countries who are aware of this growth are seeking to present studies in various journals that allow them to identify elements that contribute to the consolidation of the concept of security in cyberspace. With this reality in mind, this study, supported by a bibliometric analysis of security in cyberspace based on articles published in the last eight years, aims to analyze the evolution of scientific research, identify the most influential scientific publications on topics related to cyberspace security, and detect research opportunities in the field. The study also discusses the implementation of the legal framework for security in cyberspace and the NIS Directive, aspects that European companies should consider in their cybersecurity strategy. The study's conclusions highlight the multifaceted nature of cybersecurity challenges and the need for a holistic and collaborative approach to strengthening digital resilience, with an emphasis on promoting a culture of awareness encouraged at the organizational and social level by policymakers, industry leaders, and researchers.

Keywords: Security in cyberspace; Cybersecurity; NIS Directive; Legal regime; Bibliometric analysis.

ANÁLISE BIBLIOMÉTRICA SOBRE SEGURANÇA DO CIBERESPAÇO - DIRETIVAS NIS

Resumo

O impacto da segurança no ciberespaço tem vindo a aumentar, motivando as empresas a reconsiderar as suas estratégias de segurança. Além disso, pessoas de vários países que estão atentas a este crescimento procuram apresentar estudos em diversas revistas que lhes permitam identificar elementos que contribuem para a consolidação do conceito de segurança no ciberespaço. Tendo esta realidade em mente, este estudo, apoiado numa análise bibliométrica da segurança no ciberespaço baseada em artigos publicados nos últimos oito anos, tem como objectivo analisar a evolução da investigação científica, identificar as publicações científicas mais influentes sobre temas relacionados com a segurança do ciberespaço, e detectar oportunidades de pesquisa na área. O estudo discute também a implementação do quadro jurídico para a segurança no ciberespaço e a Diretiva NIS, aspectos que as empresas europeias devem considerar na sua estratégia de cibersegurança. As conclusões do estudo destacam a natureza multifacetada dos desafios de cibersegurança e a necessidade de uma abordagem holística e colaborativa

[1] ISPGAYA /Instituto Superior Politécnico Gaya, Portugal

[2] CEOS.PP; ISPGAYA /Instituto Superior Politécnico Gaya, Portugal

[3] CID ISPGAYA; ISPGAYA /Instituto Superior Politécnico Gaya, Portugal

https://doi.org/10.58086/625w-1k44

para reforçar a resiliência digital, com ênfase na promoção de uma cultura de sensibilização incentivada a nível organizacional e social por decisores políticos, líderes industriais e investigadores.

Palavras-chave: Segurança no ciberespaço, Cibersegurança, Diretiva NIS, Regime jurídico, Análise bibliométrica.

Introduction

In the last few years, the security of cyberspace has become a fundamental issue for the European Union (EU), demonstrating a strong commitment to promoting a global, open, stable, and secure cyberspace. This commitment is evident in the stance taken by the EU in international security debates related to cyberspace (Salvaggio & González, 2022). One of the main initiatives in this field is the Network and Information Security Directive (NIS), which aims to raise the general level of cybersecurity in the EU (Drivas et al., 2020). The NIS Directive establishes a mandatory reporting regime for operators of essential services and digital service providers, reflecting the EU's determination to strengthen cybersecurity (Franke et al., 2021). Additionally, under the NIS Directive, the European Commission has adopted a comprehensive cybersecurity package to further strengthen the EU's resilience and response to cyberattacks (Maglaras et al., 2020). However, according Cesarec (2020), challenges remain in achieving the highest level of cybersecurity in all EU Member States, indicating gaps in their capabilities.

The legal landscape around cyberspace security in the EU has changed significantly, particularly with the introduction of the NIS Directive and the General Data Protection Regulation (GDPR) (Urquhart & McAuley, 2018). The NIS Directive (Directive (EU) 2016/1148) imposes specific obligations on Member States to improve the cybersecurity posture across the EU (Drivas et al., 2020). In addition, the proposed NIS Directive 2 seeks to modernize the current EU legal framework on cybersecurity and address the limitations of the NIS Directive (Chiara, 2022). Despite these regulatory efforts, there is still a lack of stakeholders in the EU cybersecurity ecosystem, which highlights the need for greater engagement and collaboration (Bederna & Rajnai, 2022).

The increasing exposure to cyber threats due to global interconnectivity requires the adoption of cybersecurity standards and frameworks (Ponsard et al., 2021). The European Union Cybersecurity Act and the NIS Directive play key roles in assisting EU internal market organizations in resisting and recovering from cyber threats (Ferguson, 2022). The NIS Directive is the first EU legal instrument that focuses on incident notification and information sharing as key requirements, highlighting the importance of such information for cyber defense (Ducuing, 2021). Furthermore, the protection of cyberspace has emerged as one of the top security priorities for governments around the world (Carrapico & Farrand, 2016).

https://doi.org/10.58086/625w-1k44

This paper is divided into four parts. The first part reviews the literature on cybersecurity, information security, and the NIS Directive. The next part presents the methodology and the research questions, followed by an analysis of the results obtained from the bibliometric analysis. Finally, the final considerations are presented.

1. Literature review

1.1. Cybersecurity

Cybersecurity encompasses the protection of networks and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction of data (Ferguson, 2022). It involves implementing measures to ensure the confidentiality, integrity, and availability of data and services, particularly in critical sectors such as energy, healthcare, and essential services (Biasin & Kamenjašević, 2022; Skias et al., 2021). The NIS and NIS 2 Directives play a crucial role in defining the threshold for reporting cybersecurity incidents and promoting improvements in the cybersecurity of essential services (Schmitz-Berndt, 2023; Wallis & Johnson, 2020).

The dynamic nature of cybersecurity requires taking advantage of information on cyber threats to develop a risk framework that supports decision-making and resilience against them (Riesco & Villagrá, 2019). Additionally, compliance with the NIS Directive requires the development of cybersecurity maturity assessment frameworks to evaluate and improve cybersecurity measures (Drivas et al., 2020). This is exemplified in the case of Greece, where the National Cybersecurity Authority and a cybersecurity framework were created to align with the NIS Directive and ensure the security of critical infrastructure (Maglaras et al., 2020).

1.2. Information security

The term "Information Security" encompasses the protection of data and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction. It involves ensuring the confidentiality, integrity, and availability of information, as well as the systems and processes that store, process, and transmit that information (Schmitz-Berndt & Schiffner, 2021). Information security is crucial for safeguarding sensitive data, such as personal and financial information, intellectual property, and organizational data, from unauthorized access and cyber threats (Wallis & Johnson, 2020). It also involves implementing measures to prevent, detect, and respond to security incidents, including cyberattacks, data breaches, and other security breaches (Skias et al., 2021). In addition, “Information Security” is closely linked to compliance with regulations and standards, such as the NIS Directive, which aims to improve the overall level of cybersecurity in the European Union (Wallis & Johnson, 2020). The NIS

https://doi.org/10.58086/625w-1k44

Directive gives Operators of Essential Services (OES) responsibility for ensuring the security of networks and information systems, underlining the need for an objective-oriented approach to implementing security and protection standards (Ponsard et al., 2021).

Generally, information security, in the context of the NIS Directive, plays a key role in strengthening the cybersecurity posture of essential services, promoting early detection and adequate mitigation of cybersecurity incidents, and fostering a dynamic risk framework to address emerging cyber threats (Riesco & Villagrá, 2019). Therefore, understanding and defining "Information Security" is essential for organizations to effectively comply with the NIS Directive and contribute to the overall cybersecurity resilience of critical infrastructure and essential services (Bagnato, 2020).

1.3. NIS Directive

The Network and Information Systems (NIS) Directive is the first EU legal instrument to focus on incident notification and information sharing as key requirements, based on studies showing the importance of such information for cyber defense (Ducuing, 2021). It defines critical infrastructures and operators of essential services, boosting improvements in the cybersecurity of services (Bagnato, 2020; Wallis & Johnson, 2020). It also modernizes the EU's legal framework on cybersecurity and seeks to strengthen the EU's resilience and response to cyberattacks (Ferguson, 2022). The private sector has seen a change in its role in NIS regulation, moving from being the subject of regulation to becoming an active player in policymaking, providing technical expertise for network resilience (Carrapico & Farrand, 2016). In addition, the NIS Directive poses challenges in practice, requiring compliance frameworks and cybersecurity maturity assessments (Biasin & Kamenjašević, 2022).

The NIS Directive has been reformed, leading to the proposal of the NIS 2 Directive, which seeks to modernize the existing EU legal framework on cybersecurity while correcting the shortcomings that prevented the NIS Directive from unlocking its full potential (Chiara, 2022). Furthermore, the NIS Directive has implications for various sectors, including healthcare, as seen in the context of the cybersecurity challenges arising from the AI Act and the NIS 2 Directive proposals for medical devices (Biasin & Kamenjašević, 2022). The literature also emphasizes the importance of dialogue, partnership, and capacity building for network and information security, highlighting the changing role of the private sector from regulatory object to regulatory shaper in the context of the NIS Directive (Carrapico & Farrand, 2016). Overall, the NIS Directive represents a significant step taken by the EU to strengthen the security of networks and information systems, with implications for various sectors and an emphasis on incident reporting, information sharing, and the modernization of cybersecurity legal frameworks.

https://doi.org/10.58086/625w-1k44

1.4. Concept relationship

In summary, these three terms are interlinked: the NIS Directive is a legislative measure that establishes standards and requirements for "Information Security" in the EU. In turn, "Information Security" is a subset of the broader field of "Cybersecurity", which encompasses all measures taken to protect digital data and systems. Thus, it can be said that the NIS Directive is part of "Information Security" and that "Information Security" is part of "Cybersecurity" (cf. Figure 1).

Figure 1
Relationship between "Cybersecurity", "Information Security" and the "NIS Directive"

Source: own.

Table 1.
Concepts of "Cybersecurity", "Information Security" and "NIS Directive"

Concept	Description	Authors
Cybersecurity	Cybersecurity involves protecting networks and information systems, particularly in critical sectors, by implementing measures to ensure data confidentiality, integrity, and availability and developing a risk framework and maturity assessment framework in compliance with the NIS Directives.	Drivas et al. (2020); Schmitz-Berndt (2023); Skias et al. (2021)
Information Security	Information Security, in the context of the NIS Directive, involves protecting data and information systems, ensuring their confidentiality, integrity, and availability, safeguarding sensitive data, preventing, detecting, and responding to security incidents, and strengthening the cybersecurity posture of essential services.	Bagnato (2020); Ponsard et al. (2021); Schmitz-Berndt & Schiffner (2021)
NIS Directive	The NIS Directive, the first EU legal instrument focusing on incident notification and information sharing, defines critical infrastructures and operators of essential services, modernizes the EU's cybersecurity legal framework, and has been reformed into the NIS 2 Directive to address its shortcomings and expand its implications to various sectors.	Carrapico & Farrand (2016); Chiara (2022); Ducuing (2021)

https://doi.org/10.58086/625w-1k44

2. Methodology

Bibliometric analysis, a quantitative method for evaluating scientific production, has become increasingly popular due to its reliability and efficiency. Zupic and Čater (2014) state that in recent years, there has been an increasing emphasis on advancing theory and practice through bibliometric research (Mukherjee et al., 2022), contributing to a deeper understanding of academic production and its impact. This method involves processing bibliometric data from databases such as Scopus and Web of Science to provide an overview of published scientific articles. According to Ellegaard and Wallin (2015), using statistical tools, researchers can carry out a systematic and transparent review process, allowing bibliographic data to be aggregated to identify the main themes and research trends. However, it is important to note that bibliometric analysis has limitations, such as the consideration of qualitative elements like the impact factor of a journal (Hicks et al., 2015).

The methodology for bibliometric analysis often follows the PRISMA guidelines, which provide a 27-point checklist and a flowchart for preparing systematic reviews and meta-analyses (cf. Figure 2). These guidelines cover several aspects, including the study title, abstract, introduction, methods, results, discussion, and financing, as well as points related to the search strategy, study selection, and data extraction. For Moher (2009), the use of such guidelines guarantees a rigorous and standardized approach to bibliometric analysis, increasing the reliability of the results.

1.1. Research questions

This paper, supported by a bibliometric study, focuses on cyberspace security and the respective implementation of the NIS Directive, and aims to answer the following four research questions:

- RQ1: How has the implementation of the legal regime for security in cyberspace and the NIS Directive evolved in academic research over the last eight years?
- RQ2: Which articles stand out most in this topic of study (more citations)?
- RQ3: What are the main focuses of the investigation implementation of the legal regime for security in cyberspace and the NIS Directive?

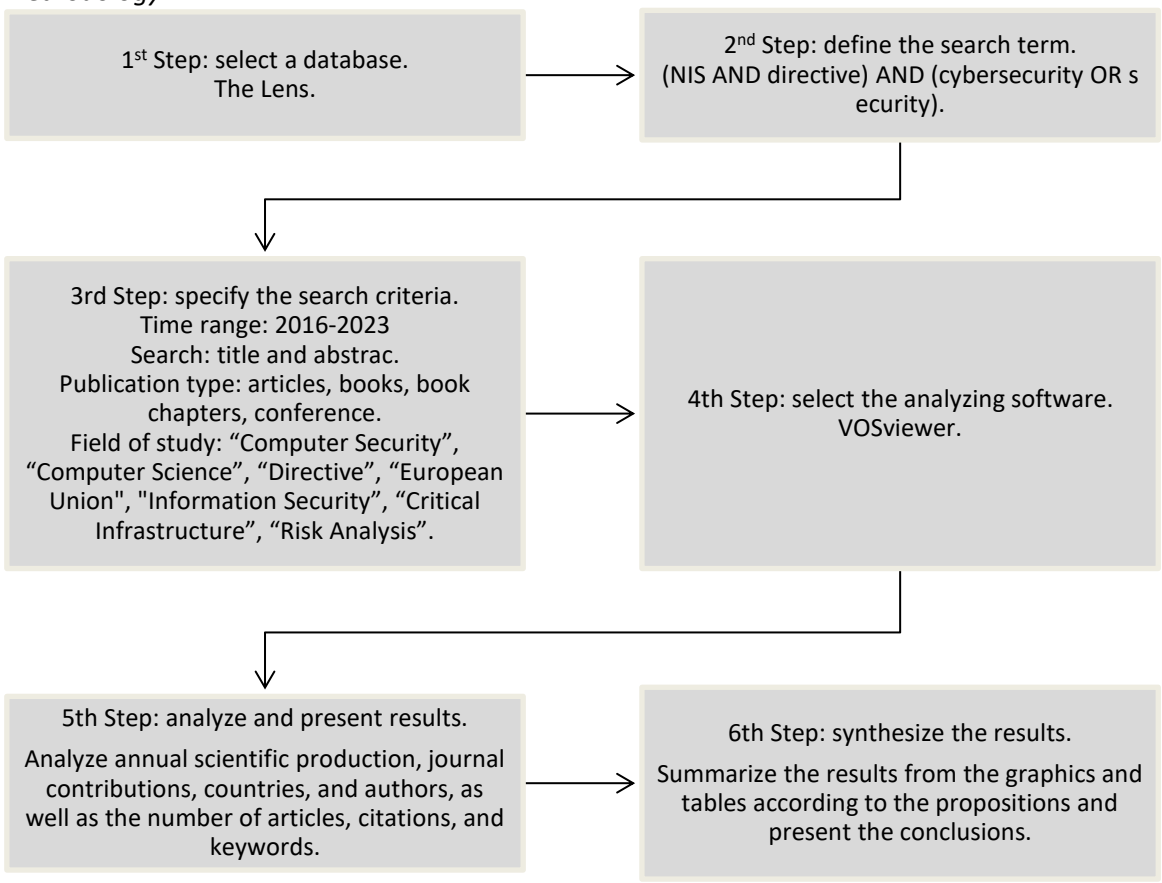
1.2. PRISMA method

Figure 2 presents the methodology used in the research, based on the PRISMA method. It is observed that six stages were considered to carry out the research: selection of the database; definition of search terms; specification of search criteria; selection of analysis software; analysis and presentation of results; and synthesizing the results.

https://doi.org/10.58086/625w-1k44

Figure 2

Methodology



Source: own.

1.3. Database

The selection of the database for the bibliometric analysis is crucial, and platforms with an extensive collection of patents and academic scientific articles provide valuable data for researchers and students in various fields of science, technology, engineering, and mathematics. Thus, the database chosen was The Lens, a free and open data platform with 144.3 million patents and 252.1 million academic scientific articles and research papers in the fields of science, technology, engineering, and mathematics for researchers and students (The Lens, n.d.).

1.4. Search terms

The terms chosen for the search were "NIS Directive" and "Cybersecurity" from a conjunctive perspective, using the AND operator between the words. So, the query was as follows: (nis AND directive) AND (cybersecurity OR security).

https://doi.org/10.58086/625w-1k44

1.5. Search criteria

The analysis focused on the last eight years, i.e., the search was restricted to publications between 2016 and 2023. Consideration was given to the technical-scientific quality of the type of publication: journal articles, books, book chapters, and conferences. In addition, to obtain specific results within the scope of this study, the following areas of study were selected: "Computer Security", "Computer Science", "Directive", "European Union, Information Security", "Critical Infrastructure", "Risk Analysis".

A total of 340 publications were obtained. A preliminary analysis of the results revealed that some publications did not focus on the research area. So, the search was refined using the fields title, abstract, keywords, and area of study, and 141 publications were obtained. Finally, VOSviewer software version 1.6.20 was used to analyze and visualize the data obtained.

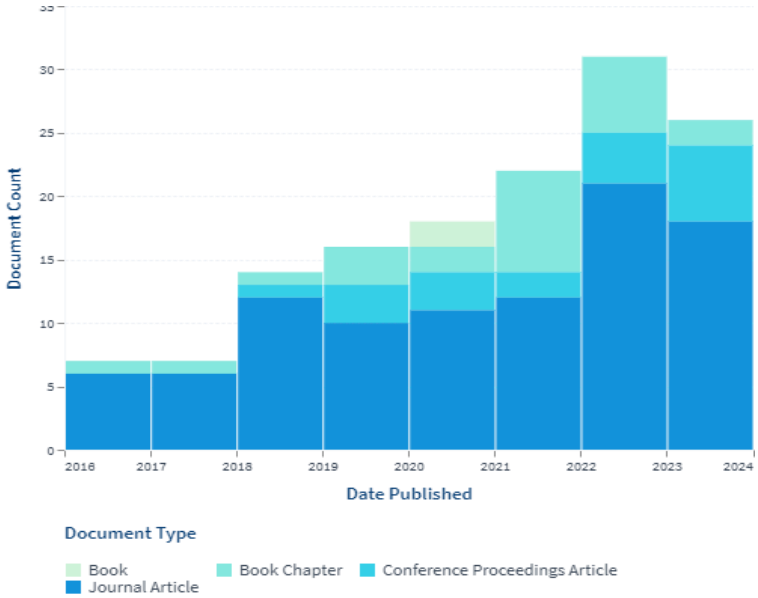
3. Analysis of results

3.1. Descriptive analysis (RQ1 and RQ2)

This study includes 141 documents over a period of eight years, i.e., between 2016 and 2023.

Figure 3 shows the volume of annual scientific production resulting from the research carried out, considering the elements presented in steps 2 and 3 of Figure 2.

Figure 3
Number of publications by type of document



Source: The Lens.

https://doi.org/10.58086/625w-1k44

It can therefore be seen that the annual scientific output about the NIS Directive is growing. Considering that 7 documents were published in 2016 and 26 in 2023, the growth is 271%. Attending Table 2, the biggest annual increase was seen in 2022, with 31 publications (two book chapters, six conference proceedings, and 18 articles).

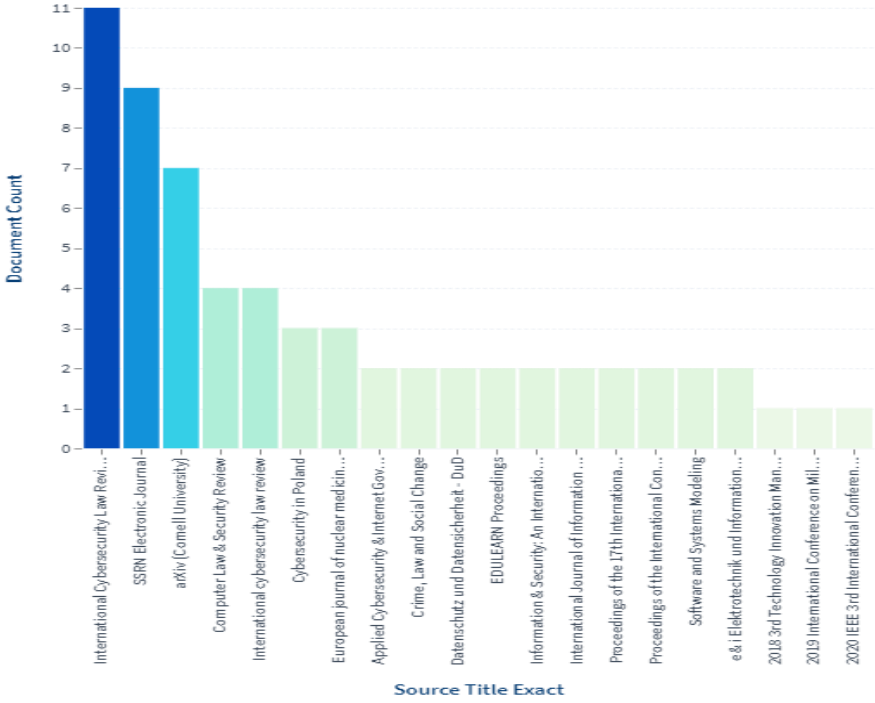
Table 2.
Number of publications by type and year

Year	Books	Book Chapters	Conferences	Articles	Total
2016	-	1	-	6	**7**
2017	-	1	-	6	**7**
2018	-	1	1	12	**14**
2019	-	3	3	10	**16**
2020	2	2	3	11	**18**
2021	-	8	2	12	**22**
2022	-	6	4	21	**31**
2023	-	2	6	18	**26**

Source: The Lens.

The statistics also show that these documents were published in 20 different journals (cf. Figure 4). Table 3 shows the top 5 journals (International Cybersecurity Law Review; SSRN Electronic Journal; arXiv (Cornell University); Computer Law & Security Review; European Journal of Nuclear Medicine and Molecular Imaging) that accounted for 31 publications.

Figure 4
Publications by journal



Source: The Lens.

https://doi.org/10.58086/625w-1k44

Table 3

Top 5 journals by number of publications

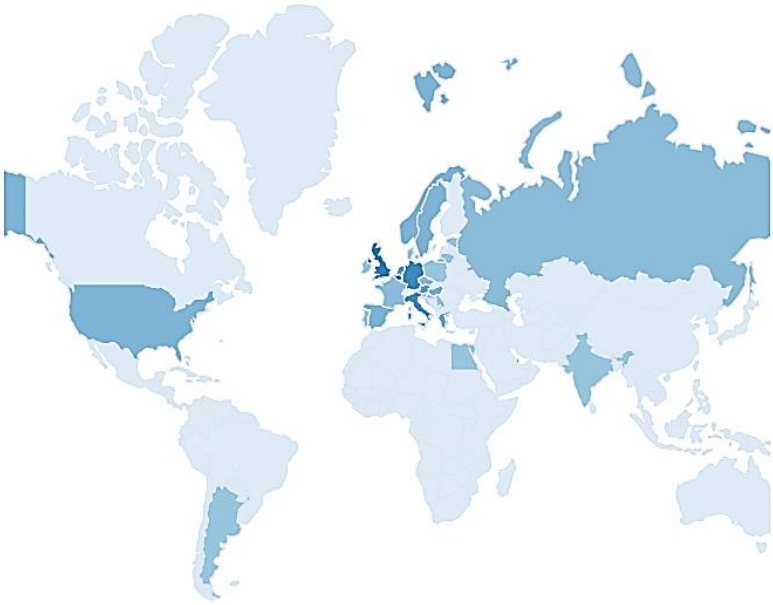
Journal	Field	Number of publications
International Cybersecurity Law Review	Cybersecurity, data security, technology, legislation, and regulation.	15
SSRN Electronic Journal	Social Sciences, Economics, Law, Corporate Governance and Human Sciences.	9
arXiv (Cornell University)	Physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics.	7
Computer Law & Security Review	Law, telecommunications regulation, intellectual property, cybercrime, surveillance and security, e-commerce, outsourcing, data protection, e-privacy, EU and public sector IT policy.	4
European Journal of Nuclear Medicine and Molecular Imaging	Physics, dosimetry, radiation biology, radiochemistry, and pharmacy.	3

Source: The Lens.

