Journal of Engineering Science *Vol. XXIX, no. 4 (2022), pp. 72 - 83*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2022.29(4).08
UDC 004+004.056.5

THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY

Arina Alexei *, ORCID: 0000-0003-4138-957X,
Anatolie Alexei, ORCID: 0000-0002-0570-4854

Technical University of Moldova, 168 Stefan cel Mare Blvd., Chisinau, Republic of Moldova
*Corresponding author: Arina Alexei, *arina.alexei@tse.utm.md*

Received: 11. 02. 2022
Accepted: 12. 10. 2022

Abstract. The terms cyber security and information security are often used interchangeably, both in the academic literature and by organizations. This article aimed to identify whether these terms can be used interchangeably, analyzing the differences between the terms, based on several definitions identified in scientific articles and books, as well as definitions presented by specialized organizations. The analysis consists in determining the keywords, that define the terms, based on which conclusions were made. It has been determined that information security places a strong emphasis on the protection of information, cyber security refers to all assets that are part of cyberspace, such as end devices (including IoT), network devices, communication media and information. Cybersecurity is an umbrella term that includes: electronic communications network and computer security, physical security, infrastructure security, personnel security, hardware and application security, business process security. Through the identified results, important contributions are made both for the academic environment, as well as for governmental and non-governmental organizations, for the understanding and correct use of terms, to reduce uncertainty and to correctly approach specialist terminology, because the field of security is increasingly important, the challenges are complex and diverse.

Keywords: *asset, availability, confidentiality, cyber, information, integrity, threat.*

Rezumat. Termenii de securitate cibernetică și securitate a informației sunt adesea folosiți în mod interschimbabil, atât în literatura academică, cât și de către organizațiile specializate. Acest articol și-a propus să identifice dacă acești termeni pot fi utilizați interschimbabil, analizând diferențele dintre termeni, pe baza mai multor definiții identificate în articole științifice și cărți, precum și definițiile prezentate de organizațiile specializate. Analiza constă în determinarea cuvintelor cheie, care definesc termenii, în baza cărora s-au făcut concluzii. S-a stabilit că securitatea informației pune un accent puternic pe protecția informației, securitatea cibernetică se referă la toate activele care sunt parte a spațiului cibernetic, cum ar fi dispozitivele finale (inclusiv IoT), dispozitivele de rețea, mediile de comunicații și informația. Securitatea cibernetică este un termen umbrelă care include: securitatea rețelelor de comunicații electronice și a computerelor, securitatea fizică, securitatea infrastructurii, securitatea personalului, securitatea hardware și a aplicațiilor, securitatea proceselor de afaceri. Prin rezultatele identificate se aduc contribuții importante atât pentru mediul academic, cât și pentru organizațiile guvernamentale și neguvernamentale, pentru

înțelegerea și utilizarea corectă a termenilor, pentru reducerea incertitudinii și pentru abordarea corectă a terminologiei de specialitate, deoarece domeniul securității devine tot mai important, provocările fiind complexe și diverse.

Cuvinte cheie: *activ, disponibilitate, confidențialitate, cibernetică, informații, integritate, amenințare.*

1. Introduction

Currently, most of the economic, commercial, cultural, social and governmental activities and interactions of countries at all levels, including individuals, non-governmental and governmental organizations are carried out through the cyber environment [1], which has developed rapidly with the advent of the Internet. Along with the intense digitization attested at the international level, through the massive growth of electronic services, which are becoming more and more popular, the risks associated with cyber security also increase. The importance of cyber security increased substantially as a result of the use of the Internet between the 1980s and 1990s when the Internet became a quality resource for the consumer [2, pp. 33-39]. So that in the report presented by ENISA (The European Union Agency for Cybersecurity), for the years 2020-2021, cyber-attacks continued to grow, both in the diversity of the attack vectors used, as well as in the number of attacks and the impact they had [3]. The attack vectors were very diverse including: phishing and RDP attacks, DDoS campaigns, software supply chain, malware distribution, website compromise, vulnerable web applications, email-relevant vectors including phishing, spear phishing, whaling, business email compromises, etc.

The impact of the security breach can be estimated financially and in terms of the volume of compromised information. Thus, according to the annual report, produced by the Ponemon Institute and sponsored, analyzed, and published by IBM Security, which studied 550 organizations, from 17 countries and 17 industries, affected by data breaches that occurred between March 2021 and March 2022, reached the following results, the reported data breach losses are continuously increasing, so that from 2017 to 2022, they increased from $3.62 million to $4.35 million [4], with a percentage increase of about 12%. ENISA also published in July 2022, a worrying report on ransomware attacks, which have adapted and evolved to become more and more effective and cause more and more devastating damage. The monthly impact on the volume of data stolen, associated only with ransomware attacks, increased from 8 TB in May 2021 to 136 TB in June 2022 [5].

Cyber-attacks with a major impact on state infrastructures, at the international level, have devastating outcomes, and their number increases exponentially every year, The Center for Strategic and International Studies (CSIS), research organization dedicated to advancing practical ideas to address the world's greatest challenges, publishes troubling data on security incidents on a monthly basis. This data relates to the theft of personal data, such as the attack on Chinese police databases in July 2022, in which 1 billion records were compromised, this data was later put up for sale online; the attacks on the largest natural gas distributors from Greece in August 2022, caused a system outage; the DDOS attacks, which hit multiple public and private sector websites of the Romanian ministry of defense, border police, national railway company, and the OTP Bank in April 2022; the ransomware attacks in January 2022 on the Ukrainian government, which compromised the computers of government agencies [6]. Another cyber-attack, from October-November 2022, targeted the social media accounts of several officials from the Republic of Moldova, in the end all private conversations were made public.

With the start of the war in Ukraine and complicated geopolitical relations, the aggressiveness of attacks led by state-sponsored groups has essentially increased, according to the report presented by Microsoft, the most targeted industries in 2022 were Information Technology, NGOs and the education sector. The education and research sector were declared the most targeted in the report also presented by Check Point Software, multinational provider of software and combined hardware and software products for IT security [7]. A good example of this is the multiple attacks on China's Northwestern Polytechnical University, China accuses the U.S. National Security Agency (NSA), of infiltrating the university's electronic communications networks and stealing data [6].

In addition to all the challenges in the field, which are becoming more complex every year, an additional point of uncertainty is the interchangeable use of the term cyber security and information security. In the name of the governmental organizations of different countries, whose purpose and goals are similar, the terms cyber security and information security seem to have the same meaning, for example: Information Technology Service and Cyber Security (Republic of Moldova), the Federal Office for Information Security (Germany), National Cyber Security Center (Great Britain), Cybersecurity & Infrastructure Security Agency (USA), French National Agency for the Security of Information Systems (France). The same situation refers to the national state strategies, whose names also vary, as follows: Information Security Strategy of the Republic of Moldova 2019-2024, the German Cybersecurity Strategy, the Cyber Security Strategy of the United Kingdom, The National Cyber Strategy of the United States of America or The French national digital security strategy and not least the Cybersecurity Strategy adopted by the European Union in December 2020; using both terms, which creates uncertainty.

Based on the issues mentioned above, this research paper will try to identify the similarities and differences between cyber security and information security, to see if these two terms can be used interchangeably. The difference between this article and other articles that had the same purpose it to present different types of security, which are part of the umbrella term: cyber security; and based on the examples presented, to make a difference between cyber security and information security, which allows the correct use of the terms, when discussing issues related to national security, because the targets of cyber-attacks could be: individuals, states, connected devices and of course information, so it cannot be said that only information requires protection. Expanding the knowledge bases by presenting several definitions both taken from the academic and industrial environments, contributes to a better understanding of the studied terms and allows their use as appropriate. Also, the presentation of the trends of the last 18 years, in order to be able to analyze the international use of the terms in this field, contributes to highlighting the term cyber security versus other types of security.

The second section of the article is reserved for the literature review, the third section will contain various reflections and discussions on the research question, and the last section is reserved for conclusions.

2. Literature review

The definitions that will be presented in this section have been divided into those given by the academic environment, through books and published scientific articles and the industrial environment.

2.1 Information Security

Information security is a science that was tackled many centuries ago. The Encyclopedia Britannica records the use of cryptology in 400 BC by the Spartans, who used a device called the scytale for secret communication between military commanders [8]. During the 4th century, A.H. Aeneas Tacticus wrote a work entitled "On the Defense of Fortifications", one chapter of which was devoted to cryptography, making it the earliest treatise on the subject [8]. Since then, the importance of information security has been addressed and studied to meet the challenges of data protection, first for the classic form of data retention and analyzed also in the case of electronically stored data, with the evolution of modern technologies.