Figure 5 shows the most active countries in scientific production and research, noting that the countries of the European Union and the United Kingdom have the highest number of publications.

Figure 5

Scientific production by country



Source: The Lens.

https://doi.org/10.58086/625w-1k44

Complementing Figure 5, Table 4 illustrates the five countries with the greatest scientific production according to the terms researched. This analysis identifies the countries where there is the greatest concern when investigating the issue of implementing the NIS Directive. It should be noted that the countries with the highest number of publications are on the European continent. This may be because the NIS Directive is, precisely, a European directive.

Table 4
Top 5 countries by number of publications

Country	**Number of publications**
Belgium	12
United Kingdom	11
Germany	7
Italy	7
Luxembourg	7

Source: The Lens.

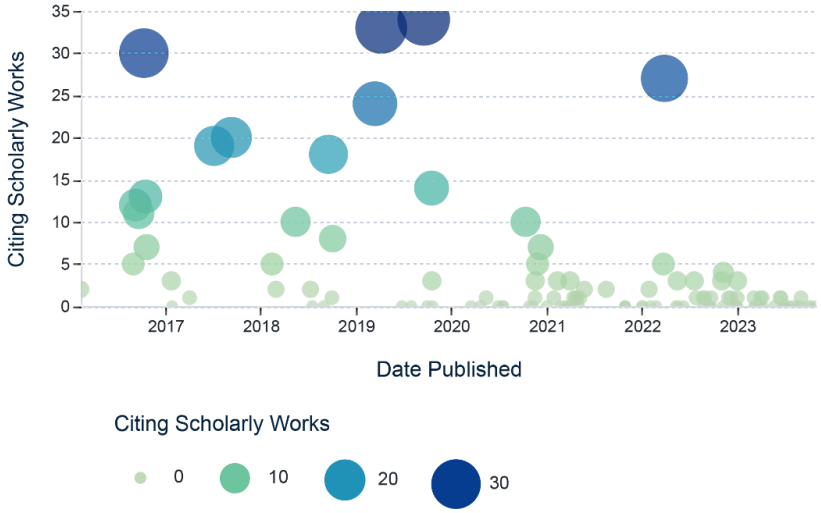
RQ1: Over the past eight years, academic research into the application of the cyberspace security legal regime and the NIS Directive has evolved, resulting in an increasing number of publications covering a wide range of topics (e.g., computer security, scientific computing, business, law, and political science), especially in countries on the European continent.

RQ2: According to Figure 6, there are two articles that stand out, with more than 30 citations. They are: "Dialogue, partnership and empowerment for network and information security: the changing role of the private sector from objects of regulation to regulation shapers", from Carrapico and Farrand (2017), and "Leveraging cyber threat intelligence for a dynamic risk framework" form Riesco and Villagrá (2019).

https://doi.org/10.58086/625w-1k44

Figure 6.

Top citations by publication



Source: The Lens.

Table 5 shows the five authors who contributed most to scientific production. Sandra Schmitz-Berndt and George Drivas are the authors with the greatest scientific production, with six publications, followed by Argyro Chatzopoulou, Chris Johnson, and Costas Lambrinoudakis, each with four publications. Again, most authors are based in Europe.

Table 5

Top 5 authors by number of publications

Author	Number of publications
Sandra Schmitz-Berndt	6
George Drivas	6
Argyro Chatzopoulou	4
Chris Johnson	4
Costas Lambrinoudakis	4

Source: The Lens.

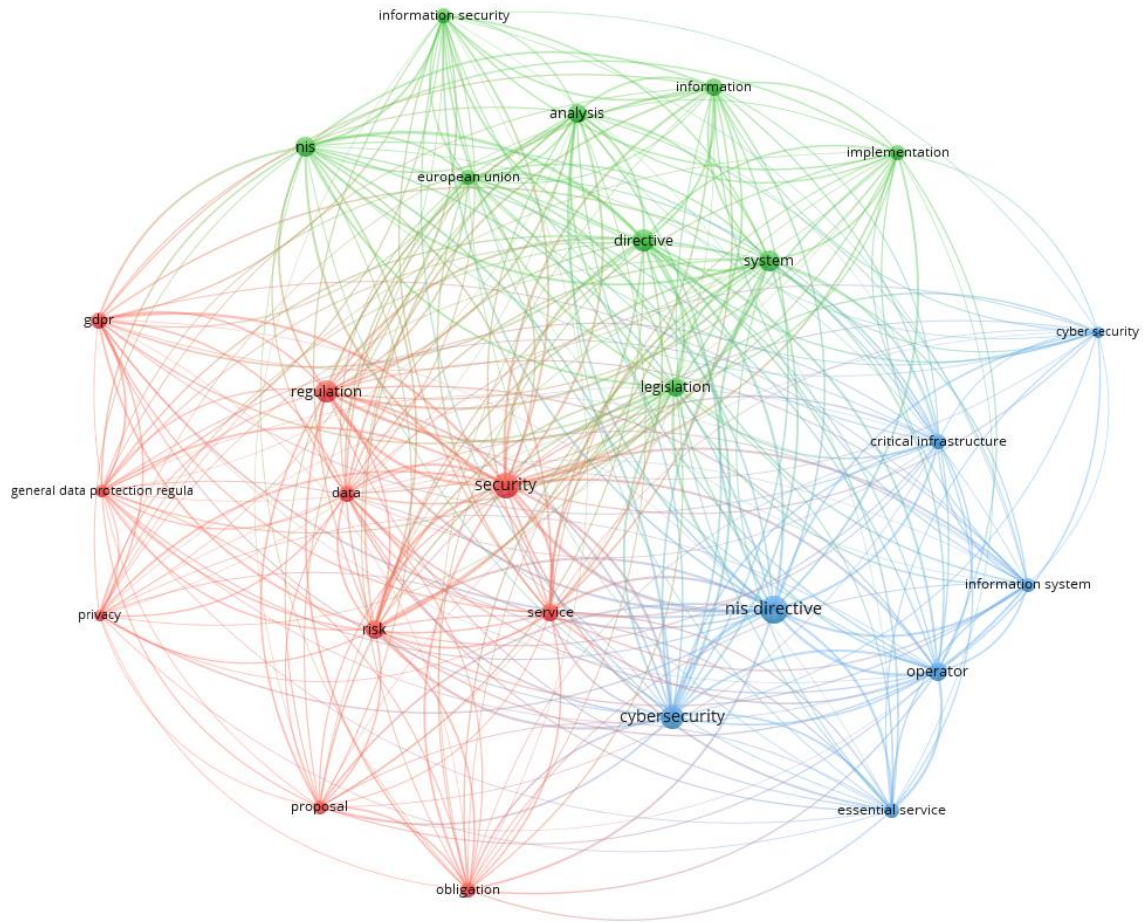
3.2. Keyword analysis (RQ3)

According to Wang and Chai (2018), keyword analysis is an important method for identifying the most relevant publications in a research area, helping to recognize trends and gaps. By examining the most frequent keywords, such as “European Union”, “NIS Directive”, “Regulation” and “Cybersecurity”, it is possible to gain insight into the current focus of the area of investigation. For example, the analysis reveals that the most cited keywords are “NIS Directive” and “Cybersecurity”, indicating a significant emphasis on regulatory frameworks and cybersecurity measures. This suggests a growing concern about the security of information systems and the need for regulatory compliance in the context of cybersecurity.

https://doi.org/10.58086/625w-1k44

By examining the most frequent keywords in publications related to these topics, researchers can gain a comprehensive understanding of the evolving landscape of cybersecurity regulation in the European Union. This approach can shed light on the impact of the NIS Directive on cybersecurity practices and the EU's regulatory framework, thus identifying potential areas for further research and development in this critical area. Using the computer tool VOSviewer, Figure 7 shows the occurrence of the authors' keywords. A minimum of 10 occurrences of a keyword was considered, resulting in a total of 42 keywords distributed across 3 clusters. The largest cluster is the red one, with 10 words in which the keyword "Security" stands out, with 24 occurrences. It is followed by the green cluster with nine words. In this cluster, the keyword "Directive" stands out, with 25 occurrences. Finally, the blue cluster, with seven words, where the keyword "NIS Directive" stands out, with 25 occurrences.

Figure 7
keywords occurrence



Source: VOSviewer.

https://doi.org/10.58086/625w-1k44

Table 6 presents the keywords that make up each cluster. In the next section of the paper, each of the clusters is analyzed.

Table 6

Keywords by Cluster

Cluster	Keywords
Red	"data"; "gdpr"; "general data protection regulation"; "obligation"; "privacy"; "proposal"; "regulation"; "risk"; "security"; "service"
Green	"analysis"; "directive"; "european union"; "implementation"; "information"; "information security"; "legislation"; "nis"; "system"
Blue	"critical infrastructure"; "cyber security"; "cybersecurity"; "essential service"; "information system"; "nis directive"; "operator"

Source: VOSviewer.

3.2.1. Red cluster

The keyword sets "data", "gdpr", "general data protection regulation", "obligation", "privacy", "proposal", "regulation", "risk", "security" and "service" cover and interconnect crucial topics in the context of cybersecurity regulation and the NIS Directive. The General Data Protection Regulation (GDPR) has a significant impact on data processing and privacy practices, requiring organizations to comply with strict regulations to ensure the protection of personal data (Torre et al., 2019). GDPR compliance involves several obligations and risks related to data security and privacy, which are essential components of cybersecurity and NIS Directive regulation (Mekovec & Peras, 2020). Remember that, according to Koltay (2016), GDPR also led to a paradigm shift in data governance, emphasizing the importance of data quality, literacy, and management to meet regulatory requirements.

Furthermore, GDPR has triggered the need for organizations to implement robust security measures to protect personal data, thus emphasizing the importance of data security in the context of cybersecurity and NIS Directive regulation (Peloquin et al., 2020). The regulation also requires a comprehensive understanding of GDPR principles and requirements, leading to an assessment of GDPR compliance and its implications in various domains, including, for example, higher education institutions (Penev, 2019). Overall, the set of keywords underscores the multifaceted nature of the GDPR and data-related topics, highlighting their role in shaping cybersecurity practices and regulatory compliance.

https://doi.org/10.58086/625w-1k44

3.2.2. Green Cluster

The set of keywords "analysis"; "directive"; "european union"; "implementation"; "information"; "information security"; "legislation"; "nis" and "system" covers interconnected and important topics in the context of cybersecurity and the regulation of the NIS Directive. The NIS Directive, which is the first piece of legislation at the EU level on cybersecurity, aims to achieve a high common level of network and "Information Security" across the European Union. It requires member states to adopt a national strategy for the security of networks and information systems and establishes security and notification requirements for operators of essential services and digital service providers (Pravdiuk, 2023).

Implementing the NIS Directive involves developing and applying information security policies, complying with legal requirements, and adopting information security practices in organizations. This process is essential to ensuring the effectiveness of information security measures and promoting a culture of security awareness and compliance (Park & Chai, 2018). In addition, the NIS Directive highlights the need for functional modeling of information security culture status monitoring systems to assess and improve the level of security in organizations, thus contributing to the overall security of information systems and critical infrastructures (Voitsekhovska et al., 2022).

The NIS Directive also highlights the importance of governance and legislation in relation to information security, seeking to simplify it while at the same time addressing the complexities and challenges associated with ensuring effective governance structures and practices (Fitzgerald & Peltier, 2016).

In summary, the NIS Directive highlights the multifaceted nature of cybersecurity and information security governance, highlighting the interconnected themes of legislation, implementation, analysis, and culture in the context of ensuring the security and resilience of critical infrastructure, information systems, and organizations in the European Union.

3.2.3. Blue Cluster

The set of keywords "critical infrastructure"; "cyber security"; "cybersecurity"; "essential service"; "information system"; "nis directive" and "operator" encompass interconnected and crucial themes in the context of cybersecurity regulation and the NIS Directive. The NIS Directive emphasizes the protection of essential services and information systems, which are integral components of critical infrastructure. It is essential to define critical infrastructures, as they include assets or systems vital to social functions, health, security, and economic well-being, the disruption of which would have a significant impact (Zlateva & Hadjitodorov, 2022). Additionally, the protection of essential services is crucial to preventing

https://doi.org/10.58086/625w-1k44

attacks and limiting the spread of damage caused by malware, highlighting the importance of cybersecurity in safeguarding critical infrastructure and essential services (Sato et al., 2019).

The integration of information systems into critical infrastructure and essential services is essential to guaranteeing the effective management and protection of these systems. Information systems play a fundamental role in the management and optimization of critical infrastructure resources, thus contributing to the global governance of information systems (Falih et al., 2019). Furthermore, the development of a multidisciplinary cybersecurity workforce is crucial to address the complex challenges associated with protecting critical infrastructure and essential services against cyber threats (Hulatt & Stavrou, 2021). This highlights the importance of a qualified workforce in implementing cybersecurity measures and safeguarding critical infrastructure, information systems, and essential services.

The NIS Directive and cybersecurity practices are also interlinked with the concept of "operator" and the management of information systems in the context of essential services and critical infrastructures (Korablyov & Lutskyy, 2022). The directive highlights the need for a systemic approach to optimizing information technology resources within the framework of information systems governance, aligning with the interconnected themes of "information system" and "essential service" (Falih et al., 2019). The set of keywords therefore underlines the multi-faceted nature of cybersecurity and the regulation of the NIS Directive, emphasizing its key role in safeguarding essential services and critical infrastructure against cyber threats.

4. Limitations and future research

The results obtained were a consequence of the choices made in stages one to three, as presented in the methodology section, namely the database used and, above all, the words used to support the search. These choices are therefore a limitation of the work carried out.

In future work, it would be relevant to explore the contributions that technology can make to the implementation of cyberspace security regulations. It is important to keep abreast of technological developments. It is therefore suggested that a study be carried out between new technologies, namely Artificial Intelligence and the Internet of Things, and the implementation of NIS 2 in organizations.

https://doi.org/10.58086/625w-1k44

5. Conclusion

This bibliometric review paper has provided a comprehensive analysis of the current state of cybersecurity, security in cyberspace, and the application of the NIS and NIS 2 directives. The analysis has highlighted the growing importance of cybersecurity in the digital age as well as the evolving nature of threats in cyberspace.

Firstly, the review highlighted the growing importance of cybersecurity in protecting critical infrastructure, digital services, and personal data. The multiplication of digital technologies and interconnected systems has increased the vulnerability of organizations and individuals to cyber threats. As evidenced by bibliometric analysis, there has been an increase in research output and academic publications focused on cybersecurity, reflecting the growing attention and resources devoted to addressing cyber risks. This underscores the urgency of implementing robust cybersecurity measures to mitigate potential disruptions and protect sensitive information.

Secondly, the review clarified the main components and objectives of the NIS and NIS 2 directives, underlining their role in strengthening the resilience of essential services and digital infrastructures. The directives aim to strengthen cooperation between EU member states, promote risk management practices, and build incident response capabilities to effectively tackle cyber incidents. The review revealed a growing body of literature examining the implications and challenges associated with implementing these directives, highlighting the importance of regulatory frameworks in enhancing cybersecurity preparedness and response.

Additionally, the review highlighted the imperative need to promote a culture of cybersecurity awareness and resilience, both at the organizational and societal levels. Effective cybersecurity measures require not only technological solutions but also a proactive and vigilant mindset on the part of users and stakeholders.

In conclusion, this literature review article has provided valuable insights into the current landscape of cybersecurity, security in cyberspace, and the application of the NIS and NIS 2 directives. The findings highlight the multifaceted nature of cybersecurity challenges and the need for a holistic and collaborative approach to strengthening digital resilience. As the digital ecosystem continues to evolve, it is imperative that policymakers, industry leaders, and researchers remain vigilant and proactive in addressing cyber threats and advancing cybersecurity capabilities.

Bibliographic references

Bagnato, D. (2020). The network information systems directive (EU) 2016/1148: internet service providers and registraties. *Central and Eastern European eDem and eGov Days*, *338*, 111–122. https://doi.org/10.24989/ocg.v.338.9

Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, *3*(1), 35–49. https://doi.org/10.1365/s43439-022-00048-9

Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, *3*(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

Carrapico, H., & Farrand, B. (2017). 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law, and Social Change*, *67*(3), 245–263. https://doi.org/10.1007/s10611-016-9652-4

Cesarec, I. (2020). Beyond physical threats: Cyber-attacks on critical infrastructure as a challenge of changing security environment – overview of cyber-security legislation and implementation in SEE countries. *Annals of Disaster Risk Sciences*, *3*(1). https://doi.org/10.51381/adrs.v3i1.45

Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review*, *3*(2), 255–272. https://doi.org/10.1365/s43439-022-00067-6

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS directive compliant cybersecurity maturity assessment framework. *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*.

Ducuing, C. (2021). Understanding the rule of prevalence in the NIS directive: C-ITS as a case study. *Computer Law and Security Report*, *40*(105514), 105514. https://doi.org/10.1016/j.clsr.2020.105514

Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact? *Scientometrics*, *105*(3), 1809–1831. https://doi.org/10.1007/s11192-015-1645-z

Falih, N., Jabir, B., & Rahmani, K. (2019). Systemic approach for optimizing information technology resource as a contribution of information system governance. *Indonesian Journal of Electrical Engineering and Computer Science*, *14*(1), 135. https://doi.org/10.11591/ijeecs.v14.i1.pp135-142

Ferguson, D. D. S. (2022). European Cybersecurity Certification Schemes and cybersecurity in the EU internal market. *International Cybersecurity Law Review*, *3*(1), 51–114. https://doi.org/10.1365/s43439-021-00044-5

Fitzgerald, T., & Peltier, T. (2016). *Information security governance simplified: From the boardroom to the keyboard*. CRC Press.

Franke, U., Turell, J., & Johansson, I. (2021). The cost of incidents in essential services—data from Swedish NIS reporting. In *Critical Information Infrastructures Security* (pp. 116–129). Springer International Publishing.

Hicks, D., Wouters, P., Waltman, L., de Rijcke, S., & Rafols, I. (2015). Bibliometrics: The Leiden Manifesto for research metrics. *Nature*, *520*(7548), 429–431. https://doi.org/10.1038/520429a

Hulatt, D., & Stavrou, E. (2021). The development of a multidisciplinary cybersecurity workforce: An investigation. In *Human Aspects of Information Security and Assurance* (pp. 138–147). Springer International Publishing. https://doi.org/10.1007/978-3-030-81111-2_12

Koltay, T. (2016). Data governance, data literacy and the management of data quality. *IFLA Journal*, *42*(4), 303–312. https://doi.org/10.1177/0340035216672238

Korablyov, M., & Lutskyy, S. (2022). System-information models for intelligent information processing. *Innovative Technologies and Scientific Solutions for Industries*, *3(21)*, 26–38. https://doi.org/10.30837/itssi.2022.21.026

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., & Ioannidis, S. (2020). Cybersecurity in the Era of Digital Transformation: The case of Greece. *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)*. https://doi.org/ 10.1109/ITIA50152.2020.9312297

Mekovec, R., & Peras, D. (2020). Implementation of the general data protection regulation: Case of higher education institution. *International Journal of E-Education e-Business e-Management and e-Learning*, *10*(1), 104–113. https://doi.org/10.17706/ijeeee.2020.10.1.104-113

Michelberger, P., & Kemendi, Á. (2020). Data, information and it security - software support for security activities. *Problems of Management in the 21st Century*, *15*(2), 108–124. https://doi.org/10.33225/pmc/20.15.108

Moher, D. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine*, *151*(4), 264. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

Mukherjee, D., Lim, W. M., Kumar, S., & Donthu, N. (2022). Guidelines for advancing theory and practice through bibliometric research. *Journal of Business Research*, *148*, 101–115. https://doi.org/10.1016/j.jbusres.2022.04.042

Park, M., & Chai, S. (2018). Internalization of information security policy and information security practice: A comparison with compliance. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics: EJHG*, *28*(6), 697–705. https://doi.org/10.1038/s41431-020-0596-x

Penev, L. (2019). Data ownership and data publishing. *ARPHA Conference Abstracts*, *2*. https://doi.org/10.3897/aca.2.e39250

Ponsard, C., Grandclaudon, J., & Massonet, P. (2021). A goal-driven approach for the joint deployment of safety and security standards for operators of essential services. *Journal of Software (Malden, MA)*, *33*(9). https://doi.org/10.1002/smr.2338

Pravdiuk, A. (2023). Information security of Ukraine: Information influence and information wars. *European Political and Law Discourse*, *10*(1), 111–121. https://doi.org/10.46340/eppd.2023.10.1.6

Riesco, R., & Villagrá, V. A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL). *International Journal of Information Security*, *18*(6), 715–739. https://doi.org/10.1007/s10207-019-00433-2

Salvaggio, S. A., & González, N. (2023). The European framework for cybersecurity: strong assets, intricate history. *International Cybersecurity Law Review*, *4*(1), 137–146. https://doi.org/10.1365/s43439-022-00072-9

Sato, Y., Hasegawa, H., & Takakura, H. (2019). Construction of Secure Internal Networks with Communication Classifying System. In *ICISSP* (pp. 552-557). DOI: 10.5220/0007571905520557

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad009

Schmitz-Berndt, S., & Schiffner, S. (2021). Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR. *International Review of Law Computers & Technology*, *35*(2), 101–115. https://doi.org/10.1080/13600869.2021.1885103

Skias, D., Tsekeridou, S., Zahariadis, T., Voulkidis, A., Velivassaki, T.-H., & Fotiadou, K. (2021). Pan-European cybersecurity incidents information sharing platform to support NIS directive. *Proceedings of the 16th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3465481.3470477

The Lens. (n.d.). Explore Global Science and Technology Knowledge. https://www.lens.org/

Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using models to enable compliance checking against the GDPR: An experience report. *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*. DOI: 10.1109/MODELS.2019.00-20

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law and Security Report*, *34*(3), 450–466. https://doi.org/10.1016/j.clsr.2017.12.004

Voitsekhovska, M. M., Dorosh, M. S., Grechaninov, V. F., & Verenych, O. V. (2022). Functional modeling of the organization's information security culture state monitoring system development. *Herald of Advanced Information Technology*, *5*(4), 297–308. https://doi.org/10.15276/hait.05.2022.22

Wallis, T., & Johnson, C. (2020). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. DOI: 10.1109/CyberSA49311.2020.9139641

Wang, M., & Chai, L. (2018). Three new bibliometric indicators/approaches derived from keyword analysis. *Scientometrics*, *116*(2), 721–750. https://doi.org/10.1007/s11192-018-2768-9

Zlateva, P., & Hadjitodorov, S. (2022, September). An approach for analysis of critical infrastructure vulnerability to climate hazards. *In IOP Conference Series: Earth and Environmental Science* (Vol. 1094, No. 1, p. 012004). IOP Publishing. DOI 10.1088/1755-1315/1094/1/012004

Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods*, *18*(3), 429–472. https://doi.org/10.1177/1094428114562629

Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/gtcy-wt23

BIBLIOMETRIC STUDY ON THE DEVELOPMENT AND IMPLEMENTATION OF CYBERSECURITY IN AUTONOMOUS VEHICLES

Henrique Teixeira[1]

Mário Lousã[2]

José Morais[3]

Abstract

The main objective was to examine the trajectory of scientific research in this domain, identify the most influential publications related to cybersecurity in autonomous vehicles and pinpoint research opportunities, supported by the PRISMA method. Additionally, the study explores cybersecurity themes in autonomous vehicles, emphasizing the significance of concepts like blockchain, machine learning, and deep learning essential in formulating business strategies. Furthermore, the research identifies influential scientific publications, predominant journals, the most productive countries, and authors with the most publications on cybersecurity in autonomous vehicles. It identifies research opportunities organized into two distinct clusters to provide a comprehensive understanding of the current state of research in this field and offer insights for companies and academics interested in contributing to future advancements in the cybersecurity of autonomous vehicles. The article demonstrates that cybersecurity is a fundamental area for the development and implementation of secure and reliable autonomous vehicles.