Over time, this term has been analyzed and addressed both by the industrial and the academic environment. Several definitions have been presented for a more accurate approach to the term. To achieve the purpose of this paper, an attempt will be made to analyze information security from different perspectives to understand whether it is an interchangeable term with cyber security or not. The fundamental principles of both terms are the same: confidentiality which ensures the access of authorized persons to information, integrity which refers to the accuracy of data and the availability of data to authorized users at the time of the request. In the meantime, some additional properties have been attributed to information security, by International Organization for Standardization (ISO), such as: authenticity, accountability, non-repudiation, and reliability [9]. ISO defines information security as: "the preservation of confidentiality, integrity and availability of information" [10], and extended the definition by adding the previously mentioned properties.

Several published scientific papers were identified, the purpose of which was to identify the meaning of the term information security, the purpose of which was similar to that of the present paper, namely to better understand the term to have a correct approach. Researchers from the Republic of Moldova define information security as a process that refers to "any information, IT or non-IT (books, reports, documents, etc.), on any traditional supports (paper, cloth, etc.) or electronic media (magnetic tape, CD, etc.), in any form (text, graphics, audio, video), communicated traditionally (written, oral, regular mail) or electronically (e-mail, chat, mobile phone)" [11]. The researcher's von Solms & van Niekerk, who over time have carried out several types of research in this field, define Information security as: "the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities" [12], in other words, information is the asset that needs to be protected, information security is seen to be the process [12]. Having clearly defined the intention to identify a theory relevant to information security, Craig A. Horne et al. [13], concluded that no theory on information security was apparent in the literature, and there does not seem to be a way to measure when information has been protected enough. In his book, Whitman & Herbert define information security as" the protection of information and the systems and hardware that use, store, and transmit that information" [14, p.3]. According to the definition given by Ogbanufe, information security refers to the protection of digital and physical data against unauthorized access, disclosure, modification, or deletion [15].

Definitions were also identified in the most developed dictionaries and specialized organizations, so Oxford Dictionary defines information security as "ways of protecting information, especially electronic data, from being used or seen without permission". The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and information systems from unauthorized access, use, disclosure,

disruption, modification, or destruction to provide confidentiality, integrity, and availability". Information security, according to the Escal Institute of Advanced Technologies (SANS Institute) which specializes in information security and cybersecurity training, refers to "the processes and methodologies which are designed and implemented to protect the print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption" [16]. ISACA (Information Systems Audit and Control Association) treats information security as assurances within the enterprise that information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability) [17].

From the analysis of the definitions presented above, proposed by both researchers and specialized organizations, it can be stated that information security is particularly oriented towards information, as an important asset, which requires protection, regardless of its state: digital or printed. In other words, the main emphasis is placed specifically on information, ICT (information and communication technology) systems are targeted only from the perspective of protecting the information that resides in these systems as well as the physical environments in which the information could be located, such as cabinets, storage areas and buildings.

2.2 Cyber Security

The term cyber security appears in the literature and various studies, in two different forms. As a combination of 2 words "cyber security" or as a single word with the prefix "cybersecurity", in any case, it has 2 components, just like the term information security. In the case of information security, it is clear that it mainly refers to information, as the definitions in the previous section have also shown. In the case of cyber security, various discussions arise concerning the word "cyber". The analysis of specialized literature showed that the terms "Cybersecurity" and "Cyber Security" can be used interchangeably, because they have the same object of study, to demonstrate this, the definitions related to cyber security in this section will be given with the terms used by the authors.

The word "cyber" evolved from the scientific work of Norbert Wiener [9], in his work "Cybernetics; or control and communication in the animal and the machine", from 1948, which described the term cybernetics as the interaction between man and machine, the resulting system can create an alternative environment of interaction [18]. The etymological meaning of the term "cybernetics", according to Wiener's notes [18], is the Greek word "kybernetes", which was selected due to the sense of control over actions, comes from the Greek word "steersman", meaning "the one who steers" [19].

Meanwhile, multiple definitions have been given to the term "cyber". Thus, NIST defines cyber as "referring to both information and communications networks" [20]. Merriam-Webster Dictionary and Cambridge Dictionary, define cyber: as relating to or involving computers or computer networks (such as the Internet). To expand the contemporary definitions and make a connection with the initial definition given by Wiener, the definition of the term "cyber" must include the human factor, without which the interaction of systems and technologies would not exist, the interaction environment called by Wiener "cybernetic" does not can be formed, which directly contradicts the original definition of the term. The hypothesis is also supported by researchers Thomas Edgar & David Manz, in the book "Research Methods for Cyber Security", who claim that: "Cyber systems would not have a

function without human intervention" [4, pp. 33-39]. Cyber systems are part of cyberspace, they represent the physical manifestations of cyberspace activity, with which humans interact, and cyber security is part of every interaction [4, pp. 33-39].

The history of cyber security began much later, researchers refer to the first research published in 1970 [21], the paper was a technical report that analyzed and presented the security issues of computer systems and presented the comprehensive approach to security as a mix of hardware, software, communications, physical, personal and administrative controls, which require an implementation to ensure security [21].

Next, as in the previous section, various definitions for the term cyber security, addressed by researchers and the industrial environment, will be presented.

Researchers Bragaru & Briceag presented a definition adapted from the ISO/IEC 27032 standard, such that cyber security has the meaning of "...any security related to cyberspace, which is a complex environment that occurs in the process of interaction between people, software and internet services provided through technological devices or integrated networks" [11]. Edgar & Manz define: cyber security as a domain that includes the technologies, policies, and procedures to secure something within cyberspace [4, pp. 33-39]. Cyberspace was defined by NIST as: "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [20].

Von Solms & van Niekerk define cyber security as "the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" [12]. The tangible asset is e.g. the protection of network devices, and the intangible assets are e.g. all the ethical aspects, vulnerable to cyber-attacks [12]. Researchers Li & Liu define cyber-security as" includes practical measures to protect the information, networks, and data against internal or external threats" [22]. Another definition characterizes cyber security as that which refers to the understanding of the problems that can arise as a result of various cyber-attacks and the development of defense strategies (e.g countermeasures) that preserve the confidentiality, integrity and availability of any digital and information technologies [23]. Researcher Shahid Alam defines cybersecurity as the security of the new digital age, also known as Cyberspace [24]. The CIA triad, analyzed from the perspective of cyber security refers to confidentiality as control over access, operations and disclosure of system elements; integrity as modification, manipulation, or destruction of elements in the system; availability as well as access to the services of elements in the system [24]. Researchers Schatz & al defined cyber security as "The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users" [25].

In the industrial environment, cyber security has many definitions, which will allow us to analyze this term even more deeply. Cybersecurity is "the practice of protecting systems, networks and programs from digital attacks," according to Cisco, "these attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes". IBM defines Cybersecurity as" the practice

of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization". The International Telecommunication Union (ITU) defines cybersecurity as " the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment" [26]. The cyber environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks [26]. ISO/IEC describes cybersecurity as the " preservation of confidentiality, integrity and availability of information in Cyberspace"[27]. ENISA defines that "cybersecurity shall refer to the security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalized telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace" [28]. ISACA refers to the cybersecurity as "the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems". In Gartner Glossary, cybersecurity is the combination of people, policies, processes, and technologies employed by an enterprise to protect its cyber assets.

The Oxford Dictionaries defines cybersecurity as: "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". The Merriam –Webster dictionary defines cybersecurity as: "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack".

From the definitions presented above, it can be concluded that cyber security is an umbrella term, which includes several types of security, the common property of which is the connection to communication networks, the services provided to users are electronic services because cyber security does not exist outside cyberspace. Figure 1 shows all the components of cyber security from the authors' perspective, as a result of analyzing the key words in the definitions presented above.

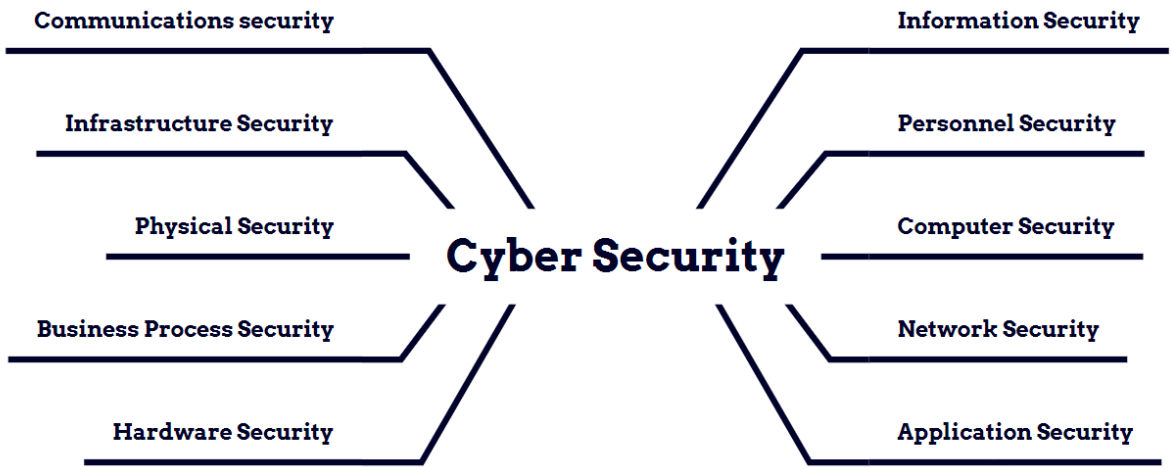

Figure 1. Cyber security - umbrella term.