Keywords: V2X (vehicles-to-everything) network security; 5G and 6G; mobility security; communication network security; attack prevention.

ESTUDO BIBLIOMÉTRICO SOBRE O DESENVOLVIMENTO E IMPLEMENTAÇÃO DA CIBERSEGURANÇA EM VEÍCULOS AUTÓNOMOS

Resumo

O objetivo principal foi examinar a trajetória da investigação científica neste domínio, identificar as publicações mais influentes relacionadas com a cibersegurança em veículos autónomos e identificar oportunidades de investigação, apoiadas pelo método PRISMA. Além disso, o estudo explora temas de segurança cibernética em veículos autónomos, enfatizando a importância de conceitos como blockchain, aprendizado de máquina e aprendizado profundo, essenciais na formulação de estratégias de negócios. Além disso, a pesquisa identifica publicações científicas influentes, periódicos predominantes, os países mais produtivos e os autores com mais publicações sobre segurança cibernética em veículos autónomos. Identifica oportunidades de investigação organizadas em dois clusters distintos para fornecer uma

[1] ISPGAYA, Instituto Superior Politécnico Gaya, Portugal

[2] CID ISPGAYA; ISPGaya /Instituto Superior Politécnico Gaya, Portuga

[3] CEOSP.PP; ISPGaya /Instituto Superior Politécnico Gaya, Portugal

https://doi.org/10.58086/7edc-2s28

compreensão abrangente do estado atual da investigação neste campo e oferecer insights para empresas e académicos interessados em contribuir para avanços futuros na segurança cibernética de veículos autónomos. O artigo demonstra que a cibersegurança é uma área fundamental para o desenvolvimento e implementação de veículos autónomos seguros e fiáveis.

Palavras-chave: segurança de rede V2X (veículos para tudo); 5G e 6G; segurança da mobilidade; segurança de redes de comunicação; prevenção de ataques.

Introduction

Technological advances are profoundly redefining the autonomous vehicle landscape, influencing the way we move, and raising essential cybersecurity considerations. As interconnection and automation become integral parts of autonomous vehicles, new challenges and opportunities arise in ensuring cybersecurity (Bathla et al., 2022). The rapid pace of technological advances in the autonomous vehicle landscape raises critical cybersecurity considerations, making them increasingly susceptible to a wide range of cyber threats (Sun et al., 2022). The growing dependence on various autonomous systems and their interaction with intelligent systems in urban traffic infrastructure has further expanded the threat landscape, making cybersecurity a growing concern (Chattopadhyay et al., 2021).

There are several factors that influence the adoption of autonomous vehicles, where efficiency and trust in technologies play essential roles. Acheampong and Cugurullo (2019) state that vehicle efficiency, convenience, driving experience, and trust in autonomous technologies are crucial for the acceptance and adoption of these technologies. By prioritizing cybersecurity in autonomous vehicles, businesses and the automotive industry can strengthen their strategies for responding to cybersecurity threats. The growing presence of digital capabilities through 6G technology requires a robust approach to ensure the continued safety of autonomous vehicles (Algarni & Thayananthan, 2023).

This paper aims to guide future research on crucial elements contributing to the advancement of the cybersecurity concept in autonomous vehicles. Divided into four parts, it reviews the current literature on cybersecurity in this context, presents the methodology used, analyzes the results obtained from bibliometric analysis, and concludes with final considerations. This article is supported by bibliometric analysis, focusing on cybersecurity in autonomous vehicles, and seeks to answer the following four questions:

- RQ1: How has the concept of cybersecurity in autonomous vehicles evolved in academic research over the past 20 years?
- RQ2: What are the most influential scientific publications on cybersecurity in autonomous vehicles?

https://doi.org/10.58086/7edc-2s28

– RQ3: What are the main authors and papers in scientific publications on cybersecurity in autonomous vehicles?
– RQ4: What are the main focuses of research in the field of cybersecurity in autonomous vehicles?

2. Literature review

2.1. Cybersecurity

Cybersecurity has received significant attention in recent years due to the increasing number of threats and continuous efforts by cybercriminals to overcome security barriers. According to Taherdoost (2022), the process involves protecting sensitive data against unauthorized access, damage, or theft. Sabillon (2018) defines cybersecurity as the protection of information assets, dealing with threats to information processed, stored, and transported by interconnected information systems. Additionally, Sallos et al. (2019) tells us that cybersecurity is increasingly being recognized as a "knowledge problem," emphasizing the need to understand vectors, mechanisms, and trends related to knowledge to address cybersecurity challenges.

As the digital landscape continues to evolve, the importance of cybersecurity in various domains such as health, critical infrastructure, and the automotive industry has become increasingly prominent. Cybersecurity, in the digital era, stands out for its importance and complexity, increased by its interdisciplinary nature. Its areas of application are diverse, from industry to education and health. For example, according to Gordon et al. (2022), cybersecurity is identified as a necessity for the provision of reliable healthcare, especially in the context of robotic surgery. In the automotive industry, according to Wang et al. (2021), there has been an increase in the development of solutions to address increasing incidents of security threats. At the same time, several cybersecurity practices emerged, presenting variations between different industrial areas regarding risks and respective mitigations (Héroux & Fortin, 2020).

2.2. Autonomous vehicles

Autonomous vehicles can transform urban transportation systems, providing safer roads, improving mobility, and enhancing traffic efficiency (Li et al., 2022). According to Qu et al. (2022), autonomous vehicles are equipped with sensors that can perceive environmental information to make informed decisions. For example, lane change is the most common scenario (Wu et al., 2020). In the decision-making process, Guo (2023) states that continuous learning is frequent, incorporating risk awareness and replicating human behaviors to ensure intuitive understanding by other road users.

https://doi.org/10.58086/7edc-2s28

The implementation of autonomous vehicles raises important considerations in terms of policies, responsibility, and security (Alheeti et al., 2016). According to Nees (2016), there is a need for policies and changes in infrastructure to prepare cities for the integration of autonomous vehicles into existing urban transportation systems. Additionally, Nyholm and Smids (2016) ensure that the security of autonomous vehicles and their communication networks is crucial to preventing intrusions and attacks. Autonomous vehicles, according to Muhammad et al. (2020), have the potential to significantly impact road transportation systems, traffic flow, and user acceptance.

Table 1 summarizes the concepts of cybersecurity and autonomous vehicles.

Table 1
Cybersecurity and Autonomous Vehicles Concepts

Concept	Description	Authors
Cybersecurity	Refers to a set of activities and other measures aimed at protecting computers, computer networks, hardware, related devices, software, and the information they contain and communicate, as well as other elements in cyberspace, from attacks, disruptions, or other threats.	Fischer, 2016; Reegård et al., 2019; Veale et al., 2020
Autonomous Vehicles	Refers to vehicles capable of operating and moving without the need for direct human intervention. The autonomy of vehicles can vary at different levels, from driver assistance to complete autonomy, where the vehicle can travel the entire route without requiring human intervention.	Kato et al., 2015; Wachenfeld & Winner, 2016; J. Wang et al., 2020

3. Methodology

Bibliometric analysis is a valuable tool for assessing the impact and influence of scientific production in various areas. It involves, for example, the statistical analysis of published articles and their citations to measure their impact (Baraibar-Diez et al., 2020). However, it is important to note that bibliometric analysis has limitations. It is retrospective in nature, and developments in the literature only become apparent after some time has passed (Coombes, 2023). Bibliometric analysis methods are employed to provide a comprehensive perspective on published scientific articles. This approach is based on processing bibliometric data collected from databases such as Scopus, The Lens, or Web of Science. In recent years, there has been an increase in the application of bibliometric methods in research papers, driven by their reliability and, above all, their effectiveness (Mukherjee et al., 2022).

The methodological foundation of this bibliometric analysis was established using the PRISMA method, which provides a set of guidelines for the preparation of systematic reviews and meta-analyses (Page et al., 2023).

To carry out this study, the database selected was The Lens, a free and accessible data source containing 151.9 million patents and 266.4 million scientific articles and research works in various areas (The Lens, n.d.).

https://doi.org/10.58086/7edc-2s28

The keywords "cybersecurity" and "autonomous vehicles" were used for the complex boolean search, employing the AND and OR operators between the two expressions to encompass more literature. The analysis focused on the last 20 years, restricting publications to the period between 2004 and 2023. To obtain more specific results for this study, subjects such as "Control and Systems Engineering," "Automotive Engineering," and "Computer Networks and Communications" were selected, along with the study fields "computer science," "engineering," "computer security," "Control (management)," and "Control engineering," resulting in a total of 3028 publications. For the analysis and visualization of the obtained data, VOSviewer version 1.6.19 software and The Lens analysis tool were used.

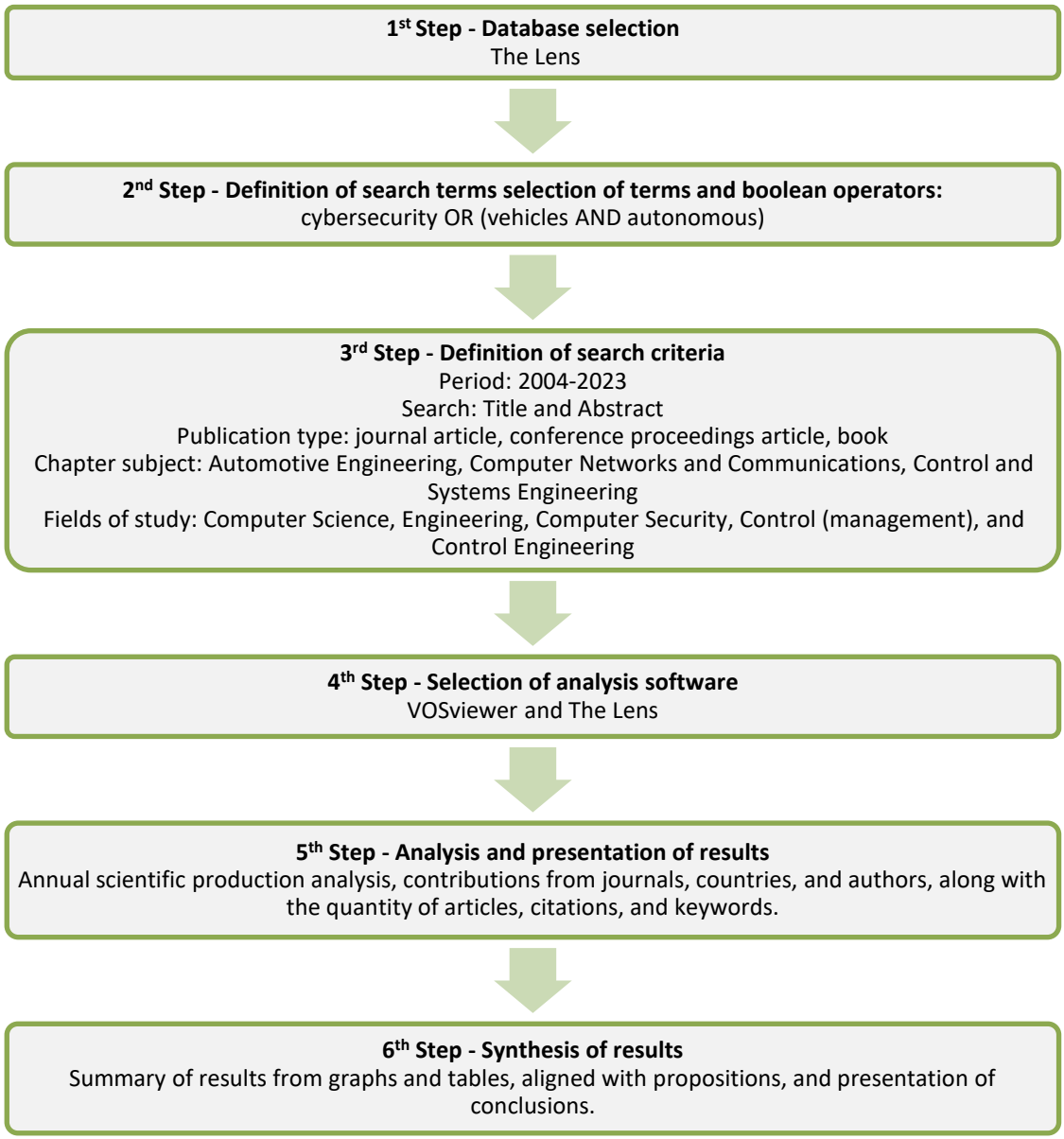
The analysis covers the distribution of publications over the 20 years analyzed, identifying the five types of considered documents: books, conference proceedings, book chapters, journal articles, and conference papers. The top 10 journals contributing the most publications, the top 10 countries with the highest production, the top 10 prominent authors, and the top 10 most cited articles are highlighted. Finally, co-authorship analysis, co-citation analysis, keyword analysis, and cluster analysis of keywords are part of stage five (cf. Figure 1).

Figure 1 presents the methodology used in the research, based on the PRISMA method, consisting of six stages (database selection; definition of search terms and Boolean terms and operators; definition of search criteria; selection of analysis software; analysis and presentation of results; synthesis of results).

https://doi.org/10.58086/7edc-2s28

Figure 8

Methodology



4. Analysis

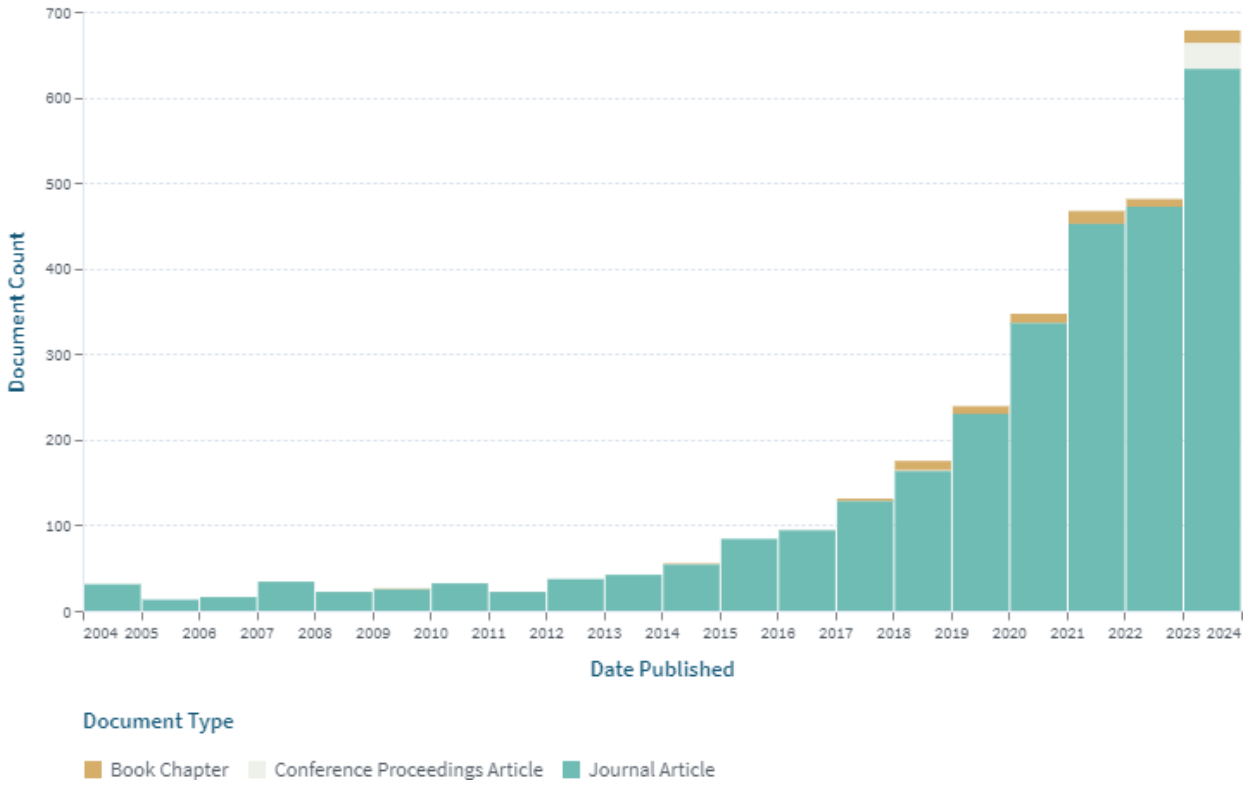
4.1. Evolution of academic research over the last 20 years on the concept of cybersecurity in autonomous vehicles (RQ1)

This study covers a total of 3280 documents over a 20-year period, spanning from 2004 to 2023. Figure 2 illustrates the annual volume of scientific production resulting from the conducted research, considering the elements presented in steps 2 and 3 of Figure 1. Thus, it is possible to observe an increase in annual scientific production on the topic of "Cybersecurity in Autonomous Vehicles". In 2004, 31 documents were published, while in 2023, this number rose to 678, representing a growth of 2187%, with a steady annual increase from 2011 onwards.

https://doi.org/10.58086/7edc-2s28

Figure 2

Evolution of the number of publications by document type



4.2. Most influential scientific publications on cybersecurity in autonomous vehicles (RQ2)

The results indicate that 3028 documents were published in 110 different journals, with the top 10 representing 82% of the total with 2484 publications (cf. Figure 2 and Table 2). IEEE occupies first place with 909 publications in the areas of engineering, automotive industry, and security.

Table 2

Top 10 Journals by Number of Publications

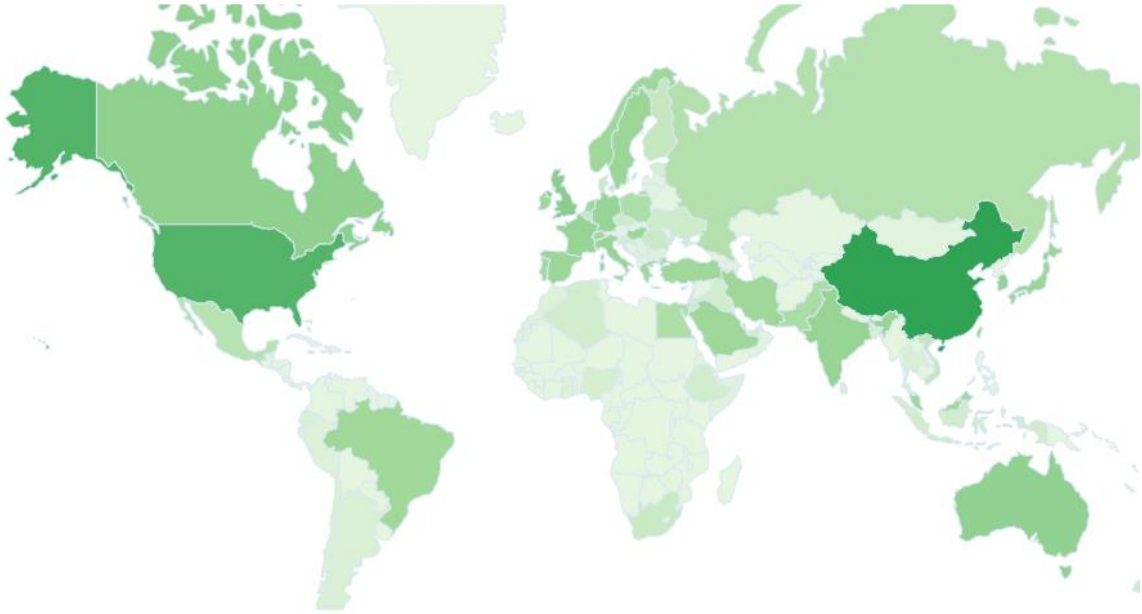
Journal	Fields	Number of publications
Institute of Electrical and Electronics Engineers (IEEE)	Engineering; Automotive Industry; Security.	909
Elsevier BV	Academic and Governmental; Health; Industry.	592
Springer Science and Business Media LLC	Engineering; Medicine; Computing; Mathematics.	221
MDPI AG	Computing; Mathematics; Behavioral Science.	220
Wiley	Computing and Technology; Earth, Spaces, and Environment.	135
Hindawi Limited	Mathematics, Engineering, and Computing; Social Sciences and Education.	94
Informa UK Limited	Science, Technology, and Medicine; Humanities and Social Sciences.	92

https://doi.org/10.58086/7edc-2s28

Journal	Fields	Number of publications
Inderscience Publishers	Computer Science and Mathematics; Risk Management, Security, and Emergencies; Science, Engineering, and Technology.	82
Institute of Electrical and Electronics Engineers Inc.	Engineering; Automotive Industry; Security.	81
Emerald	Sustainability; Health; Mathematics.	55

In Figure 4, it shows the most active countries in the production of scientific publications in this area, highlighting China and the United States of America with the highest number of publications.

Figure 4
Scientific Production by Country



Complementing the representation in Figure 4, Table 3 shows the top 10 leading countries in terms of production in research dedicated to the topic of cybersecurity in autonomous vehicles.

Table 3
Top 10 Countries with the greatest number of publications

Country	Number of publications
China	876
USA	611
United Kingdom	188
Canada	148
Australia	143
Republic of Korea	110
France	88
India	86
Germany	80
Italy	74

https://doi.org/10.58086/7edc-2s28

4.3. Main authors and papers of scientific publications on cybersecurity in autonomous vehicles (RQ3)

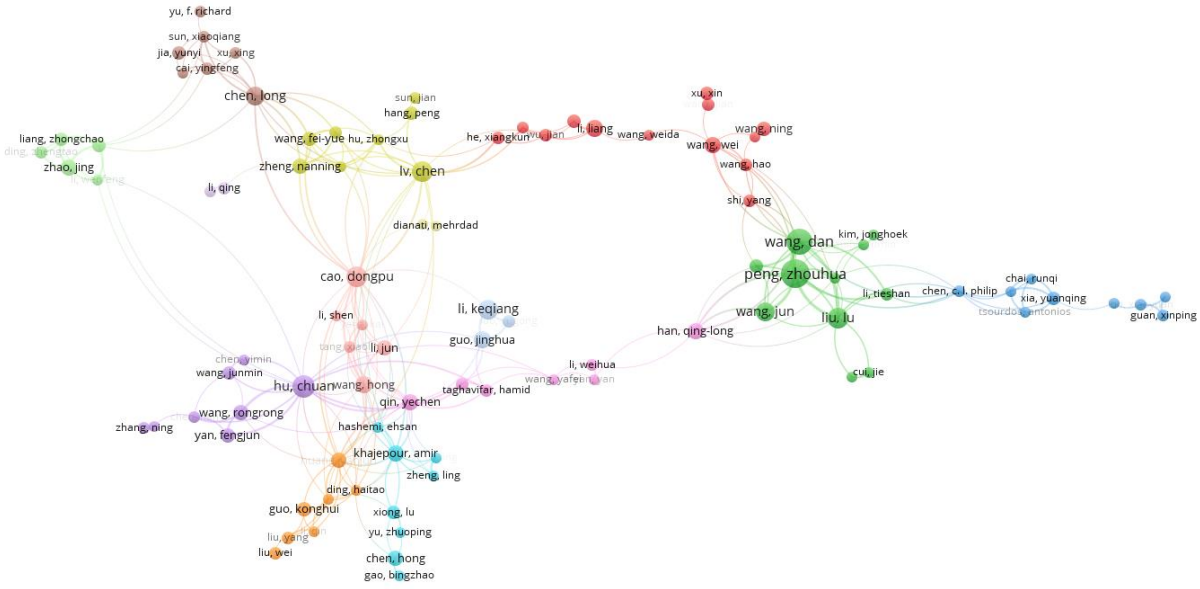
Table 4 highlights the main authors in scientific production, revealing Dan Wang as the most productive author with twenty-six publications. Following, Zhouhua Peng and Chuan Hu appear with twenty-five and eighteen publications, respectively. It is observed that many of the authors presented in Table 4 are from the Asian continent, especially China, indicating their leadership in scientific production in the context of research that addresses the terms “cybersecurity” or “autonomous vehicles”.

Table 4
Number of Published Articles per Author

Authors	Number of publications	Affiliation
Dan Wang	26	Dalian Maritime University, China
Zhouhua Peng	25	Dalian Maritime University, China
Chuan Hu	18	Southeast University, China
Chen Lv	17	Nanyang Technological University, China
Keqiang Li	12	Tsinghua University, China
Amir Khajepour	11	Beijing Institute of Technology, China
Balázs Németh	11	Hungarian Academy of Sciences, Hungary
Bidyadhar Subudhi	10	National Institute of Technology, India
Amr Mohamed	9	University of Ontario Institute of Technology, Canada
António M Pascoal	8	University of Lisbon, Portugal

According to Zupic and Čater (2015), the co-authorship method can reveal patterns of collaboration and productivity among researchers. A total of 173 authors were found in the context of the analysis, each having at least five published documents. Out of these authors, 96 were selected, divided into 14 clusters, with a total of 260 connections. Figure 5 demonstrates the connections among them. The green cluster features the author with the most co-authorships, Zhouhua Peng.

Figure 5
Author Relationships per Document



https://doi.org/10.58086/7edc-2s28

The articles with the highest number of citations are "Planning and decision-making for autonomous vehicles" (Schwarting et al., 2018), with 538 citations, and "Perception, planning, control, and coordination for autonomous vehicles" (Pendleton et al., 2017), with 403 citations. It is also noted that the most cited paper is the one with the highest average annual citations (107.6).

Table 5
Top 10 Most cited papers

Article	Year of publication	Citations	Average*
Chwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and decision-making for autonomous vehicles. *Annual Review of Control, Robotics, and Autonomous Systems, 1*(1), 187–210.	2018	538	107.6
Pendleton, S., Andersen, H., Du, X., Shen, X., Meghjani, M., Eng, Y., Rus, D., & Ang, M. (2017). Perception, planning, control, and coordination for autonomous vehicles. *Machines, 5*(1), 6.	2017	403	67.2
Arslan, G., Marden, J. R., & Shamma, J. S. (2007). Autonomous vehicle-target assignment: A game-theoretical formulation. *Journal of Dynamic Systems, Measurement, and Control, 129*(5), 584–596.	2007	374	23.4
Amer, N. H., Zamzuri, H., Hudha, K., & Kadir, Z. A. (2017). Modelling and control strategies in path tracking control for autonomous ground vehicles: A review of state of the art and challenges. *Journal of Intelligent & Robotic Systems, 86*(2), 225–254.	2016	261	37.3
Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data, 7*(1).	2020	235	78.3
Qiao, L., & Zhang, W. (2017). Adaptive non-singular integral terminal sliding mode tracking control for autonomous underwater vehicles. *IET Control Theory and Applications, 11*(8), 1293–1306.	2017	223	37.2
Peng, Z., Wang, D., Li, T., & Han, M. (2020). Output-feedback cooperative formation maneuvering of autonomous surface vehicles with connectivity preservation and collision avoidance. *IEEE Transactions on Cybernetics, 50*(6), 2527–2535.	2019	205	51.3
Faessler, M., Fontana, F., Forster, C., Mueggler, E., Pizzoli, M., & Scaramuzza, D. (2016). Autonomous, vision-based flight and live dense 3D mapping with a quadrotor micro aerial vehicle. *Journal of Field Robotics, 33*(4), 431–450.	2015	193	24.1
Yuan, C., Licht, S., & He, H. (2018). Formation learning control of multiple autonomous underwater vehicles with heterogeneous nonlinear uncertain dynamics. *IEEE Transactions on Cybernetics, 48*(10), 2920–2934.	2017	193	32.2
Bingham, B., Foley, B., Singh, H., Camilli, R., Delaporta, K., Eustice, R., Mallios, A., Mindell, D., Roman, C., & Sakellariou, D. (2010). Robotic tools for deep water archaeology: Surveying an ancient shipwreck with an autonomous underwater vehicle. *Journal of Field Robotics, 27*(6), 702–717.	2010	183	14.1

* The average was calculated based on the interval between the year of publication and the year 2023.

https://doi.org/10.58086/7edc-2s28

4.4. Main areas of research on cybersecurity in autonomous vehicles (RQ4)

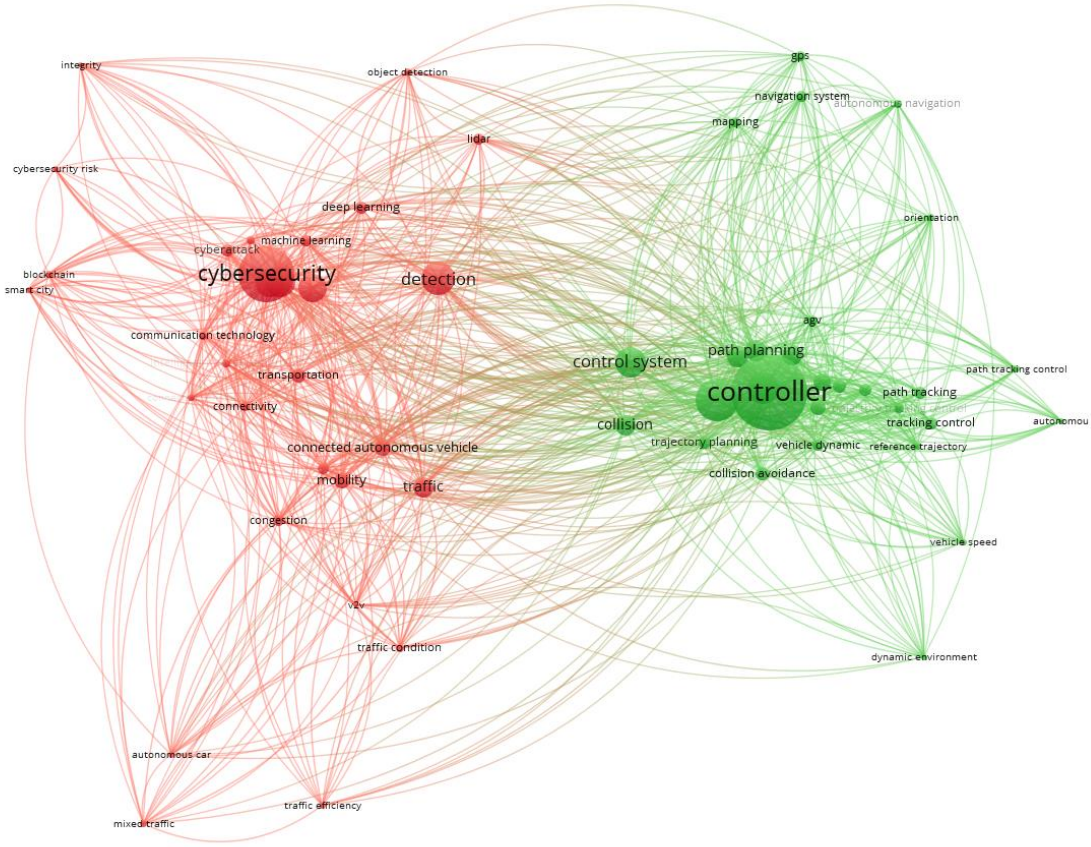
The co-occurrence analysis of the authors' keywords is presented in Figure 6, reflecting the strong connection between cybersecurity and the control system. Keywords with a minimum occurrence of 20 were considered, resulting in a total of 59 keywords distributed across two clusters (cf. Figure 6 and Table 6). The most prominent cluster is the red one, with 30 keywords, where "cybersecurity" is the dominant keyword, recording 323 occurrences. In the green cluster, the keyword "controller" stands out, with 456 occurrences. Table 6 presents the two clusters (red and green) obtained and their respective keywords.

Table 6
Keywords per Cluster

Cluster	Keywords
1 - Red	“Attack”, “autonomous car”, “blockchain”, “cavs”, “communication technology”, “congestion”, “connected autonomous”, “connected vehicle”, “connectivity”, “cyber attack”, cyberattack”, “cybersecurity”, “cybersecurity risk”, deep learning”, “detection”, “integrity”, “inteligente transportation”, “lidar”, “machine learning”, “mixed traffic”, “mobility”, “object detection”, “security”, “smart city”, “threat”, “traffic”, “traffic condition”, “traffic efficiency”, “transportation” e “v2v”.
2 - Green	“agv”, “autonomou”, “autonomous ground vehicle”, “autonomous navigation”, “collision”, “collision avoidance”, “control law”, “control system”, “controller”, “dynamic environment”, “gps”, “mapping”, “navigation system”, “orientation”, “path planning”, “path tracking”, “path tracking control”, “proposed controller”, “reference trajectory”, “tracking”, “tracking control”, “trajectory”, “trajectory planning”, “trajectory tracking”, “trajectory tracking control”, “vehicle model”, “vehicle speed” e “velocity”.

https://doi.org/10.58086/7edc-2s28

Figure 6
Keyword Co-occurrence Network



4.4.1. Cluster 1 – Red

The cluster presents keywords such as "attack", "detection", "traffic", "mobility", and "connected autonomous vehicle", which are interconnected with the context of this paper, specifically with cybersecurity.

According to Craigen et al. (2014), cybersecurity encompasses a wide range of tools, policies, concepts, and technologies aimed at protecting individuals, organizations, and governments from online threats. For Da Veiga (2016), cybersecurity is essential to protecting intelligent resources in cyberspace. Matheu et al. (2020) argue that cybersecurity involves the use of various technologies and protocols to connect physical devices to online infrastructure, especially in scenarios such as the Internet of Things. In this context, Karagiannis et al. (2022) state that the National Institute of Standards and Technology launched the National Initiative for Cybersecurity Education with the aim of providing a systematic framework for education and learning in cybersecurity and establishing concepts and practices adopted by professionals. According to Gcaza and von Solms (2017), the notion of cybersecurity is also linked to the urgency of safeguarding multiple resources simultaneously against a variety of cyber threats, influencing cybersecurity strategies and culture.

https://doi.org/10.58086/7edc-2s28

To address cybersecurity concerns in connected Autonomous Vehicles (AVs), it is crucial to consider potential attacks, detection methods, traffic management, and the impact on mobility. For Liu et al. (2022), AVs are susceptible to various attacks, posing serious security risks. Detection of attacks in AVs can be achieved through advanced technologies such as blockchain or Bayesian attack graphs (Fu et al., 2022; Queralta et al., 2020). These technologies enhance autonomy and provide real-time data for precise location and environment updates, thus improving the detection of potential cyber threats. AVs have the potential to mitigate traffic congestion, increase road safety, and reduce fuel consumption and emissions (Montanaro et al., 2019). However, Martin-Gasulla et al. (2019) state that the initial incorporation of AVs with low penetration rates may result in more limited traffic capabilities. It is essential to develop comprehensive traffic analysis methods and traffic management strategies to ensure the gradual introduction of AVs into existing traffic systems (Zhou et al., 2022). Additionally, the connectivity of AVs, from vehicle to vehicle and infrastructure to vehicle, can significantly improve traffic management and safety by collecting information from nearby vehicles and infrastructures, enhancing their perception capabilities and decision-making processes (Yamazato, 2017).

4.4.2. Cluster 2 – Green

The cluster presents keywords such as "controller", "control system", "collision", "trajectory", "tracking", "path planning", and "autonomous ground vehicle" which are interconnected with the context of this article, specifically with autonomous vehicles.

The development of controllers for autonomous vehicles has increasingly improved their collision prevention capabilities (Tiwari et al., 2021). These controllers are essential to enable autonomous vehicles to navigate complex traffic scenarios and avoid collisions with other vehicles and obstacles (Lin et al., 2020). According to Matous et al. (2021), the development of collision prevention systems for autonomous vehicles has been a key area of development, aiming to provide these vehicles with the ability to react to sudden changes in their environment and avoid potential collisions. Additionally, Lin et al. (2020) highlights the importance of integrating trajectory replanning and vehicle-to-vehicle information interaction in collision prevention control systems. For Guo, J. et al. (2018), an adaptive trajectory control approach based on neural networks was proposed for autonomous vehicle collision prevention control systems, demonstrating stability using Lyapunov theory.

However, Evtukov et al. (2018) argue that attention should be focused on addressing cybersecurity vulnerabilities to prevent external interference with the control unit of an autonomous vehicle. The complexity of data and traffic behaviors in autonomous vehicle networks may enable various types of attacks (Aldhyani & Alkahtani, 2022). To address these challenges, Vitale et al. (2021) propose the

https://doi.org/10.58086/7edc-2s28

development of methodologies to assess the vulnerabilities and impacts of potential cyberattacks on autonomous vehicles.

5. Results

Scientific interest in the field of cybersecurity in autonomous vehicles has been growing over the past 20 years, from 2004 to 2023. In 2004, there were 31 publications, which increased to 678 publications in 2023, representing a growth of 2187%. The year 2012 marked an annual growth of 168%, after which scientific production maintained an upward trend. The significance of cybersecurity in autonomous vehicles has been reinforced due to the emerging availability of technologies such as blockchain, machine learning, and deep learning, as well as the use of technologies like 5G and 6G, making vehicles increasingly interconnected with each other and their environmental context.

Bibliometric analysis revealed that China, the United States, the United Kingdom, and Canada are the most active in producing scientific publications on the topic. This analysis aligns with the level of investment and prioritization of research and development in the area that these countries demonstrate, such as the creation of regulatory policies as indicated using keywords like "guidance law," "regulation," or "law".

Consumer perspectives play a crucial role in the widespread acceptance and adoption of autonomous vehicles. Trust in security, along with other aspects such as reliability and user experience, will significantly influence consumers' willingness to adopt autonomous vehicles. Keywords such as "control design," "awareness," and "cybersecurity awareness" represent the importance in their regard.

By analyzing existing literature, the article provides a comprehensive perspective on the current state, highlighting key themes, trends, and identified security gaps, such as the use of artificial intelligence and environmental connectivity, contributing to reinforcing the need for research by academics and investment by companies.

Aspects such as cybersecurity, reliability, and regulation were identified as key areas. Thus, automotive companies can benefit from this analysis, which identified fundamental elements to be addressed in the cybersecurity of autonomous vehicles.

6. Limitations and future research

As in any study, the present research has some limitations that need to be recognized but may represent a starting point for future work. The results obtained reflect the choices made in steps one to three (Figure

https://doi.org/10.58086/7edc-2s28

1), as described in the methodology section. This includes the selection of the database and the keywords used in the search. Therefore, these decisions represent an inherent limitation of the paper.

For future research, it would be relevant to explore the contributions that technology can provide to boost cybersecurity in autonomous vehicles. The results suggest conducting a study that investigates the relationship between vehicle-to-vehicle and environmental communication and their predictive capabilities.

7. Conclusions

Cybersecurity is a fundamental challenge for the development and implementation of safe and reliable autonomous vehicles. Challenges include the vulnerability of control systems, the possibility of cyber-attacks, and the lack of specific regulations. The development of new security technologies, cooperation between industry and researchers, and collaboration between education and public awareness are opportunities for development.

Bibliographic references

Acheampong, R. A., & Cugurullo, F. (2019). Capturing the behavioural determinants behind the adoption of autonomous vehicles: Conceptual frameworks and measurement models to predict public transport, sharing and ownership trends of self-driving cars. *Transportation Research Part F: Traffic Psychology and Behaviour*, *62*, 349–375. https://doi.org/10.1016/J.TRF.2019.01.009

Aldhyani, T. H. H., & Alkahtani, H. (2022). Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors 2022, Vol. 22, Page 360*, *22*(1), 360. https://doi.org/10.3390/S22010360

Algarni, A. M., & Thayananthan, V. (2023). Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model. *IEEE Access*, *11*, 15284–15296. https://doi.org/10.1109/ACCESS.2023.3244883

Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. (2016). Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks. *Computers 2016, Vol. 5, Page 16*, *5*(3), 16. https://doi.org/10.3390/COMPUTERS5030016

Baraibar-Diez, E., Luna, M., Odriozola, M. D., & Llorente, I. (2020). Mapping Social Impact: A Bibliometric Analysis. *Sustainability 2020, 12*(22), 9389. https://doi.org/10.3390/SU12229389

Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., Kumar, A., Thakur, R. N., & Basheer, S. (2022). Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/7632892

Chattopadhyay, A., Lam, K. Y., & Tavva, Y. (2021). Autonomous Vehicle: Security by Design. *IEEE Transactions on Intelligent Transportation Systems*, *22*(11), 7015–7029. https://doi.org/10.1109/TITS.2020.3000797

Coombes, P. (2023). A review of business model research: what next for industrial marketing scholarship? *Journal of Business and Industrial Marketing*, *38*(3), 520–532. https://doi.org/10.1108/JBIM-06-2021-0296

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 1006–1015. https://doi.org/10.1109/SAI.2016.7556102

Evtukov, S., Golov, E., & Sazonova, T. (2018). Prospects of scientific research in the field of active and passive safety of vehicles. *MATEC Web of Conferences*, *239*, 04018. https://doi.org/10.1051/MATECCONF/201823904018

Fischer, E. A. (2016). *Cybersecurity Issues and Challenges: In Brief*. www.crs.gov

Fu, Y., Wang, C., Wang, F., S., L., Du, Z., & Cao, Z. (2022). An intelligent method for building attack paths based on Bayesian attack graphs. *Https://Doi.Org/10.1117/12.2653480*, *12474*, 264–268. https://doi.org/10.1117/12.2653480

Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. *IFIP Advances in Information and Communication Technology*, *503*, 98–109. https://doi.org/10.1007/978-3-319-58553-6_9

Gordon, W. J., Ikoma, N., Lyu, H., Jackson, G. P., & Landman, A. (2022). Protecting procedural care—cybersecurity considerations for robotic surgery. *Npj Digital Medicine 2022 5:1*, *5*(1), 1–3. https://doi.org/10.1038/s41746-022-00693-8

Guo, J., Luo, Y., & Li, K. (2018). Adaptive coordinated collision avoidance control of autonomous ground vehicles. *Proceedings of the Institution of Mechanical Engineers. Part I: Journal of Systems and Control Engineering*, *232*(9), 1120–1133. https://doi.org/10.1177/0959651818774991

Guo, S. (2023). Automatic driving model based on machine learning agents. *In Fifth International Conference on Computer Information Science and Artificial Intelligence (CISAI 2022)* (Vol. 12566, pp. 859-864). SPIE. https://doi.org/10.1117/12.2667914

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Karagiannis, S., Magkos, E., Karavaras, E., Karnavas, A., Nikiforos, M. N., & Ntantogian, C. (2022). *Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams*. https://doi.org/10.21203/RS.3.RS-1902186/V1

Kato, S., Takeuchi, E., Ishiguro, Y., Ninomiya, Y., Takeda, K., & Hamada, T. (2015). An open approach to autonomous vehicles. *IEEE Micro*, *35*(6), 60–68. https://doi.org/10.1109/MM.2015.133

Li, G., Yang, Y., Li, S., Qu, X., Lyu, N., & Li, S. E. (2022). Decision making of autonomous vehicles in lane change scenarios: Deep reinforcement learning approaches with risk awareness. *Transportation Research Part C: Emerging Technologies*, *134*, 103452. https://doi.org/10.1016/J.TRC.2021.103452

Lin, F., Wang, K., Zhao, Y., & Wang, S. (2020). Integrated Avoid Collision Control of Autonomous Vehicle Based on Trajectory Re-Planning and V2V Information Interaction. *Sensors 2020, Vol. 20, Page 1079*, *20*(4), 1079. https://doi.org/10.3390/S20041079

Liu, Y., Yang, X., Li, M., Wu, M., Sun, C., & Zhou, S. (2022). On the Criteria for Cybersecurity and Risk Assessment Based on ISO/SAE 21434 for the Application of Autonomous Vehicle. *Proceedings of the 2022 International Conference on Computer Science, Information Engineering and Digital Economy (CSIEDE 2022)*, *103*, 134–143. https://doi.org/10.2991/978-94-6463-108-1_16

Martin-Gasulla, M., Sukennik, P., & Lohmiller, J. (2019). Investigation of the Impact on Throughput of Connected Autonomous Vehicles with Headway Based on the Leading Vehicle Type. *Transportation Research Record*, *2673*(5), 617–626. https://doi.org/10.1177/0361198119839989

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A Survey of Cybersecurity Certification for the Internet of Things. *ACM Computing Surveys (CSUR)*, *53*(6), 115. https://doi.org/10.1145/3410160

Matous, J., Basso, E. A., Thyri, E. H., & Pettersen, K. Y. (2021). Unifying Reactive Collision Avoidance and Control Allocation for Multi-Vehicle Systems. *CCTA 2021 - 5th IEEE Conference on Control Technology and Applications*, 76–81. https://doi.org/10.1109/CCTA48906.2021.9658918

Montanaro, U., Dixit, S., Fallah, S., Dianati, M., Stevens, A., Oxtoby, D., & Mouzakitis, A. (2019). Towards connected autonomous driving: review of use-cases. *Vehicle System Dynamics*, *57*(6), 779–814. https://doi.org/10.1080/00423114.2018.1492142

Muhammad, T., Kashmiri, F. A., Naeem, H., Qi, X., Chia-Chun, H., & Lu, H. (2020). Simulation Study of Autonomous Vehicles' Effect on Traffic Flow Characteristics including Autonomous Buses. *Journal of Advanced Transportation*, *2020*. https://doi.org/10.1155/2020/4318652

Mukherjee, D., Lim, W. M., Kumar, S., & Donthu, N. (2022). Guidelines for advancing theory and practice through bibliometric research. *Journal of Business Research*, *148*, 101–115. https://doi.org/10.1016/J.JBUSRES.2022.04.042

Nees, M. A. (2016). Acceptance of Self-driving Cars: An examination of idealized versus realistic portrayals with a self-driving car acceptance scale. In *Proceedings of the human factors and ergonomics society annual meeting 60*(1), pp. 1449-1453. Sage CA: Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/1541931213601332

Nyholm, S., & Smids, J. (2016). The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem? *Ethical Theory and Moral Practice*, *19*(5), 1275–1289. https://doi.org/10.1007/S10677-016-9745-2/METRICS

Page, M. J., Moher, D., Bossuyt, P., Boutron, I., Hoffmann, T., mulrow, cindy, Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., … McKenzie, J. (2023). *PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews*. https://doi.org/10.31222/OSF.IO/GWDHK

Pendleton, S. D., Andersen, H., Du, X., Shen, X., Meghjani, M., Eng, Y. H., Rus, D., & Ang, M. H. (2017). Perception, Planning, Control, and Coordination for Autonomous Vehicles. *Machines 2017, Vol. 5, Page 6*, *5*(1), 6. https://doi.org/10.3390/MACHINES5010006

Qu, D., Zhang, K., Song, H., Wang, T., & Dai, S. (2022). Analysis of Lane-Changing Decision-Making Behavior of Autonomous Vehicles Based on Molecular Dynamics. *Sensors 2022, Vol. 22, Page 7748*, *22*(20), 7748. https://doi.org/10.3390/S22207748

Queralta, J. P., Qingqing, L., Zou, Z., & Westerlund, T. (2020). Enhancing Autonomy with Blockchain and Multi-Access Edge Computing in Distributed Robotic Systems. *2020 5th International Conference on Fog and Mobile Edge Computing, FMEC 2020*, 180–187. https://doi.org/10.1109/FMEC49853.2020.9144809

Reegård, K., Blackett, C., & Katta, V. (2019). *The Concept of Cybersecurity Culture*. In 29th European Safety and Reliability Conference, pp. 4036-4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, *9*(1), 127–137. https://doi.org/10.29019/ENFOQUEUTE.V9N1.214

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041/FULL/XML

Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and Decision-Making for Autonomous Vehicles. *Https://Doi.Org/10.1146/Annurev-Control-060117-105157*, *1*, 187–210. https://doi.org/10.1146/ANNUREV-CONTROL-060117-105157

Sun, X., Yu, F. R., & Zhang, P. (2022). A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6240–6259. https://doi.org/10.1109/TITS.2021.3085297

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics 2022, Vol. 11, Page 2181*, *11*(14), 2181. https://doi.org/10.3390/ELECTRONICS11142181

The Lens. (n.d.). *The Lens - Free & Open Patent and Scholarly Search*. Retrieved December 31, 2023, from https://www.lens.org/

Tiwari, T., Agarwal, S., & Etar, A. (2021). Controller design for autonomous vehicle. *Proceedings of the 2021 1st International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies, ICAECT 2021*. https://doi.org/10.1109/ICAECT49130.2021.9392498

Veale, M., Fundação, I. B., & Vargas, G. (2020). *Standard-Nutzungsbedingungen: Cybersecurity*. https://doi.org/10.14763/2020.4.1533

Vitale, C., Piperigkos, N., Laoudias, C., Ellinas, G., Casademont, J., Escrig, J., Kloukiniotis, A., Lalos, A. S., Moustakas, K., Diaz Rodriguez, R., Baños, D., Roqueta Crusats, G., Kapsalas, P., Hofmann, K. P., & Khodashenas, P. S. (2021). CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks. *Eurasip Journal on Wireless Communications and Networking*, *2021*(1), 1–28. https://doi.org/10.1186/s13638-021-01971-x

Wachenfeld, W., & Winner, H. (2016). The release of autonomous vehicles. *Autonomous Driving: Technical, Legal and Social Aspects*, 425–449. https://doi.org/10.1007/978-3-662-48847-8_21

Wang, J., Zhang, L., Huang, Y., & Zhao, J. (2020). Safety of Autonomous Vehicles. *Journal of Advanced Transportation*, 2020, 1-13. https://doi.org/10.1155/2020/8867757

Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., & Wang, J. (2021). A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automotive Innovation*, *4*(3), 253–261. https://doi.org/10.1007/S42154-021-00140-6

Wu, X., Qiao, B., & Su, C. (2020). Trajectory Planning with Time-Variant Safety Margin for Autonomous Vehicle Lane Change. *Applied Sciences, 10*(5), 1626. https://doi.org/10.3390/APP10051626

Yamazato, T. (2017). V2X communications with an image sensor. *Journal of Communications and Information Networks 2017 2:4*, *2*(4), 65–74. https://doi.org/10.1007/S41650-017-0044-4

Zhou, J., Shen, Z., Wang, X., & Wang, L. (2022). *Unsignalized Intersection Management Strategy for Mixed Autonomy Traffic Streams*. arXiv preprint arXiv:2204.03499. https://doi.org/10.48550/arXiv.2204.03499

Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, *18*(3), 429–472. https://doi.org/10.1177/1094428114562629

Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/0myf-4a66

BIBLIOMETRIC STUDY ON THE IMPORTANCE OF ENDPOINT SECURITY IN COMPANIES

João Gonçalves[1]

Mário Lousã[2]

José Morais[3]

Abstract

This bibliometric study addresses the importance of endpoint security in companies, considering the growing use of information technologies, both in business and personal use. It highlights the need to protect endpoints such as computers, mobile devices, servers, and IoT devices. Endpoint security encompasses measures such as monitoring the files and binaries on and running on the machine using antivirus, data encryption, and threat detection solutions. The literature review highlights the importance of terminology and best practices, highlighting the application of graph-based approaches to strengthen security in medical information networks. Tools such as EDR are cited as essential, especially for small and medium-sized companies. The study emphasizes the importance of business continuity in the face of cyber threats, highlighting the role of artificial intelligence, machine learning, and frameworks. It takes a bibliometric approach, using a specific database to collect bibliometric data on scientific publications published between 2017 and 2023. As a basis for the study, the words "cybersecurity", "endpoint security", "business continuity", and "business" were used. Various analyses of bibliometric results are also presented, including the number of publications by type of document, the scientific journals with the highest number of publications, the countries with the highest number of publications, the number of publications per author, the most cited articles, and the occurrence of identified keywords.

Keywords: Endpoint Security; Business continuity; Vulnerability; Risk; Security threats.

ESTUDO BIBLIOMÉTRICO SOBRE A IMPORTÂNCIA DA SEGURANÇA DE ENDPOINT NAS EMPRESAS

Resumo

Este estudo bibliométrico aborda a importância da segurança de endpoint nas empresas, considerando o crescente uso de tecnologias de informação, tanto no uso empresarial quanto pessoal. Ele destaca a necessidade de proteger terminais como computadores, dispositivos móveis, servidores e dispositivos IoT. A segurança de endpoint abrange medidas como monitoramento de arquivos e binários e em execução na máquina usando antivírus, criptografia de dados e soluções de detecção de ameaças. A

[1] ISPGaya /Instituto Superior Politécnico Gaya, Portugal

[2] CID ISPGAYA; ISPGaya /Instituto Superior Politécnico Gaya, Portugal

[3] CEOSP.PP; ISPGaya /Instituto Superior Politécnico Gaya, Portugal

https://doi.org/10.58086/7edc-2s28

revisão da literatura destaca a importância da terminologia e das melhores práticas, destacando a aplicação de abordagens baseadas em gráficos para fortalecer a segurança nas redes de informação médica. Ferramentas como o EDR são citadas como essenciais, principalmente para pequenas e médias empresas. O estudo enfatiza a importância da continuidade dos negócios diante das ameaças cibernéticas, destacando o papel da inteligência artificial, do aprendizado de máquina e dos frameworks. Adota uma abordagem bibliométrica, utilizando uma base de dados específica para coletar dados bibliométricos sobre publicações científicas publicadas entre 2017 e 2023. Como base para o estudo, foram utilizadas as palavras "cibersegurança", "endpoint security", "businesscontinuity" e "business" foram usados. São também apresentadas diversas análises de resultados bibliométricos, incluindo o número de publicações por tipo de documento, as revistas científicas com maior número de publicações, os países com maior número de publicações, o número de publicações por autor, os artigos mais citados, e a ocorrência de palavras-chave identificadas.

Palavras-chave: Segurança de Endpoint; Continuidade dos negócios; Vulnerabilidade; Risco; Ameaças à segurança.

Introduction

The growing use of information technology has made endpoint security a major concern for companies. Also, with the increase in devices connected to the internet and the rise in cyber threats, it has become essential to guarantee the security of endpoints on a company's network (Shao et al., 2023). Endpoint security encompasses a series of measures designed to protect the various entry points into a network, such as computers, mobile devices, servers, and IoT devices. As companies continue to embrace digital transformation in their businesses, the need to apply robust security measures to their endpoints becomes essential to safeguard sensitive data and ensure business continuity in whatever area of the business it falls under (Yevseiev et al., 2023). With the help of antivirus installed directly on the endpoints, data encryption software, IPS (Intrusion Prevention Systems), Endpoint Threat Detection and Response solution, and NGFW (Next Generation Firewall), greater security of an organization's endpoints is possible, ensuring a greater likelihood of a minimum of false positives or false negatives (Chochliouros et al., 2021).

In this bibliometric study, the main objective is to explore the importance of endpoint security in companies, based on several bibliographic analyses carried out in various scientific articles related to this topic. To this end, a review was carried out of the existing literature on endpoint security, business continuity, and cybersecurity. The number of publications by type of document, the scientific journals with the highest number of publications, the countries with the highest number of publications, the number of publications per author, the most cited articles, and the occurrence of identified keywords were analyzed.

https://doi.org/10.58086/7edc-2s28

1. Literature review

1.1. Endpoint Security

The endpoint security approach refers to the act of protecting the devices used by end users, such as computers, mobile devices, servers, and IoT devices, from potential security threats. It involves implementing measures to protect these devices from unauthorized access, data breaches, malware, and other cyber threats (Sharma et al., 2021). The history of endpoint security goes back to the early days of network computing, when the priority was to protect endpoints connected to the network from external attacks. As technology has evolved, the number of mobile devices and the growing sophistication of cyber threats have increased significantly, causing this concept to evolve to encompass a wide range of security measures aimed at protecting end users' devices and the data they contain (Sarker, 2023). The importance of terminology and good practices in the general IT field was highlighted by Coravos et al. (2020). It is relevant for endpoint security, since the terminology used in this field is crucial for understanding and applying effective security measures.

It is also essential to guarantee the security of endpoints, as this is something with a high level of criticality within cybersecurity, especially in the context of emerging technologies such as the Internet of Things (IoT) and cyber-physical systems (CPS). The increasing complexity and connectivity of endpoints has raised some concerns about the vulnerability of these devices to cyber threats (Ibrahim et al., 2022). According to Angel (2022), the application of graph-based approaches has been proposed to strengthen the security of medical information networks against cyber threats, demonstrating the potential of these methods to significantly improve the performance and capacity of security operations teams. On the other hand, the use of EDR (Endpoint Detection and Response) tools has been referred to as an essential component of information security policies and strategies, particularly in small and medium-sized companies (Noronha et al., 2022). Companies can adopt some approaches combined with some physical tools and equipment to ensure greater endpoint protection, such as EDR, antivirus, NGFW, Domain Name System (DNS) protection and email gateway security (Houhamdi & Athamena, 2021).

1.2. Business continuity

Business continuity is a critical aspect for companies to ensure that their operations are not interrupted, especially by cyber threats caused by malicious agents (Zheng & Omote, 2022).

Based on the literature review on this concept, the importance of assessing the robustness of computer systems to prevent and mitigate risks and computer attacks is emphasized, highlighting the need to implement and apply effective business continuity measures (Kafi & Akter, 2023). Some of these

https://doi.org/10.58086/7edc-2s28

measures involve creating and applying incident response plans to protect financial information and maintain business continuity. Additionally, Simonovich (2020) presents the challenges that companies face in defending their assets, indicating the need for sustainable cybersecurity practices to achieve business continuity in an organization.

In the context of cybersecurity, Sarker (2023) stresses the important role of artificial intelligence (AI), particularly machine learning, in recognizing patterns and predicting malicious activity to avoid disruption and ensure business continuity. Furthermore, George et al. (2021) emphasizes the need for companies, regardless of their involvement in cybersecurity, to adopt sophisticated detection and response mechanisms so that their operations and business continuity are safeguarded.

The evolving nature of cybersecurity threats in general, such as ransomware, malware, and social engineering, requires proactive recovery measures and continuous readiness.

This highlights the importance of recovering from a ransomware attack and planning considerations to mitigate downtime and ensure business continuity (Chen et al., 2021). Rizvi et al. (2022) also stresses the need for progressive frameworks and machine learning techniques to effectively classify and detect malware, especially in zero-day attacks, contributing to the overall goal of maintaining business continuity.

It should also be noted that with the exponential increase in employees working remotely, new challenges have been introduced, as Škiljić (2020) discusses Croatia's response to the increase in cyber threats in the context of remote work, highlighting the risks to business continuity. By implementing real-time monitoring of network traffic in these companies, files that possibly contain viruses or whose corresponding hash is unknown, activities in modern network environments gain a more robust layer of protection, providing not only reactive action on the part of information security analysts but also proactive (Kebande et al., 2021).

1.3. Vulnerability

Vulnerability in the context of cybersecurity refers to a weakness in computer systems, networks, or applications that can be exploited by malicious agents, thus compromising the confidentiality, integrity, or availability of information and resources (Walker-Roberts et al., 2020). These vulnerabilities can come from various sources, such as software failures, incorrect configurations of computer programs, network equipment, or even computers and human errors, thus posing significant risks to the security of organizations and employees themselves (Victor et al., 2023). The constant increase in the use of IoT

https://doi.org/10.58086/7edc-2s28

devices within companies has made them an attractive target for hackers, who are actively trying to exploit these vulnerabilities to launch attacks in a wide variety of ways and techniques.

To reduce the risk of a company being the target of a cyber-attack because its systems and software contain vulnerabilities, various approaches and technologies have been developed. Machine learning, in particular AI based on machine learning, has shown promise in recognizing patterns and predicting potential malicious activities, thus helping to prevent and detect threats to the proper functioning of systems (Mandal et al., 2021). Additionally, Jia et al. (2022) points out that another measure has been developed that will contribute to advances in cybersecurity. Specifically, the development of lightweight DDoS (Distributed Denial-of-Service) schemes in software-defined networking (SDN) contexts has demonstrated reduced false alarm rates, thus improving the ability to effectively identify and respond to DDoS attacks.

In the event of a computer attack, such as ransomware, recovery and imaging operations are crucial. Learning from these incidents can improve planning to prevent and mitigate future attacks, highlighting the importance of preparedness and response strategies. In addition, the robustness of malware detection models is a critical area of study, since evaluating the resilience of these models is essential to ensuring their effectiveness in real-life scenarios (Shahhosseini et al., 2022).

1.4. Endpoint Security, Business Continuity and Vulnerability

Within the area of cybersecurity, the concepts of Endpoint Security, Business Continuity, and Vulnerability complement each other and are all related, although they are different. Endpoint security plays a fundamental role in a company's business continuity. If endpoints are compromised due to vulnerabilities in systems or software, the normal operation of the organization can be interrupted and even incur losses for the company. Therefore, ensuring the security of these endpoints by identifying and correcting known vulnerabilities is a proactive measure to maintain continuity of operations (Ayub et al., 2023).

Table 1 presents descriptions of the three concepts of Endpoint Security, business continuity and vulnerability.

https://doi.org/10.58086/7edc-2s28

Table 1
Concepts of Endpoint Security, Business Continuity and Vulnerability

Concept	Description	Authors
Endpoint Security	Described as the approach of protecting the various endpoints, such as computers, mobile devices, servers, and IoT devices, that are connected to a network. It involves protecting these endpoints from unauthorized access, data breaches, ransomware attacks, and other threats. Endpoint security solutions are crucial for organizations to protect the integrity, confidentiality, and availability of the network and data.	Gao et al. (2021) Goldsack et al. (2020) Heino et al. (2022)
Business Continuity	Refers to the strategic and tactical capacity of an organization to ensure the continuity of its operations during and after a catastrophe or any other significant disruption. It involves a proactive plan to ensure that critical operations continue to function, even after serious security incidents or disasters have occurred, and is considered a fundamental aspect of cyber resilience. This concept becomes important within cybersecurity since organizations need to guarantee the continuity of their operations even in the face of cyber threats and attacks.	Bolpagni (2022) Teichmann et al. (2023) Yang et al. (2022)
Vulnerability	Described as a weakness in a computer system or program that can be exploited by malicious agents to compromise the confidentiality, integrity, or availability of the systems or data processed. Vulnerabilities can come in many forms, including software, hardware, and human factors. They can also be exploited through different attack vectors, such as malware, phishing, social engineering, and DDoS (Distributed Denial-of-Service). Identifying and mitigating vulnerabilities is crucial to maintaining system security and preventing unauthorized access and data breaches.	Baiardi & Tonelli (2021) Taddeo (2019) Tan et al. (2020)

2. Methodology

Bibliometric analysis is an important method for assessing the impact and influence of scientific articles in a specific field. It involves the quantitative analysis of publications, including citation counts, authorship patterns, and journal impact factors. This approach provides information on the productivity and impact of researchers and the evolution of scientific knowledge in each discipline. For a concise analysis, bibliometric data is usually collected from databases such as The Lens, Scopus, or the Web of Science (Aapro et al., 2020).

Taking the theme of this article as a reference, a series of research questions were posed:

- RQ1: How has the topic of endpoint security evolved in academic research over the last six years?
- RQ2: Who are the main authors, countries, and articles in scientific publications related to the topic of endpoint security?
- RQ3: What are the main areas of research in the field of endpoint security?

https://doi.org/10.58086/7edc-2s28

For this bibliometric study, the PRISMA method was used, which consists of a verification of 27 items and a four-phase flowchart, thus helping to guide the researcher through the systematic review process, from the definition of relevant studies to the final inclusion of studies (Zhang et al., 2022).

The database "The Lens" was used, which is widely used as a cost-free platform with millions of patents and scientific articles in the most varied fields of study. This data can then be exported so that it can be processed as the researcher sees fit (The Lens, n.d.). The keywords used in “The Lens” as search categories were “cybersecurity”, “endpoint security”, “business continuity”, and “business”.

With these search criteria, a total of 158 publications were obtained. However, to further delimit the desired publications, with the aim of making them current, some filters were used. In particular, the publication dates of the articles were limited to 2017–2023, and only articles, books, book chapters, and conferences were considered. With these filters, 141 publications were obtained.

To aid this research, the Boolean operators "AND" and "OR" were used strategically with the search terms mentioned in Table 2 (2nd step). Several graphs generated by "The Lens" platform were extracted and included in this document for a more in-depth bibliometric study. Version 1.6.20 of the "VOSviewer" software was also used to carry out the analysis and visualization of the most used terms, referring to the bibliometric data extracted. The following table shows the methodology used in this bibliographical study, in which the PRISMA method was used.

Table 2.
PRISMA methodology applied to bibliometric studies

1st step	Select the database	The Lens
2nd step	Define the search term(s)	cybersecurity AND (endpoint AND (security AND (business AND (continuity OR business))))
3rd step	Specify the search criteria	Time period: 2017-2023; Type of publications: articles, books, book chapters, conference: Field of study: cybersecurity, business.
4th step	Select analysis software	VOSviewer
5th step	Present and analyze the results	Analysis resulting from the results of the bibliometric data collected, regarding scientific publications, authors, number of citations, articles, and keywords.
6th step	Summarizing the results	Based on the results of the graphs and tables, summarize and present conclusions.

3. Bibliometric analysis

3.1. Evolution of academic research over the last six years on the topic of endpoint security (RQ1)

In the six-year period between 2017 and 2023, 141 publications were recorded. According to Figure 1, there has been an increase in the number of publications on the topic’s “cybersecurity”, “endpoint security”, “business continuity”, and “business” over the past six years, especially between 2020 and

https://doi.org/10.58086/7edc-2s28

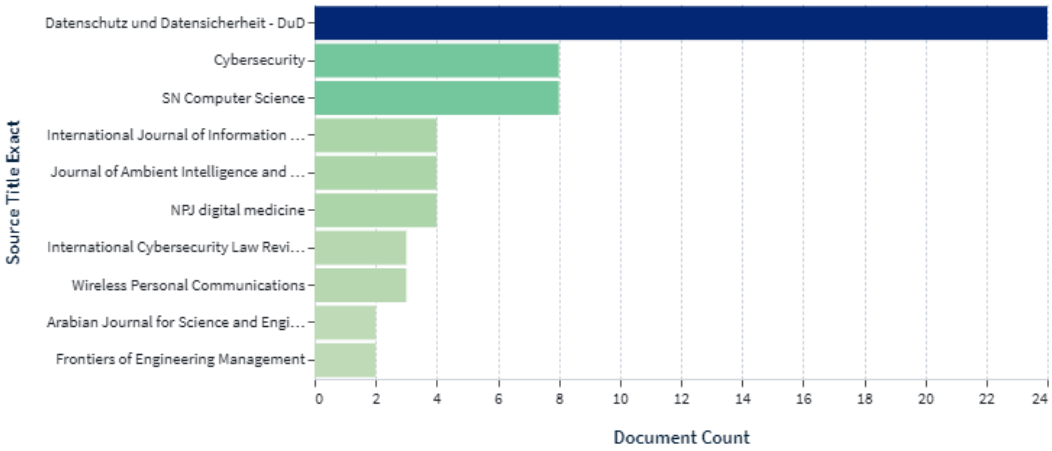
2021. This period coincided with the increase in cyber-attacks on companies around the world, thus creating the need to publish in this area (Wan et al., 2022).

Figure 1
Number of publications by type of document

3.2. Main authors, countries, and articles in scientific publications related to the topic of endpoint security (RQ2)

Figure 2 presents the 10 scientific journals with the most publications, with "Datenschutz und Datensicherheit - DuD" leading the list with 24 publications.

Figure 2
10 Journals with the most publications



Among the 10 countries with the highest number of publications of scientific material, the United States appears with 18 publications, followed by India with 17 (cf. Table 3).

https://doi.org/10.58086/7edc-2s28

Table 3
Countries with the most publications

Country	Number of publications
United States of America	18
India	17
China	10
United Kingdom	10
Italy	7
Saudi Arabia	7
Australia	6
Spain	5
Spain	4
Ireland	4

Figure 3 shows the 10 authors with the most publications, with no major difference between them. The author with the most publications under the defined terms is Andrea Coravos, with three from the Harvard-MIT Center for Regulatory Science, associated with digital medicine. The following six authors have two publications, showing that there is no author or authors who stand out with many publications in this area.

Figure 3
Number of publications per author

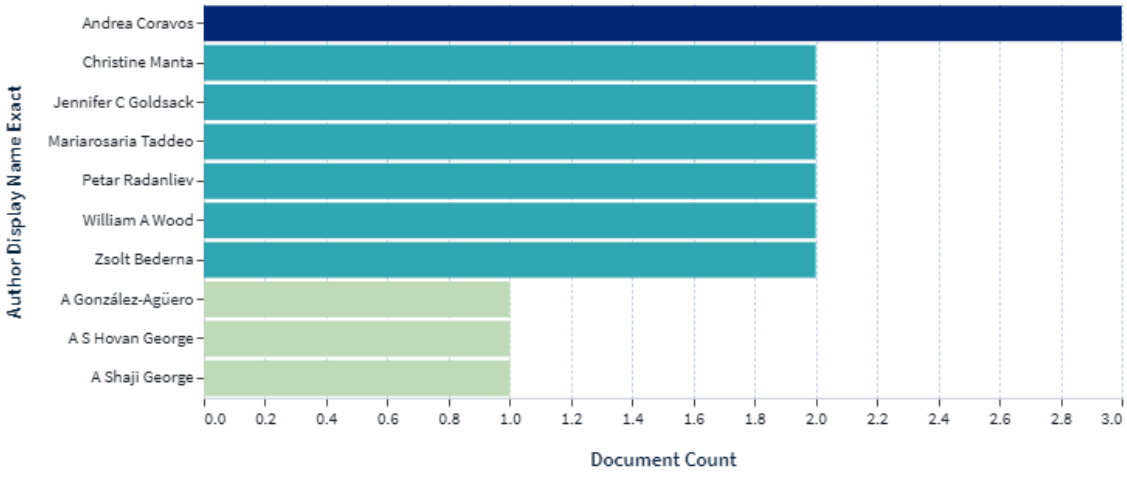


Table 4 presents the data corresponding to the 10 publications with the highest number of citations. The first article on the list was cited 217 times and published in 2020. The second and third articles on the list were cited 181 and 140 times, respectively. Next, the fifth most cited publication has 73 citations, almost half compared to the previous publication. It appears that the three articles with the highest number of citations are associated with the health area, more specifically digital medicine.

https://doi.org/10.58086/7edc-2s28

Table 4.
10 most cited articles

Title	DOI	Year of publication	Number of times cited
Verification, analytical validation, and clinical validation (V3): the foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs)	10.1038/s41746-020-0260-4	2020	217
Developing and adopting safe and effective digital biomarkers to improve patient outcomes	10.1038/s41746-019-0090-4	2019	181
Digital health for optimal supportive care in oncology: benefits, limits, and future perspectives	10.1007/s00520-020-05539-1	2020	140
Internet of Things: information security challenges and solutions	10.1007/s10586-018-2823-6	2018	73
A Systematic Review on AI-based Proctoring Systems: Past, Present and Future	10.1007/s10639-021-10597-x	2021	56
Modernizing and designing evaluation frameworks for connected sensor technologies in medicine	10.1038/s41746-020-0237-3	2020	54
Threats on the horizon: understanding security threats in the era of cyberphysical systems	10.1007/s11227-019-03028-9	2019	46
A Review on the Security of the Internet of Things: Challenges and Solutions	10.1007/s11277-021-08348-9	2021	39
Self-Service Cybersecurity Monitoring as Enabler for DevSecOps	10.1109/access.2019.2930000	2019	34
Provenance-Aware Knowledge Representation: A Survey of Data Models and Contextualized Knowledge Graphs	10.1007/s41019-020-00118-0	2020	33

3.3. Main areas of research in the field of endpoint security (RQ3)

Analyzing the keywords of scientific publications is important to understand the focus and scope of the work. By examining the keywords used by authors, researchers can gain insights into key themes, concepts, and areas of interest in each field of study. According to Ghadi et al. (2021), this process can help find and identify relevant literature, understand current trends, and establish connections between different pieces of research.

Based on the collection of bibliometric data and its processing in the “VOSviewer” software, 12 keywords cited by the authors of the analyzed publications were identified, as can be seen in Figure 4. The most frequent keywords were “security” with 33 occurrences and “attack” with 32. Considering the theme of this study and the two most cited keywords, these terms are linked to the scope of the study since the

https://doi.org/10.58086/7edc-2s28

importance of endpoint security is intrinsically linked to security and attack, because when trying to defend or protect something, there is a risk of some type of attack (Rao & Deebak, 2023).

As a result of analyzing the occurrences of keywords, three clusters were identified, as shown in Table 5 and Figure 4.

Figure 4.
Keyword occurrences

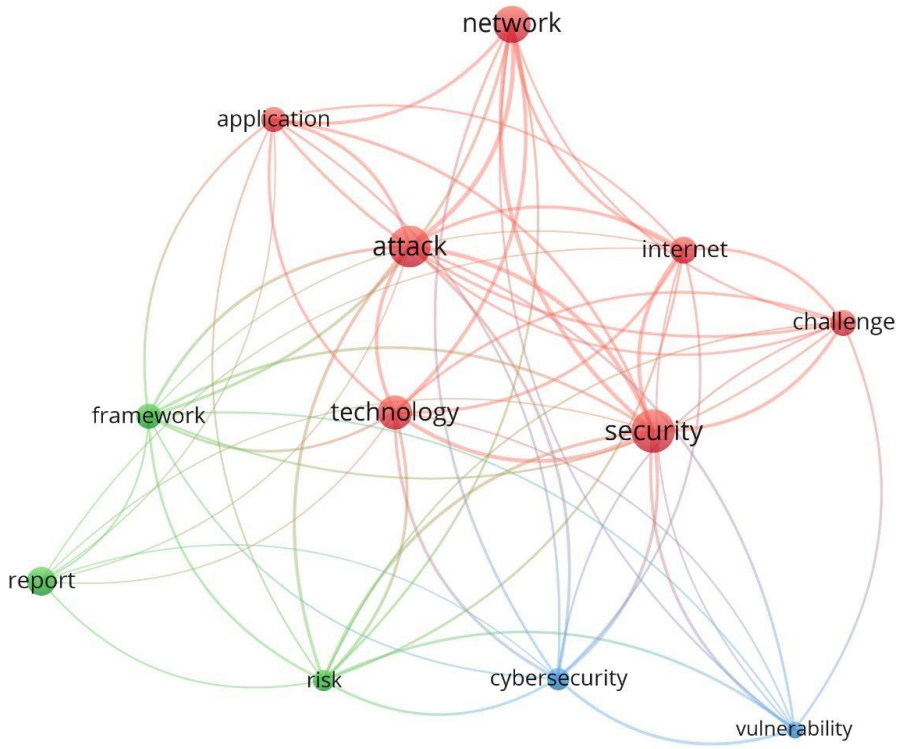


Table 5
Keywords for each Cluster

Cluster	Keywords
Red	“application”, “attack”, “challenge”, “internet”, “network”, “security”, “technology”
Green	“framework”, “report”, “risk”
Blue	“cybersecurity”, “vulnerability”

3.3.1. Red cluster

In this cluster, the keywords "application", "attack", "challenge", "internet", "network", "security" and "technology" were identified, which are connected and important in the role of endpoint security in organizations.

The keyword "application" is widely discussed in the context of semantic web applications, provenance, and knowledge representation. Applications play a very active role in endpoint security (Sikos & Philp, 2020).

https://doi.org/10.58086/7edc-2s28

Regarding "attack", several articles delve into different aspects of cyber-attacks, including strategies for attacking precision timing protocols, attacks on SCADA systems, and detecting zero-day attacks (Alghamdi & Schukat, 2021).

The “challenge” is addressed in the context of cybersecurity considerations for the health area, robotic surgery, IoT applications, and the ethical challenges of AI applications in cybersecurity, which highlight the challenges posed by cybersecurity threats in various domains (Bhavsar et al., 2023).

"Internet" and "network" are interconnected keywords discussed in the context of IoT applications, cloud-based access control policies, and the design of dynamic, self-adaptive systems for predictive risk analysis in cyberspace (Nagajayanthi, 2022).

Regarding “security”, this is a central theme in several publications, including those that focus on precision timing protocol attack strategies, cybersecurity monitoring, and strengthening the continuous integration workflow (Elhag et al., 2022).

The keyword "technology" is addressed in the context of extracting knowledge from unstructured information, antivirus applications for the detection of JAR malware, and the creation of a dynamic and self-adaptive system for the predictive analysis of cyber risk (Takko et al., 2023). These articles highlight the role of technology in knowledge extraction, malware detection, and predictive risk analysis in cybersecurity.

3.3.2. Green cluster

In the green cluster, the keywords “framework”, “report”, and “risk” are mentioned. "Framework" has been widely mentioned in the literature. Several frameworks have been proposed, particularly to analyze the predictability of cyber risks in critical environments where a cyber-attack must be avoided at all costs (Krishnan et al., 2023).

The keyword “report” is also significant in the context of cybersecurity in the sense that endpoint security incident reports and vulnerability reports are important and fundamental in this area. (Radanliev et al., 2020).

“Risk” is a key word in this area of cybersecurity, as it is essential to identify and plan the mitigation of risks associated, in this case, with endpoints (Aghamohammadpour et al., 2023).

https://doi.org/10.58086/7edc-2s28

3.3.3. Blue Cluster

The blue cluster includes the keywords are “cybersecurity” and “vulnerability”.

“Cybersecurity” refers to the protection of information technology assets against threats that may compromise their confidentiality, integrity, and availability. According to Diaz et al. (2019), with increasing dependence on technology, several sectors, including healthcare, face new risks, making cybersecurity considerations essential.

“Vulnerability” is a key concept in this cybersecurity context, particularly regarding detecting and mitigating potential weaknesses in systems. One of the main objectives of this area and the theme presented in this study is to try to reduce existing vulnerabilities in physical systems and devices. One way to do this is to update the operating system versions to the most recent and restrict the user to certain access and functionalities of the software or the system itself.

4. Conclusions

The bibliometric study carried out on the importance of endpoint security in companies provided a comprehensive view of trends, challenges, and advances in this crucial area of cybersecurity. The growing digital transformation of companies and the increase in cyber threats reinforce the importance of endpoint security. Protecting the various entry points into the network, such as computers, mobile devices, and servers, is crucial to safeguarding sensitive data and ensuring the continuity of the company's business.

In this study, the literature review highlights the diversity of security measures, from antivirus to advanced solutions such as EDR, IPS, and NGFW. The combination of these measures helps strengthen endpoint security by minimizing false positives and negatives. Business continuity stands out as one of the key points in this area. Incident response plans, the adoption of artificial intelligence and machine learning, and the need for sustainable cybersecurity practices are measures highlighted to help ensure operational resilience.

Endpoint security, business continuity. and vulnerability, although distinct concepts, are interlinked in cybersecurity. Endpoint security plays a crucial role in business continuity, and the identification and proactive correction of vulnerabilities are fundamental to avoiding interruptions in operations.

The bibliometric analysis carried out showed an increase in the number of publications over the last six years, reflecting the importance of endpoint security in several areas (e.g., medicine, industry, and

commerce) to guarantee business continuity. Countries such as the United States of America, India, and China have led in terms of the number of applications in this area.

As with any study, this research has some limitations that need to be recognized. However, they may represent a starting point for future work. The search terms, the area of the most cited articles, and the number of articles themselves can be considered limitations of this bibliometric study.

Taking the present study as a starting point, new lines of investigation can be outlined. For example, exploring detection strategies and evaluating the effectiveness of endpoint security practices. Another line of investigation may focus on security techniques and mechanisms, depending on the operating systems and the different types of endpoint devices used, to guarantee business continuity.

Bibliographic references

Aapro, M., Bossi, P., Dasari, A., Fallowfield, L., Gascón, P., Geller, M., Jordan, K., Kim, J., Martin, K., & Porzig, S. (2020). Digital health for optimal supportive care in oncology: Benefits, limits, and future perspectives. *Supportive Care in Cancer*, *28*(10), 4589–4612. https://doi.org/10.1007/s00520-020-05539-1

Aghamohammadpour, A., Mahdipour, E., & Attarzadeh, I. (2023). Architecting threat hunting system based on the DODAF framework. *The Journal of Supercomputing*, *79*(4), 4215–4242. https://doi.org/10.1007/s11227-022-04808-6

Alghamdi, W., & Schukat, M. (2021). Precision time protocol attack strategies and their resistance to existing security extensions. *Cybersecurity*, *4*(1), 12. https://doi.org/10.1186/s42400-021-00080-y

Angel, D. (2022). Application of graph domination to defend medical information networks against cyber threats. *Journal of Ambient Intelligence and Humanized Computing*, *13*(8), 3765–3770. https://doi.org/10.1007/s12652-022-03730-2

Ayub, M., Lajam, O., Alnajim, A., & Niazi, M. (2023). Use of Machine Learning for Web Denial-of-Service Attacks: A Multivocal Literature Review. *Arabian Journal for Science and Engineering*, *48*(8), 9559–9574. https://doi.org/10.1007/s13369-022-07517-7

Baiardi, F., & Tonelli, F. (2021). Twin Based Continuous Patching To Minimize Cyber Risk. *European Journal for Security Research*, *6*(2), 211–227. https://doi.org/10.1007/s41125-022-00079-7

Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things*, *3*(1), 5. https://doi.org/10.1007/s43926-023-00034-5

Bolpagni, M. (2022). Cyber risk index: A socio-technical composite index for assessing risk of cyber attacks with negative outcome. *Quality & Quantity*, *56*(3), 1643–1659. https://doi.org/10.1007/s11135-021-01199-3

Chen, P.-H., Bodak, R., & Gandhi, N. S. (2021). Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *Journal of Digital Imaging*, *34*(3), 731–740. https://doi.org/10.1007/s10278-021-00466-x

Chochliouros, I. P., Spiliopoulou, A. S., Kostopoulos, A., Kourtis, M.-A., Lazaridis, P.I., Zaharis, Z. D., & Prasad, N. R. (2021). Security Threat Analysis of the 5G ESSENCE Platform. *Wireless Personal Communications*, *120*(3), 2409–2426. https://doi.org/10.1007/s11277-021-08554-5

Coravos, A., Doerr, M., Goldsack, J., Manta, C., Shervey, M., Woods, B., & Wood, W. A. (2020). Modernizing and designing evaluation frameworks for connected sensor technologies in medicine. *Npj Digital Medicine*, *3*(1), 37. https://doi.org/10.1038/s41746-020-0237-3

Diaz, J., Perez, J. E., Lopez-Pena, M. A., Mena, G. A., & Yague, A. (2019). SelfService Cybersecurity Monitoring as Enabler for DevSecOps. *IEEE Access*, *7*, 100283–100295. https://doi.org/10.1109/ACCESS.2019.2930000

Elhag, S., Alghamdi, A. M., & Al-Shomrani, N. A. (2022). Toward an Improved Security Performance of Industrial Internet of Things Systems. *SN Computer Science*, *4*(2), 131. https://doi.org/10.1007/s42979-022-01566-3

Gao, R., Li, S., Gao, Y., & Guo, R. (2021). A lightweight cryptographic algorithm for the transmission of images from road environments in self-driving. *Cybersecurity*, *4*(1), 3. https://doi.org/10.1186/s42400-020-00066-2

George, A. S., George, A. S. H., Baskar, T., & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 8*(1). https://doi.org/10.48175/IJARSCT-1888

Ghadi, M., Sali, Á., Szalay, Z., & Török, Á. (2021). A new methodology for analyzing vehicle network topologies for critical hacking. *Journal of Ambient Intelligence and Humanized Computing*, *12*(7), 7923–7934. https://doi.org/10.1007/s12652-020-02522-w

Goldsack, J. C., Coravos, A., Bakker, J. P., Bent, B., Dowling, A. V., Fitzer-Attas, C., Godfrey, A., Godino, J. G., Gujar, N., Izmailova, E., Manta, C., Peterson, B., Vandendriessche, B., Wood, W. A., Wang, K. W., & Dunn, J. (2020). Verification, analytical validation, and clinical validation (V3): The foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs). *Npj Digital Medicine*, *3*(1), 55. https://doi.org/10.1038/s41746-020-0260-4

Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity*, *5*(1), 25. https://doi.org/10.1186/s42400-022-00127-8

Houhamdi, Z., & Athamena, B. (2021). IoT Framework for Effective and Fine–Grain Access Control. *2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 1-6). https://doi.org/10.1109/IOTSMS53705.2021.9704977

Ibrahim, R. F., Abu Al-Haija, Q., & Ahmad, A. (2022). DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors*, *22*(18), 6806. https://doi.org/10.3390/s22186806

Jia, K., Liu, C., Liu, Q., Wang, J., Liu, J., & Liu, F. (2022). A lightweight DDoS detection scheme under SDN context. *Cybersecurity*, *5*(1), 27. https://doi.org/10.1186/s42400-022-00128-7

Kafi, M. A., & Akter, N. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *American Journal of Trade and Policy*, *10*(1), 15–26. https://doi.org/10.18034/ajtp.v10i1.659

Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, *13*(1), 5–17. https://doi.org/10.1007/s41870-020-00585-8

Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: A scalable network security framework for SDN-based OpenStack cloud infrastructure. *Journal of Cloud Computing*, *12*(1), 26. https://doi.org/10.1186/s13677-023-00406-w

Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic. *New Generation Computing*, *39*(3–4), 599–622. https://doi.org/10.1007/s00354-021-00130-6

Nagajayanthi, B. (2022). Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective. *Wireless Personal Communications*, *123*(4), 3661–3697. https://doi.org/10.1007/s11277-021-09308-z

Noronha, G.M.S., Silva, A. A., & Pinheiro, J. S. S. (2022). Information Security Policies and Strategies and Practices Adopted in It: the Importance of Consultancy in Small and Medium-sized Companies. *International Journal of Advanced Research*, *10*(11), 779–786. https://doi.org/10.21474/IJAR01/15730

Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L., Burnap, P., Anthi, E., & Maple, C. (2020). Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments – cyber risk in the colonisation of Mars. *Safety in Extreme Environments*, *2*(3), 219–230. https://doi.org/10.1007/s42797-021-00025-1

Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10517–10553. https://doi.org/10.1007/s12652-022-03707-1

Rizvi, S. K. J., Aslam, W., Shahzad, M., Saleem, S., & Fraz, M. M. (2022). PROUDMAL: Static analysis-based progressive framework for deep unsupervised malware classification of windows portable executable. *Complex & Intelligent Systems*, *8*(1), 673–685. https://doi.org/10.1007/s40747-021-00560-1

Sarker, I. H. (2023). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, *10*(6), 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

Shahhosseini, M., Mashayekhi, H., & Rezvani, M. (2022). A Deep Learning Approach for Botnet Detection Using Raw Network Traffic Data. *Journal of Network and Systems Management*, *30*(3), 44. https://doi.org/10.1007/s10922-022-09655-7

Shao, X., Xie, L., Li, C., & Wang, Z. (2023). A Study on Networked Industrial Robots in Smart Manufacturing: Vulnerabilities, Data Integrity Attacks and Countermeasures. *Journal of Intelligent & Robotic Systems*, *109*(3), 60. https://doi.org/10.1007/s10846-023-01984-2

Sharma, R., Dangi, S., & Mishra, P. (2021). A Comprehensive Review on Encryption based Open Source Cyber Security Tools. *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, 614–619. https://doi.org/10.1109/ISPCC53510.2021.9609369

Sikos, L. F., & Philp, D. (2020). Provenance-Aware Knowledge Representation: A Survey of Data Models and Contextualized Knowledge Graphs. *Data Science and Engineering*, *5*(3), 293–316. https://doi.org/10.1007/s41019-020-00118-0

Simonovich, L. (2020). Cyber Security Incident Response in the Utility Sector. *Day 2 Tue, November 10, 2020*, D021S042R003. https://doi.org/10.2118/203220-MS

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*, *1*, 51–61. https://doi.org/10.1365/s43439-020-00014-3

Taddeo, M. (2019). Is Cybersecurity a Public Good? *Minds and Machines*, *29*(3), 349–354. https://doi.org/10.1007/s11023-019-09507-5

Takko, T., Bhattacharya, K., Lehto, M., Jalasvirta, P., Cederberg, A., & Kaski, K. (2023). Knowledge mining of unstructured information: Application to cyber domain. *Scientific Reports*, *13*(1), 1714. https://doi.org/10.1038/s41598-023-28796-6

Tan, Z., Beuran, R., Hasegawa, S., Jiang, W., Zhao, M., & Tan, Y. (2020). Adaptive security awareness training using linked open data datasets. *Education and Information Technologies*, *25*(6), 5235–5259. https://doi.org/10.1007/s10639-020-10155-x

Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? *International Cybersecurity Law Review*, *4*(3), 259–280. https://doi.org/10.1365/s43439-023-00095-w

The Lens. n.d. Explore Global Science and Technology Knowledge: Aggregated Metadata. Lens.org. Available online: https: //www.lens.org/ (accessed on 27 December 2023).

Victor, P., Lashkari, A. H., Lu, R., Sasi, T., Xiong, P., & Iqbal, S. (2023). IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. *Peer-to-Peer Networking and Applications*, *16*(3), 1380–1431. https://doi.org/10.1007/s12083-023-01478-w

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing*, *76*(4), 2643–2664. https://doi.org/10.1007/s11227-019-03028-9

Wan, B., Xu, C., Mahapatra, R. P., & Selvaraj, P. (2022). Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI. *Wireless Personal Communications*, *127*(2), 1207–1224. https://doi.org/10.1007/s11277-021-08573-2

Yang, F., Han, Y., Ding, Y., Tan, Q., & Xu, Z. (2022). A flexible approach for cyber threat hunting based on kernel audit records. *Cybersecurity*, *5*(1), 11. https://doi.org/10.1186/s42400-022-00111-2

Yevseiev, S., Tolkachov, M., Shetty, D., Khvostenko, V., Strelnikova, A., Milevskyi, S., & Golovashych, S. (2023). The concept of building security of the network with elements of the semiotic approach. *ScienceRise*, *1*, 24–34. https://doi.org/10.21303/2313-8416.2023.002828

Zhang, H., Feng, B., & Tian, A. (2022). A systematic review for smart identifier networking. *Science China Information Sciences*, *65*(12), 221301. https://doi.org/10.1007/s11432-022-3577-8

Zheng, W., & Omote, K. (2022). A study on robustness of malware detection model. *Annals of Telecommunications*, *77*(9–10), 663–675. https://doi.org/10.1007/s12243-021-00899-z

Instituto Superior Politécnico Gaya
www.ispgaya.pt
https://doi.org/10.58086/7edc-2s28

UM CISNE NEGRO NA SOCIEDADE DA PÓS-NORMALIDADE E DA PÓS-VERDADE. AS IMPLICAÇÕES DA COVID-19 NA BUSCA PELA VERDADE

Hugo Miguel Carvalho[1]

João Carlos Santos[2]

Resumo

Neste conceptual paper analisamos a presente era como um sistema definido pelas suas relações, que são representadas como inputs e outputs. Portanto, quando falamos sobre esta era enfatizamos algumas condições específicas do sistema que nos conduzem para a pós-normalidade e pós-verdade. Tentamos dar sentido ao presente e descobrir o futuro da verdade através da influência de acontecimento de impacto desproporcionado ou de eventos raros e aparentemente inverosímeis, como se verifica, no caso da COVID-19. Analisamos igualmente as razões que conduzem a pessoa humana, individualmente ou coletivamente, a não ver ou não querer ver a importância destes eventos no desenrolar da História e desenvolvimento da humanidade.

Palavras-chave: COVID-19; Pós-normalidade; Pós-verdade; Fake News

A BLACK SWAN IN THE SOCIETY OF POST-NORMALITY AND POST-TRUTH. THE IMPLICATIONS OF COVID-19 IN THE SEARCH FOR TRUTH.

Abstract

In this conceptual article, we analyze the present era as a system defined by its relations, which are represented as inputs and outputs. Therefore, when we talk about this era, we emphasize some specific conditions of the system that lead us to post-normality and post-normality. We try to make sense of the present and discover the future of truth through the influence of events of disproportionate impact or rare

[1] ISCIA- Instituto Superior de Ciências da Informação e Administração de Aveiro

[2] ISCIA- Instituto Superior de Ciências da Informação e Administração de Aveiro

https://doi.org/10.58086/7edc-2s28

and seemingly improbable events, as seen in the case of COVID-19. We also analyze the reasons that lead the human person, individually or collectively, to not see or not want to see the importance of these events in the course of the history and development of humanity.

Keywords: COVID-19, Post-normality; Post-truth; Fake News

Introdução

Estávamos longe do aparecimento da primeira pandemia do século XXI quando Ziauddin Sardar publicou o seu importante artigo Welcome to Postnormal Times (Sardar,2010) onde propunha uma nova abordagem teórica para desenvolver um melhor entendimento de como a própria mudança estava a ter um resultado importante na definição do presente. Sardar defendia que vários "artefatos" humanos, como sejam - significado, verdade, conhecimento, ordem mundial, governance, entre outros – encontravam-se em profundo estado de transformação de conceitos clássicos para modernos, de visões pós-modernas para pós-normais. E eis aqui, como humanidade em 2021 a vivermos um "novo normal".

"Tudo o que era 'normal' evaporou-se; entrámos em tempos pós-normais, o período intermediário em que velhas ortodoxias estão a morrer, novas ainda não surgiram e nada realmente faz sentido. Para se ter noção de um futuro viável, é preciso apreender o significado desse período de transição caracterizado por 3 c's: complexidade, caos e contradições. Essas forças impulsionam e sustentam tempos pós-normais que levam à incerteza e diferentes tipos de ignorância que tornam a tomada de decisões problemáticas e aumentam os riscos para os indivíduos, a sociedade e o planeta. Tempos pós-normais exigem, este artigo argumenta, que abandonemos as ideias de "controlo e gestão" e repensemos as noções acalentadas de progresso, modernização e eficiência. O caminho a seguir deve ser baseado nas virtudes da humildade, modéstia e responsabilidade, requisito indispensável para viver com a incerteza, a complexidade e a ignorância. Teremos que nos imaginar a sair de tempos pós-normais e entrar numa nova era de normalidade - com uma bússola ética e um amplo espectro de imaginações da rica diversidade de culturas humanas." (Sardar,435,2010).

Na verdade, não foi a pandemia COVID-19 que nos introduz neste "novo normal". A vivência da humanidade nestes tempos "pós-normais" já se encontrava em crescimento. Quase sem perceber já tínhamos entrado numa época em que pouca coisa pode ser confiável ou nos transmite confiança. Há muito que vivíamos cercados pela incerteza, rápida mudança, realinhamento de poderes, agitação e um generalizado comportamento caótico. Os velhos conceitos estão mortos, mas ainda temos capacidade para compreender o sentido dos novos conceitos que nascem no caos. A humanidade ainda pensava que vivia num equilíbrio global de poderes, que com todas as suas imensas imperfeições, mantinha uma aparência

https://doi.org/10.58086/7edc-2s28

de lei e ordem pacíficas. O homem queria manter esse sonho mesmo contra as evidências. Uma parte da humanidade queria continuar a acreditar naquela ilusão de que viviam em comunidades coerentes e coesas, onde acreditavam que o futuro dos seus filhos estava seguro. Para esta parte da humanidade o "antigo normal" nada mais era do que uma ilusão. O "novo normal" já era há muito vivido pela parte mais pobre da humanidade.

A humanidade continua com dificuldade em assumir que vive há já algum tempo um largo período de transição, sem poder basear-se no conforto do conhecimento do nosso passado e sem confiança em definir caminhos para um futuro sustentável. Evoluímos nesta fase entre escolhas perigosas e sonhos visionários, mas vacilantes e indecisos sobre a nossa capacidade ou vontade de os concretizar. O ser humano continua preso no paradoxo de uma realidade teimosa e de uma ilusão resiliente.

Vivemos numa época pós-normal entre o "velho" que resiste a morrer e o "novo" que ainda batalha por nascer e onde nada é dado como certo. Mas, o homem tem uma enorme dificuldade para situar-se entre o "nunca mais "e o "ainda não" numa incerteza dialética. Lidamos mal com a verdade de que a incerteza é parte fundamental da realidade. Por isso, criamos qualquer tipo de ilusão para acreditar que somos capazes de prever os fatos e mudar o curso da história.

A história demonstra a nossa incapacidade para aprender com os erros de previsão e a falta de consciência sobre os mesmos.

Vivemos num mundo globalizado que está interligado e é interdependente em todos os seus níveis, do local ao global, em todas as etapas das nossas vidas, o que regularmente e ininterruptamente, origina uma mudança pós-normal com uma rapidez nunca vista.

Em princípio, esta mudança pós-normal não deveria gerar efetivamente um acontecimento pós-normal, enquanto resultado da mudança como tal. No entanto, nesta humanidade globalizada e interligada, com uma diversidade de elementos interatuando com relações não lineares, produzem contradições estruturais e ampliam a complexidade do sistema.

A nossa sociedade, como um sistema, é agora muito mais do que a soma de todas as suas partes; e, portanto, não pode ser escrutinada pelas suas partes, dado que estas mesmas partes pela sua veloz interação vão-se auto-organizando em novos padrões e estruturas complexas.

Esta pandemia COVID-19 seria assim um acontecimento pós-normal decorrente desta lógica de evolução do sistema baseada na Complexidade, Contradições e Caos. A complexidade e as contradições do sistema que construímos como humanidade geram ciclos de feedback positivo cada vez mais velozes que levam ao Caos. Por isso, consideramos, que a maioria dos analistas está incorreto quando falam em recuperação e esperam por cenários que retornem ao seu antigo conceito de "normalidade".

https://doi.org/10.58086/7edc-2s28

Perdemos tempo precioso quando devíamos estar a projetar o novo rumo da humanidade. Os próximos anos vão relembrar-nos que esta pandemia foi apenas um convite à reflexão antes do aparecimento do verdadeiro problema. A Peste Negra do séc. XIV promoveu mudanças que foram emergindo ao longo de séculos. Sendo esta sociedade capaz de criar como sistema ciclos de feedback cada vez mais velozes, as consequências emergirão muito mais rapidamente. Esta sociedade interligada origina que os efeitos borboleta se amplifiquem com imensa rapidez. Devemos considerar, e baseando-nos em Habbermas (1987) e na sua Teoria da Ação Comunicativa, que a nossa sociedade, foi caindo numa progressiva colonização do mundo da vida pelo sistema, ou seja, a modernização social levou a que este caísse sob a dependência do sistema. Assistimos, então, ao crescimento de subsistemas cada vez mais complexos, cujos imperativos de monetarização e a burocratização se opõem contra o próprio mundo da vida. Esta é a realidade que temos de enfrentar.

Criamos demasiados Cisnes Negros (Taleb, 2007), que se formam nesta Complexidade, Contradições e Caos, para quem não sabe lidar com racionalidade com acontecimentos inesperados e raros com grandes ramificações. Muitos podem afirmar que é quase impossível de prever um Cisne Negro, sendo, portanto, acontecimentos dificilmente mitigáveis. Realçamos, no entanto, que um Cisne Negro apenas se vislumbra com clareza quando observado com um certo distanciamento. Nesse caso, o acontecimento torna-se óbvio e inevitável. Relembramos as palavras de Steve Jobs (2015).

"Vós, não conseguirão ligar os pontos apenas a olhar para a frente; vós, só conseguirão ligá-los se olharem pra trás. Então, terão de confiar que os pontos se vão ligar algum dia no futuro. Vós, têm de confiar em algo – no seu instinto, destino, vida, carma, o que for. Esta abordagem nunca me desapontou, e fez toda diferença na minha vida".

Quando desejamos entender a pós-normalidade e os fenómenos, somos obrigados a enfrentar incertezas e os erros, imprecisões e inexatidões no nosso entendimento e razão que expõem a precaridade de todos os nossos preconceitos; somos assim obrigados a reavaliar as nossas ideias, crenças e perspetivas sobre o sistema que construímos enquanto humanidade. Quem desejar entender a pós-normalidade tem de voltar a ser um descobridor por marés nunca antes navegados. Porque os eventos e problemas pós-normais não podem ser controlados ou geridos - eles apenas podem ser navegados.

A pandemia COVID-19 engloba todas as características de um processo de mudança pós-normal: velocidade, propósito, escala e simultaneidade. Mas será um acontecimento pós-normal? Acreditamos que sim, dado que é o resultado da interação das forças de Complexidade, Contradições e Caos.

Voltamos a reiterar a nossa ideia de que poderemos ser muitos resilientes na ilusão, mas a teimosia da realidade irá sempre prevalecer. Não é apenas porque um fato não aconteceu ou que não queremos que aconteça que ele não acontecerá. Um Cisne Negro implica sempre uma enorme catástrofe que

https://doi.org/10.58086/7edc-2s28

devemos assumir que irá ocorrer de forma a prepararmo-nos o melhor possível. A pergunta seguinte seria óbvia.

1. "Quem poderia conceber que seríamos afetados por uma pandemia como o COVID-19?

Na época dos novos antibióticos, os microbiologistas Macfarlane Burnet e David White previram em 1972 que o mais provável sobre o futuro das doenças infeciosas é que será muito enfadonho. (Burnet, 1972). No entanto, reconheceram que iria sempre existir o risco do surgimento totalmente inesperado de uma nova e perigosa doença infeciosa, mas nada do tipo marcou os últimos cinquenta anos. As epidemias, neste período, interessavam apenas aos historiadores.

Os tempos mudaram assim como as nossas perspetivas. Desde o herpes à doença do legionário na década de 1970, à VIH, ébola, a síndrome respiratória aguda grave (SARS) e agora Covid-19, as doenças contagiosas continuam a ser um risco existencial. Os historiadores continuam atentos a esta evolução, assim como ao seu contexto e circunstâncias locais. (Jones, 2020)

Charles Rosenberg, baseou-se em Albert Camus (Camus,1972) e concebeu uma estrutura de uma pandemia (Rosenberg,1989) que se desenvolveria em três fases.

Concebemos, desta forma uma nova interpretação, baseado em Rosenberg. Numa primeira fase, perante sinais muitos tênues, o ser humano influenciado por um desejo absurdo de negação ou de ilusória autoconfiança homocêntrica, ou mesmo perante o imperativo e a necessidade de defender o seu status quo político e económico, decide ignorar o óbvio até que a evolução da pandemia e o número crescente da taxa de mortalidade o faça acordar da autoilusão.

A segunda fase, inicia-se perante o reconhecimento do caos instalado. Toda a pandemia pressiona a sociedade onde eclode de forma a tornar evidentes as falhas nas estruturas que, de outra forma, não seriam evidentes ou se encontravam demasiado escondidas. Este é o aspeto positivo de mudança que uma pandemia origina, pois obriga a uma análise social sobre o que realmente é relevante e valorizado pela sociedade. O caos nunca tem uma ação destruidora per si, mas de regeneração e co-criação.

Perante esta pressão, a sociedade "pós-normal" exige agora rápidas explicações científicas, económicas, morais e mesmo teológicas – o que originam apressadas respostas públicas geralmente mal fundamentadas por falta de previsão. A história demonstra-nos que, corremos um maior risco perante o pânico e o medo exagerado e com a consequente elaboração de planos e prioridades mal fundamentadas. São inúmeros os exemplos históricos de sociedades que se focam numa ameaça existencial menor, ignorando riscos existenciais muito maiores, sejam eles ocultos ou demasiado visíveis.

https://doi.org/10.58086/7edc-2s28

Não devemos igualmente esquecer que um dos aspetos mais dramáticos e absurdos da resposta a uma pandemia é sempre o desejo de atribuir responsabilidades a algo ou alguém. A estigmatização é parceira íntima de todas as pandemias. Não nos surpreendamos por esta culpabilização, pois trata-se de um mero mecanismo de defesa para as manifestações do Ego diante das exigências das outras instâncias psíquicas do ser humano (como seja a ansiedade, o medo ou a necessidade de sobrevivência), que tendem a desencadear sentimentos inconscientes, provocando reações menos racionais e objetivas que buscam reduzir as manifestações iminentemente perigosas ao Ego. Falamos de mecanismos como a compensação, expiação, fantasia, formação reativa, identificação, isolamento, negação, projeção e regressão, que são perigosas quando afetam a humanidade em larga escala face a um acontecimento inesperado e que coloca em causa a sua existência. O estado instintivo ou "selvagem" do homem nunca esteve completamente controlado e delimitado pelas normas civilizacionais. O homem evolui mediante o confronto de paradoxos – e, não como num processo retilínio de civilidade, pois a barbárie ainda murmura inconscientemente no seu amago. Por isso, o ser humano não lida bem com Cisnes Negros, mesmo quando é o seu progenitor.

Esse discurso de culpabilização do outro e/ou de vitimização baseados nestes mecanismos de defesa psíquica reflete-se posteriormente nas divisões sociais existentes aos níveis da religião, raça, etnia, classe ou identidade de gênero. Os governos, como sempre o fizeram na história, respondem através da força da sua autoridade, impondo medidas públicas compulsórias, como sejam a quarentena ou vacinação obrigatória. Simplesmente, temos uma perspetiva histórica onde observamos instituições ou pessoas com poder e privilégio (nem sempre baseadas em sólidos conhecimentos ou comprovadas evidências científicas e raramente baseados numa comunicação clara e coerente) impondo intervenções sobre pessoas sem poder ou privilégio, criando e alimentando uma dinâmica que alimenta ainda mais o medo e o conflito social. (Jones, 2020). Outro fator de stress sobre a sociedade verifica-se nas análises históricas de pandemias em que se observa que as intervenções científicas / médicas e de saúde pública muitas vezes não cumprem com as suas promessas.

Tudo isto alimenta a que as respostas privadas sejam crescentemente fundamentadas em considerandos fundamentalistas, conspirativos, e totalmente absurdos, baseadas numa perspetiva de "pós-verdade" onde se estabelece o berço das fake news. As respostas ao surto tornam-se assim mais perigosas, pungentes e catastróficas do que a própria doença.

Gostávamos de relembrar que sob a capa da "normalidade", é possível esquecer que os valores que orientam a humanidade não se concretizam na prática. Por isso, torna-se necessário um "novo normal" ou uma pós-normalidade. Esta segunda fase da pandemia é uma porta entreaberta para algo novo. Por exemplo, compreendemos na leitura de Ensaio sobre a cegueira (Saramago, 1995) e La peste

https://doi.org/10.58086/7edc-2s28

(Camus,1947) uma tentativa deliberada de simbolizar a agudez da crise como um meio de transmissão da necessidade do compromisso permanente com um verdadeiro humanismo. Saramago criou uma nova peste (a cegueira branca) que descortinasse a aparência de humanidade dos dias atuais. A luta contra as doença é a alegoria da necessidade de construir um humanismo real. Camus e Saramago querem nos transmitir que é necessário o homem adoecer para perceber a sua doença, que é necessário cegar para compreender que nada vê.

A história ensina que na terceira fase, a pandemia acaba por ceder face à ação humana ou por ter completo uma espécie de ciclo de seleção natural onde ceifa os padecentes mais débeis. Este é o esquema evolutivo pandémico que presenciamos com a Covid-19.

A Organização Mundial da Saúde (OMS) e o Banco Mundial alertaram sobre o risco de pandemias entre os anos de 2000 a 2010, especialmente após o surto de SARS de 2002-2004. O Global Preparedness Monitoring Board divulgou seu primeiro relatório no final de 2019 (GPMB, 2019). Foram realizadas múltiplas iniciativas e avisos para proceder a uma conscientização sobre a ameaças de uma grave pandemia e necessidades de a humanidade se preparar.

Em maio de 2015, a OMS foi solicitada pelas organizações membros a criar um "Plano de Ação para Prevenir Pandemias" de forma a gerar ideias que reduziriam o lapso de tempo entre a identificação de surtos virais e a aprovação de vacinas / tratamentos, para evitar que os surtos se transformem em uma "emergência de saúde pública". Um grupo de especialistas globais, o “R&D Blueprint Scientific Advisory Group", foi reunido pela OMS para elaborar uma lista restrita de menos das dez "doenças prioritárias do projeto". Desta forma, em 2018, a OMS cunhou o termo, Doença X, para representar um hipotético patógeno desconhecido que eventualmente poderia vir a causar uma epidemia futura. (WHO, 2018), Na verdade, alguns dos consultores especializados da OMS, consideram que o COVID-19, causado pela cepa do vírus SARS-CoV-2. A COVID -19 seria a primeira Doença X.

Assim, Peter Daszak (2020) relata**:** “No início de 2018, durante uma reunião na Organização Mundial da Saúde em Genebra, um grupo de especialistas ao qual pertenço (o Projeto de R&D) foi criado o termo "Doença X". Estávamos referindo-nos à próxima pandemia, que seria causada por um novo patógeno que ainda não havia entrado na população humana. Enquanto o mundo está hoje à beira do precipício pandémico, vale a pena reservar um momento para considerar se a Covid-19 é a doença sobre a qual o nosso grupo procurou alertar. A doença X, dissemos naquela época, provavelmente resultaria de um vírus originado em animais e surgiria em algum lugar do planeta onde o desenvolvimento económico une as pessoas e a vida selvagem. A doença X provavelmente seria confundida com outras doenças no início do surto e espalhar-se-ia rápidamente e silenciosamente; explorando redes de viagens e comércio humanos, e alcançaria vários países e impediria a contenção. A doença X teria uma taxa de mortalidade

https://doi.org/10.58086/7edc-2s28

mais alta do que uma gripe sazonal, mas espalhar-se-ia tão facilmente quanto a gripe. Tudo isto abalaria os mercados financeiros antes mesmo de atingir o status de pandemia. Em poucas palavras, Covid-19 é a doença X."(Daszak, 2020).

Michael Osterholm, um especialista em doenças infeciosas, tem vindo a alertar há cerca de uma década e meia que o mundo teria de enfrentar uma nova pandemia. Osterholm, escreveu vários artigos na revista Foreign Affairs, Preparing for the Next Pandemic (Osterholm, 2005), Unprepared for a Pandemic (Osterholm, 2007), Chronicle of a Pandemic Foretold (Osterholm, 2020), e voltou a reiterar no seu livro de 2017 que a sociedade se encontrava num ponto crítico na sua história. Osterholm, sempre afirmou que o tempo estava a esgotar-se. Para a humanidade preparar-se para a próxima pandemia.

Vaclav Smil no seu livro, Global Catastrophes and Trends: The Next Fifty Years, avisou que depois das pandemias de 1958-59, 1968 e 2009, a humanidade nada tinha feito como medida de prevenção, o que deixava altamente vulnerável face a outra pandemia viral. Smil acreditava que a probabilidade de outra pandemia de influenza durante os próximos 50 anos era praticamente de 100%. (Smil, 2008)

Mais recentemente, numa palestra TED talk de 2015, Gates afirmou que o mundo "não estava pronto para a próxima pandemia" (Gates, 2015).

"O que aprendi é muito preocupante. Por mais terrível que tenha sido esta pandemia, a próxima poderá ser muito pior. O mundo simplesmente não está preparado para enfrentar uma doença - uma gripe especialmente virulenta, por exemplo - que infeta um grande número de pessoas muito rapidamente. De todas as coisas que podem matar 10 milhões de pessoas ou mais, de longe a mais provável é uma pandemia. Mas acredito que podemos prevenir essa catástrofe construindo um sistema global de alerta e resposta a pandemias. Aplicaria o tipo de planeamento que existe na defesa nacional - sistemas para recrutar, treinar e equipar profissionais de saúde; investimentos em novas ferramentas; etc. - ao esforço para prevenir e conter surtos" (Gates, 2015).

Em 2018, numa reflexão sobre pandemias patrocinada pelo Massachusetts Medical Society e pelo New England Journal of Medicine, Gates voltou a afirmar que uma pandemia poderia acontecer na próxima década (Hoffower,2020). Numa entrevista ao Financial Times afirmou que um surto viral provavelmente acontecerá "a cada 20 anos ou mais" (Gates, 2020).

As previsões de Bill Gates, ao alertar sobre uma pandemia foram claras e atempadas, assim como diversos especialistas em saúde. Ex-funcionários da Casa Branca também alertaram anteriormente sobre uma ameaça de pandemia iminente. Múltiplas teorias da conspiração circularam online ou em livros e filmes que faziam alusão a uma pandemia mundial. A esmagadora parte dessas previsões são pura

https://doi.org/10.58086/7edc-2s28

especulação. Mas os de especialistas em saúde, sempre foram mais precisos e todos afirmavam a mesma situação: o mundo não estava preparado para este Cisne Negro.

Resumindo, antes da pandemia uma cascata de avisos, estudos e simulações foram claramente ignorados (Sanger et al, 2020). Compreendemos que a elite dominante global ignorou as advertências de especialistas sobre uma pandemia, muito mais preocupada em propor medidas de estímulo para sustentar os mercados. A pandemia era expetável, mas esta elite preferiu reunir-se em Davos todos os anos para falar sobre poder, dinheiro e tecnologia - principalmente sobre o seu potencial de maximizar os seus retornos. Nunca foi seu intento concentrarem-se na responsabilidade principal da classe dominante - a segurança da humanidade. Se os sistemas de saúde e de investigação tivessem recebido o investimento necessário estariam preparados para uma pandemia como esta, e a taxa de mortalidade seria 100 vezes menor. (Xie, 2020). A resposta global ao COVID-19 representa a maior falha da política científica a que assistimos. Acreditamos que vivemos numa era em que a atividade humana tornou-se a influência dominante no meio ambiente. Uma ideia que evoca noções de onipotência humana. A pandemia Covid-19 revelou a fragilidade humana e expôs a nossa incapacidade de cooperar, coordenar e agir em conjunto. Talvez não sejamos tão dominantes quanto pensávamos (Horton, 2020).

O tal de 'destino' é um conceito que elaboramos tendo como base um acontecimento imprevisível e inalterável para identificar (e muitas vezes tentar personificar em si mesmo) aquilo que não é identificável. Ou seja, a humanidade tenta que o destino defina o indefinível, e por tal, criou um sistema paradoxal. Mas, na medida em que o imprevisível e o inalterável são determinados conscientemente. Quisemos pensar que o homem podia 'representar e criar um destino' e com isso 'ser ele mesmo um destino' para alguém ou a caminho de algo, enquanto não encontra a verdade (Stegmaier, 2011).

O problema é que quase todo o pensamento humano é narrativo e elabora a personagem e circunstâncias que deseja ser e viver. Quando um homem quer ser um destino, é nesse querer que se transforma pobremente no seu destino. Assume-se o destino como uma "vivência", algo que é meramente vivenciado, mas que não pode ser conceptualizado. Mas, o homem que quer ser o seu destino pela vida acaba por nunca explicar o indefinível. O homem que quer ser um destino acaba por compreender e aceitar o involuntário (Stegmaier, 2011). Quando Nietzsche exclama que “Deus está morto”, contrapomos que na verdade o “homem soberano está morto” e que foi o próprio homem que quis ser destino, que o matou.

Em toda a história observamos no homem um risco pela tentação totalitária que ignora o óbvio. O homem revolta-se contra a injustiça porque vive preso num destino que não é menos absurdo, mas é trágico porque só em raros momentos torna-se consciente do mesmo homem.

https://doi.org/10.58086/7edc-2s28

A humanidade tornou-se numa espécie de Sísifo que desafiou os deuses e foi condenado por toda eternidade, a empurrar a pedra até o topo; e a ter de começar tudo de novo, vezes sem conta.

O homem quando toma essa consciência face ao absurdo tem três consequências que são, a sua revolta, a sua liberdade e a sua paixão. Na maioria, opta pela revolta contra a injustiça, mas o império dos homens acaba sempre por desvirtuar os objetivos justos, pela cegueira do poder. Todavia, a culpa dos crimes feitos em nome desse império não é da revolta, mas sim a fuga e o esquecimento relativamente às razões dessa mesma rebelião.

Assim, o homem acaba por viver os riscos da sua ilusão sobre a infalibilidade e imparcialidade da justiça e da realidade.

É necessário cuidado com as soluções permanentes para problemas temporários. É necessário cuidado com soluções que implicam uma solução apenas num futuro possível, mas que não conseguem resolver nada no aqui e agora. É necessário cuidado com as soluções que apenas respondem ao absurdo da vida sem nos ajudar a criar o nosso próprio significado da mesma.

Citando Goethe: "Saber não basta; devemos aplicar. Desejar não é suficiente; devemos fazer." Os sinais eram claros. Tivemos o Hendra em 1994, Nipah em 1998, Sars em 2003, Mers em 2012 e Ébola em 2014; todas estas pandemias foram causadas por um vírus com origem em hospedeiros animais que se transferiram para humanos. Os riscos naturais são inevitáveis; o desastre não é (Jones, 2018). O ser humano tem a tendência a ignorar as informações que não refletem a nossa própria experiência do mundo. Normalmente, as catástrofes revelam a fraqueza da memória humana (Horton, 2020). Porque não fizemos nada?

2. Porque ignorámos os avisos evidentes?

A pandemia Covid-19 é um acontecimento da pós-normalidade e representa para muitos a primeira pandemia da era da pós-verdade. Veremos que não será exatamente esta a realidade. A COVID-19 não é a primeira epidemia a gerar boatos e mentiras. Ao longo da história, demagogos e vendedores de "ilusões e milagres" exploraram pragas para espalhar falsidades, manter o poder ou ganhar dinheiro. O que parece diferente nesta era é que enfrentamos não apenas deceções e declarações erróneas, mas um profundo ceticismo sobre a própria ideia de que a verdade possa existir (Parmet, 2020).

A expressão da pós-verdade foi eleita a palavra do ano em 2016 de acordo com Oxford Dictionaries. O seu significado refere-se a algo que denota circunstâncias nas quais os fatos objetivos não são relevantes, em termos de formação da opinião pública, pois constitui um apelo às emoções e às crenças pessoais. Portanto, quem deseja influenciar a opinião pública deve concentrar-se na criação de um discurso que

https://doi.org/10.58086/7edc-2s28

seja fácil de aceitar e dar uma maior ênfase ao que irá satisfazer as emoções e crenças do público, em vez de fatos reais (Camacho, 2019).

Foi no livro intitulado The Post-Truth Era: Dishonesty and Deception in Contemporary Life que o termo obteve um certo grau de desenvolvimento conceitual (Keys, 2004). A manipulação criativa criada nesta era levou a humanidade a ausentar-se do reino da exatidão e a mudar-se para o reino da narração da verdade. As informações embelezadas e coloridas são formuladas como verdadeiras em espírito e mais verdadeiras do que a própria verdade. Num mundo inundado por informações irrelevantes, a clareza é poder. A censura não funciona bloqueando o fluxo de informações, mas inundando as pessoas com desinformação e distrações (Harari, 2018). Se o futuro da humanidade for decidido na ausência da maioria, porque estes estão demasiado ocupados a consumir ou a tentar tudo para fazer sobreviver a sua família ou a si mesmos – tal fato não os isentará das consequências. A história nunca foi justa.

Podemos identificar muitas fontes potenciais da pós-verdade. A disseminação viral de informações contraditórias nas redes sociais cria um clima de desconfiança. A rápida mudança cultural e o aumento da desigualdade económica alimentaram a polarização política que fomenta a lealdade ao partido a uma causa em vez de uma busca compartilhada pela verdade (McIntyre, 2018). O fracasso impressionante dos organismos estatais e internacionais assim como dos especialistas em prever e prevenir os múltiplos e crescentes ataques terroristas ou as diversas crises económicas dos últimos anos, misturado com o aumento noticiado da corrupção em todos os sectores, minaram a fé nos líderes nacionais e em todo o sistema global e seus vários subsistemas.

Olhando além dessas forças, sugerimos que vários fatores adicionais merecem consideração. Sem dúvida, toda a informação divulgada sobre a chamada “ciência falsa” patrocinada pelas indústrias de tabaco, combustíveis fósseis e outras (Conway, 2010)., corroeu ainda mais a crença de que a ciência busca descobrir a “verdade” (Funk, 2019). Como podemos esperar que o ser humano aceite que a ciência busca a verdade quando somos informados consistentemente sobre retratações, estudos falsos e até “empresas científicas” criadas com base na mentira?

No entanto, será esta época da pós-verdade uma novidade? Na verdade, o ser humano sempre viveu na era da pós-verdade. O homem é uma espécie pós-verdade, que evoluiu devido à capacidade única de criar e divulgar ficções. Somos a única espécie que pode cooperar com base na capacidade de criar histórias de ficção, divulgá-las e ter a aptidão para convencer outros a acreditar nestas mesmas. O ser humano compreendeu que a forma mais fácil de todos cooperarem e obedecerem às mesmas leis seria conceber uma forma em que todos acreditem nas mesmas ficções (Harari, 2018), talvez por isso o dinheiro tenha sido o sistema mais pluralista de confiança mútua criado pelo homem (Harari, 2015). O

https://doi.org/10.58086/7edc-2s28

Homo sapiens governa o mundo porque é o único animal que pode acreditar em coisas que existem puramente na sua própria imaginação. (Harari, 2015)

Desde cedo a humanidade criou o berço das mitologias, ideologias e fake news. Quando convencemos mil pessoas a acreditar durante um mês numa história inventada, criámos uma fake news. Quando convencemos milhões de pessoas a acreditar durante um século numa teoria inventada, criámos uma ideologia. Os Estados criaram as suas próprias "mitologias", em movimentos como o comunismo, o fascismo, globalização e liberalismo que elaboraram os seus próprios credos auto-referenciais. O ser humano percebeu que a mais pura verdade da realidade nunca moveu multidões ou foi prioritária na agenda da evolução humana. (Harari, 2018).

Aparentemente, para o ser humano não existe uma divisão estrita e prática em distinguir entre o que é apenas uma convenção ou construção humana e o que é intrinsecamente verdade. O ser humano costuma ser ambíguo ou tende a esquecer-se dessa distinção. Desfocar a linha entre ficção e realidade é uma característica demasiadamente humana, dado que temos a capacidade notável de simultaneamente saber e de não querer saber. (Harari, 2018).

O ser humano sempre preferiu o poder em detrimento da verdade. Apenas assim se compreende o fato de ter passado muito mais tempo a tentar controlar o mundo do que a tentar entendê-lo. A verdade e o poder apenas são temporários companheiros de viagem. Quem deseja o poder, acaba por espalhar ficções. Quem deseja a verdade terá de renunciar ao poder, pois a verdade acabará afastar aliados, seguidores e minar uma certa harmonia, mesmo que esta seja baseada na mentira. (Harari, 2018).

A seu tempo, a principal força da evolução - a seleção natural - será substituída pelo design inteligente. Será que a sociedade da pós-verdade irá descobrir demasiado tarde que a humanidade em breve perderá não apenas o seu domínio, mas o seu próprio significado. Ao longo do século passado, a humanidade conseguiu fazer o impossível e controlar a fome, as pandemias e a guerra global. A pandemia COVID-19 aparenta ser o primeiro sério desafio a este domínio. Na nossa era, morrem mais pessoas de obesidade do que de fome; morrem mais pessoas de velhice do que de doenças infeciosas; morrem mais pessoas por cometer suicídio do que mortas em palco de guerra. O aparente sucesso gerou ambição desmedida, e a humanidade busca a imortalidade, a felicidade sem limites e os poderes divinos da criação. Mas a busca desses objetivos acabará por tornar a maioria dos seres humanos supérfluos. Mas esta é a verdade que ninguém quer enfrentar na era da pós-verdade. A ambição cega torna-nos surdos para a verdade (Harari,2017).

Na mais recente história da era pós-verdade, a humanidade não possui apenas verdades e mentiras, dado que criou uma terceira categoria de afirmações ambíguas que não são exatamente a

https://doi.org/10.58086/7edc-2s28

verdade, mas que ficam aquém de uma mentira. Criámos uma neo-verdade, uma espécie de verdade aprimorada. Katharine Viner explica a ligação da tecnologia com a era da pós-verdade:

"Somos apanhados numa série de confusas batalhas entre forças opostas: entre verdade e falsidade, fato e boato, bondade e crueldade; entre poucos e muitos, os conectados e os alienados; entre um público informado e uma multidão desorientada. O que é comum nestas lutas - e o que torna a sua resolução um assunto urgente - é que todas envolvem a diminuição do status da verdade. Isso não significa que não existam verdades. Significa simplesmente, que não podemos concordar sobre quais são essas verdades, e quando não há consenso sobre a verdade e nenhuma maneira de alcançá-la, o caos logo se segue. Cada vez mais, o que conta como um fato é apenas uma visão que alguém sente ser verdadeira - e a tecnologia tornou muito fácil para esses "fatos" circularem com uma velocidade e alcance inimagináveis na era Gutenberg (ou mesmo há uma década) ... Nesta época, as pessoas desconfiam muito do que é apresentado como fato - particularmente se os fatos em questão são desconfortáveis ou não estão em sincronia com as suas próprias visões. Na era digital, é mais fácil do que nunca publicar informações falsas, que são rapidamente compartilhadas e consideradas verdadeiras" (Viner, 2016).

A era da pós-verdade é criada em torno de algoritmos que alimentam os mecanismos de busca da internet, de forma a oferecer ao ser humano o que ele deseja. A versão do mundo a que temos acesso foi filtrada e otimizada, de forma invisível para reforçar as próprias crenças ou para nos transmitir a versão da verdade que alguém tenta fazer passar como verdade absoluta. A verdade transformou-se num algoritmo servido segundo um cardápio de gostos pessoais. Usar plataformas eletrónicas, reduz cada vez mais a hipótese de encontrar informações desafiantes, que ampliem a perspetiva do mundo ou a descoberta de fatos que refutem uma predominância de informações falsas.

Ralph Keyes revela que a consequência mais relevante da pós-verdade é a construção de uma pós-veracidade. Existe uma crescente falta de confiança no discurso público, não pelo conteúdo, mas baseada num descrédito que gera uma crescente suspeita de que a mensagem pode servir a um propósito oculto, que não é desejado pelo público (Keys, 2004). Paradoxalmente, o mesmo público que é governado e que participa ativamente, por vezes de forma inconsciente, na construção dessa pós-verdade. Um público acostumado a viver numa constante justificação da mentira em função dos seus interesses individuais. Tudo o que não coincide com as nossas ideias pode e deve ser classificado como falso – esta é a perspetiva da sociedade da pós-verdade.

Ninguém está isento da responsabilidade por participar de alguma forma em atos difamatórios, mesmo quando parece insignificativo, ou pensamos que o que transmitimos é verdade. A linguagem não é apenas um veículo de comunicação de verdades ou mentiras, pois também é portadora de valores. Esta

https://doi.org/10.58086/7edc-2s28

tendência de charlatanismo é contagiosa, e esta tendência de consumir falsidades e meias-verdades torna-se numa espécie de coprofagia amoral (Frankfurt, 1986).

A humanidade não se encontra destituída da sua liberdade e livre-arbítrio. No máximo, podemos afirmar que são conceitos condicionados. O ser humano continua livre para decidir restabelecer o preço da verdade na sua vida. O ser humano continua a ter capacidade para preservar-se das suas falsidades e as dos outros, e evitar conviver com conjunturas em que o embuste é a regra do jogo.

Historicamente, iremos retratar este período de pandemia COVID-19 como sendo caracterizado pela confusão e falta de compreensão entre o individuo e as organizações. A falta de conhecimento torna difícil responder à ansiedade e medo humano sobre a propagação do vírus, a duração da crise e as formas de enfrentá-la. Em The Pandemic Century; One Hundred Years of Panic, Hysteria and, Hubris, Mark Honigsbaum explica que argumenta que em vez de banir o pânico, um melhor conhecimento médico e vigilância de doenças infeciosas também podem semear novos medos, tornando as pessoas hiperconscientes das ameaças pandémicas que antes tinham ignorado. Os media desempenham um papel relevante nesses processos - afinal, nada vende mais do que o medo. Estes acabam por alimentar o pânico, a histeria e o estigma associados a surtos de doenças infeciosas (Honigsbaum, 2019).

Sabemos que períodos caracterizados pela falta de conhecimento são sempre acompanhados de charlatanismo, desinformação e erros, pela necessidade de preencher o vácuo deixado pelas parcas informações parciais disponíveis durante a crise (Schulman, 2020).

A pandemia COVID-19 é na verdade um fenómeno único que que revela os perigos da era pós-verdade. O período da pandemia tem se caracterizado por um decréscimo de confiança nas instituições resultante de uma indefinição da linha que separa a opinião do fato. A pandemia intensificou a urgência do ser humano encontrar certezas. O problema é que tendem a procurá-la apenas em “fatos” que são consistentes com as suas próprias opiniões. A verdade passou a ser apenas aquilo que se adequa á crença que se tem. A sensação de confusão e incerteza provém de contradições entre diferentes fatos e fontes face a essas crenças pessoais. O surgimento do logro, desinformação e inexatidão são o resultado dos desejos e interesses do individuo que lhe permitem sentir-se mais seguros confortáveis e evitar dissonâncias cognitivas (Schulman, 2020).

É evidente que a pandemia COVID-19 é claramente um fenómeno padrão da era pós-verdade - um resultado de processos inevitáveis. Criámos uma situação onde cada indivíduo considera-se capaz de decidir o que é verdadeiro quando analisa diferentes argumentos na esfera política e científica e sente-se qualificado para desenvolver teorias e refutá-las. Tudo isto resulta no aumento da incerteza geral perante uma infinidade de argumentos contraditórios. Nesta, era observamos como o charlatanismo, desinformação e os erros se assumem como argumentos válidos (Schulman, 2020).

https://doi.org/10.58086/7edc-2s28

Não enfrentamos apenas uma pandemia viral. Enfrentamos, a longo prazo, um problema imensamente mais complexo de media viral. A sociedade humana entrou em uma nova fase de desenvolvimento caraterizada pela interdependência radical entre aspetos anteriormente desconectados da realidade humana. O problema de uma modernidade viral e de uma teoria viral de pós-verdade cresce a partir de uma perspetiva desenvolvida a partir de Wittgenstein e Foucaul, dado que ambos, partem do princípio que as proposições verdadeiras não existem por si mesmas, mas são parte de um sistema de crenças (uma 'teoria') governada por uma gramática subjacente ou regras linguísticas definidas - uma interpretação semiótica fundamental que se concentra na coerência. Ambos defendem uma visão da verdade como uma relação estabelecida a uma rede de crenças que estão em consonância com o modelo ecológico, comunitário e semiótico da verdade (Peter set al, 2020). Vivemos num e para um sistema de bioinformacionalismo construído como uma espécie de ecossistema de ervas daninhas, que é a característica de sistemas onde o erro se expande progressivamente.

O verdadeiro conhecimento requer condições de crença, verdade e justificação, enquanto a mera informação não requer nenhuma dessas condições. A "condição" da existência da pós-verdade baseia-se numa cisão entre a evidência e a verdade. A informação viral e os media virais desenvolveram uma ligação especial entre a maneira como a informação se comporta nas redes digitais e o papel que a informação desempenha como um sistema de mensagens na biologia genómica. As doenças virais podem evoluir e competir numa população hospedeira, assim como os rumores e opiniões são moldadas e disseminadas pelos contatos sociais. (Kucharski, 2016).

“Os vírus biológicos requerem um organismo hospedeiro para sua reprodução e causam consequências desagradáveis para os seus hospedeiros. Os vírus de informação seguem os mesmos princípios. Eles necessitam de computadores e de consumidores humanos como hospedeiros para se reproduzirem, causam igualmente vários sintomas, como o mau funcionamento da sociedade e os sintomas da pós-verdade. No entanto, no entanto, os vírus da informação são diferentes dos vírus biológicos, dado que não reconhecem a necessidade de um nível de coexistência administrável. Nem toda a estratégia contra vírus biológicos tem uma estratégia equivalente contra o vírus da informação. As vacinas biológicas são aproximadamente equivalentes a firewalls, software de filtragem de conteúdo e assim por diante; medicamentos antivirais biológicos são aproximadamente equivalentes a programas antivírus informativos; a quarentena ou restrição de movimento de pessoas e bens é aproximadamente equivalente a desconectar uma pessoa ou um computador da Internet. Estas equivalências grosseiras não podem ser tidas como garantidas, mas na dialética bioinformacionalista entre vírus biológicos e vírus da informação, elas podem servir como pontos de partida para o desenvolvimento de uma estratégia anti-pandémica comum.”(Peters, 2020)

https://doi.org/10.58086/7edc-2s28

Nas redes sociais digitais, os media virais não discriminam entre informação e conhecimento. Qualquer um pode gerar e fazer circular informações independentemente de seu valor de verdade. É um meio ideal para exageros, falsidades, mentiras e murmúrios tóxicos que são características da era da pós-verdade (Peters et al., 2018).

Já referimos que a pós-verdade não é um conceito novo. Todos os que leram 1984 de George Orwell podem facilmente imaginar um mundo onde um poderoso Ministério da Verdade comanda a lealdade a declarações contraditórias com o slogan "Liberdade é escravidão". A crença de que a verdade existe também pode esmorecer quando, como explicou a filósofa Hannah Arendt, aqueles que estão no poder repetem mentiras com tanta frequência que sobrecarregam a capacidade do público de saber o que é verdadeiro ou falso. A verdade fatual, afirmou Hannah Arendt no final dos anos 1960, é política por natureza. Os fatos são usados para justificar opiniões, e as opiniões conflitantes podem ser sustentadas legitimamente sobre os mesmos fatos. A liberdade de opinião é uma farsa, afirmou a filósofa. Afinal, a verdade é resistente ao debate.

“Do ponto de vista da teoria de Arendt, a pós-verdade está relacionada à pós-política. Não é a pós-verdade que transforma a política em pós-política, é a pós-política que gera a pós-verdade. Quando o significado da diferenciação entre poder e violência, diálogo e monólogo, imparcialidade e parcialidade, interesse comum e privado, cidadãos e as massas que consomem bens e serviços públicos desaparece, então o cinismo que rejeita a crença em qualquer verdade aparece e o poder de julgamento graças ao qual encontramos nossa orientação no mundo é destruído, por exemplo diferenciamos entre verdade e falsidade. Na pós-política, no entendimento de Arendt, a administração do estado atende à esfera privada - os interesses de grupos de capital e / ou religiosos. Há uma erosão gradual de valores e instituições políticas: liberdade, igualdade, solidariedade, poder comunicativo.” (Sepczynska, 2019).

A liberdade de viver em realidades paralelas definidas por "fatos alternativos" foi posta sob considerável pressão pelas exigências da pandemia COVID-19. A singularidade da realidade compartilhada voltou a mostrar-se com ímpeto quando todos fomos lembrados dos limites da "liberdade de acreditar" típica do pluralismo neoliberal. Agir com base em falsas crenças afetou todos os seres humanos nesta crise de risco globalmente compartilhado, potencializando ou prolongando a pandemia. (Tafarodi, 2020).

Acreditar no que mais nos agrada deixou de ser um problema e uma questão meramente pessoal quando afeta o todo. Negar fatos e a verdade põe vidas em perigo. Vender desinformação para fins políticos mostra-se imprudente, mesmo para populistas. A credibilidade perde-se quando se brinca com questões de vida ou morte e se origina uma descrença suspensa. (Loftus, 2020). Acreditamos que a própria pandemia pode vir a mudar este cenário, como um elemento disruptivo do próprio sistema.

https://doi.org/10.58086/7edc-2s28

Nesta chegada da era "pós-verdade", as pessoas podem ter parado de exigir a verdade porque entenderam que estão excluídas de qualquer tomada de decisão ou capacidade de mudar o seu ambiente. O "Infotainment" ou informações apresentadas como entretenimento tornaram-se comuns. Mas agora, durante a pandemia do coronavírus, diante de questões de vida ou morte, parece haver mais procura pela verdade. Os meios de comunicação têm a responsabilidade fundamental de apontar desinformações e deficiências, garantir a correta divulgação das informações fatuais e abster-se de politizar questões de urgência. As fontes de media que o fazem serão rotuladas como mais legítimas, enquanto outras que estão a tentar semear discórdia perderão credibilidade. A confiança é encontrada nas circunstâncias em que as pessoas trabalham juntas em prol de um objetivo maior. Reconstruir a confiança na sociedade vai demorar um pouco, pois a nossa crise de confiança decorre de muitos fatores estruturais complicados, incluindo a economia e os processos democráticos." (Loftus, 2020).

Referências Bibliográticas:

Arendt, H. (1971, Nov 18). Lying in politics: reflections on the Pentagon Papers. *New York Review of Books*. DOI: 10.1056/NEJMp2004361

Burnet, M., & White, D. O. (1972). *Natural history of infectious disease* (4th ed.). Cambridge University Press.

Camacho, M. M. (n.d.). The era of post-truth, post-veracity and charlatanism. DOI: 10.1056/NEJMp2004361

Camus, A. (1972). *La Peste*. Gallimard.

Conway, E. M., & Oreskes, N. (2010). *Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues From Tobacco Smoke to Climate Change*. Bloomsbury Press.

Daszak, P. (2020, Feb 27). We Knew Disease X Was Coming. It's Here Now. *The New York Times*. DOI: 10.1056/NEJMp2004361

Frankfurt, H. G. (1986). *On Bullshit*. Princeton University Press.

Funk, C., Hefferon, M., Kennedy, B., & Johnson, C. (2019, Aug). Trust and mistrust in Americans' views of scientific experts. *Pew Research Organization*. DOI: 10.1056/NEJMp2004361

Gates, B. (2015, March 18). Lessons from Ebola- We're not ready for the next epidemic. *Gates Notes – The blog of Bill Gates*. DOI: 10.1056/NEJMp2004361

Gates, B. (2020, April 9). Transcript: Bill Gates speaks to the FT about the global fight against coronavirus. *Financial Times*. DOI: 10.1056/NEJMp2004361

Global Preparedness Monitoring Board. (2019). *A world at Risk- Annual report on global preparedness for health emergencies*. World Health Organization. DOI: 10.2307/resrep24975

Habermas, J. (1987). *The theory of communicative action (Vol. 2): Lifeworld and system: A critique of functionalist reason*. Beacon Press.

Harari, Y. N. (2015). *Sapiens: A Brief History of Humankind*. Vintage.

Harari, Y. N. (2017). *Homo Deus: A History of Tomorrow*. Harper.

Harari, Y. N. (2018). *21 Lessons for the 21st Century*. Random House.

Harari, Y. N. (2018, Feb 28). Are we living in a post-truth era? Yes, but that's because we're a post-truth species. DOI: 10.1056/NEJMp2004361

Hoffower, H. (2020, Dec 15). Bill Gates has been warning of a global health threat for years. Here are 12 people who seemingly predicted the coronavirus pandemic. *Insider*. DOI: 10.1056/NEJMp2004361

Honigsbaum, M. (2019). *The pandemic century: One hundred years of panic, hysteria and, hubris*. W.W. Norton and Company.

Horton, R. (2020, Apr 9). Coronavirus is the greatest global science policy failure in a generation. *The Guardian*. DOI: 10.1056/NEJMp2004361

Jobs, S. (2005). You've got to find what you love,' Jobs says - This is a prepared text of the Commencement address delivered by Steve Jobs, CEO of Apple Computer and of Pixar Animation Studios, on June 12, 2005. Retrieved from Stanford News

Jones, D. S. (2020). History in a Crisis — Lessons for Covid-19. *The New England Journal of Medicine, 382*. DOI: 10.1056/NEJMp2004361

Jones, L. (2018). *The Big Ones – How natural disasters have shaped us (and what can we do about them)*. Doubleday Book.

Keyes, R. (2004). *The Post-Truth Era: Dishonesty and Deception in Contemporary Life*. St. Martin's Press.

Kucharski, A. (2016). Post-truth: Study epidemiology of fake news. *Nature, 540*(7634), 525–525. DOI: 10.1056/NEJMp2004361

Loftus, S. (2020, Apr 17). COVID 19: Post-Truth Age – Or Facts Making a Comeback? *The Globalist*. DOI: 10.1056/NEJMp2004361

McIntyre, L. (2018). *Post-Truth*. MIT Press.

Osterholm, M. (2007). Unprepared for a Pandemic. *Foreign Affairs, 86*(2), 34-47. DOI: 10.2307/20031836

Osterholm, M. T. (2005). Preparing for the Next Pandemic. *Foreign Affairs, 84*(4), 18-32. DOI: 10.2307/20031836

Osterholm, M. T. (2017). *Deadliest Enemy: Our War Against Killer Germs*. Little, Brown and Company.

Osterholm, M. T. (2020). Chronicle of a Pandemic Foretold - Learning From the COVID-19 Failure—Before the Next Outbreak Arrives. *Foreign Affairs, 99*(4), 70-87. DOI: 10.2307/20031836

Parmet, W. E., & Paul, J. (2020, July). COVID-19: The First Posttruth Pandemic. *American Journal of Public Health, 110*(7), 945–946. DOI: 10.1056/NEJMp2004361

Peters, M. A., McLaren, P., & Jandric, P. (2020, Apr 13). A viral theory of post-truth. *Educational Philosophy and Theory*. DOI: 10.1056/NEJMp2004361

Peters, M. A., Rider, S., Hyvoenen, M., & Besley, T. (Eds.). (2018). *Post-truth, fake news: Viral modernity & higher education*. Springer.

Peters, M. A., Tesar, M., Jackson, L., & Besley, T. (Eds.). (2020). *What Comes after Postmodernism in Educational Theory?*. Routledge.

Rosenberg, C. (1989). What Is an Epidemic? AIDS in Historical Perspective. *Daedalus, 118*(2), 1-17. DOI: 10.2307/20025233

Sanger, D. E., Lipton, E., Sullivan, E., Crowley, M. (2020, Mar 19). Before Virus Outbreak, a Cascade of Warnings Went Unheeded. *The New York Times*. DOI: 10.1056/NEJMp2004361

Saramago, J. (1995). *Ensaio sobre a cegueira*. Companhia das Letras.

Sardar, Z. (2010). Welcome to postnormal times. *Futures, 42*(5), 435-444. DOI: 10.1016/j.futures.2009.11.028

Schulman, R. (2020). COVID-19 and the Post-Truth Age: The Role of Facts in Public Policy | Summary of an Online International Conference. DOI: 10.1056/NEJMp2004361

Sepczynska, D. (2019). Post-Truth from the Perspective of Hannah Arendt's Political Theory. *Filozofia, 74*(3), 209–222. DOI: 10.1056/NEJMp2004361

Smil, V. (2008). *Global Catastrophes and Trends: The Next Fifty Years*. The MIT Press.

Stegmaier, W. (2011). Nietzsche como destino da filosofia e da humanidade? interpretação contextual do § 1 do capítulo "por que sou um destino", de ecce homo. *Trans/Form/Ação, 34*(1).

Tafarodi, R. W. (2020). A 'Post-Truth' Society and the COVID-19 Pandemic. DOI: 10.1056/NEJMp2004361

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House Trade Paperbacks.

Viner, K. (2016, Jul 12). How technology disrupted the truth. *The Guardian*. DOI: 10.1056/NEJMp2004361

World Health Organization. (2018). *2018 Annual review of diseases prioritized under the Research and Development Blueprint, Informal consultation, 6-7 February 2018, Geneva, Switzerland*. DOI: 10.2307/resrep24197

Xie, A. (2020, Apr 6). How the greedy ruling elite failed us, by putting profit before pandemic preparedness. *South China Morning Post*. DOI: 10.1056/NEJMp2004361