Infrastructure Security refers to protecting electronic systems and responding to unauthorized incidents involving a country's infrastructure [29]. Physical security refers to all the devices, technologies and materials used for the perimeter, external and internal protection, which includes: doors, barriers, sensors, access control systems, etc. [30], to protect an enterprise's cyber assets. Business process security is based on the integration of security in the life cycle of business processes that use modern technologies, such as Cloud Computing [31]. Hardware security refers to the protection of devices that are part of cyberspace, that is, they are capable of being connected to communication networks. Information security as part of cyber security is based on the protection of electronic information. Personnel security refers to intangible cyber assets and ethical aspects of protecting human beings as part of the cyber environment. Computer security in the context of cyber security refers to computer systems that connect to telecommunications networks to communicate, excluding computers that are not connected to the network [12]. Network security refers to the security of network devices and connection media. Application security refers to the development of secure software. Communications security refers to ”the protection of all communications media, technology, and content” [12].

3. Discussion

In cyber security, electronic information is an asset as important as devices, applications, telecommunications networks and people, is part of the cyber assets; more than that information can be seen as an important vulnerability in cyberspace. Whereas in information security, information is the primary asset that requires protection [12].

To identify the important differences between cyber security and information security, an attempt will be made to analyze the nature of attacks in cyberspace, to elucidate whether the ultimate target is information, or not.

When referring to the attack vectors described in the first section of this article, the vast majority are aimed at information security in cyberspace, that is, in this context cyber security and information security are interchangeable terms since the asset to be protected is electronic information, concerning such attacks as phishing, spear phishing, whaling, business email compromises, DoS and DDoS, malware distribution especially ransomware, website compromise, vulnerable web applications, etc. The variety of security threats in cyberspace is much more complex than those described here.

Definitions given by researchers, concerning the nature of cyber-attacks, are further confirmation of the differences between the terms. Researchers Bullock et al, define cyber security as addressing different cyber threats, such as cyber war, cyber terrorism, cyber-crime, cyber espionage and cyber sabotage [32], which do not necessarily target information, targets can also be other cyber assets: telecommunications networks, computers, IoT devices, and humans.

Cyberspace is very dynamic, so changes in cyberspace are happening all the time and at an accelerated pace, based on the constant development of communication and computing technologies [22]. The dependence of states on the cyber environment has greatly increased for communication and control over physical environments [22], unknown vulnerabilities appear with every change in modern technologies and provision of new electronic services.

In Table 1, several common cyber-threats that do not target information can be reviewed.

Table 1

Threats on cyber assets except for information

No	Target	Vulnerable cyber assets	Vulnerable protocols	Attack Types	Recent cases
1.	IoT devices	Smart homes, smart offices, smart classroom or smart lab devices: smart lock, web cameras, home gateway, voice-activated home automation device, etc.	TCP UDP Non-standard Wireless protocols: Wi-Fi, Z-wave, XBee, Zigbee, Bluetooth, LoRA	DDoS Buffer Overflow Backdoor Installation Address Spoofing Man in the Middle Session Hijacking SQL Injection Routing Attack Malicious codes [33]	The Mirai malware, which mainly compromises IoT devices, diversified its number of variants by 57% in 2019 compared to the same period in 2018 [34].
2.	Person	Users' end devices, social media accounts	TCP UDP	Cyber bullying	The Cyberbullying Research Center in the USA has conducted 12 research studies from 2007 until now, the data is worrying, from May 2007 to April 2021, the percentage of teenagers aged 12-17 years, who were victims of cyberbullying have increased from 18.8% to 45.5%.
3.	End devices	Users' end devices and their resources, like: RAM, CPU, SSD/HDD, tec.	RDP HTTP	Malware	The Emotet malware in 2019 created 100,000 more botnets than in 2018, representing a 913% increase in the number of botnetized end-user devices [34].
4.	Digital media	Network devices: routers, switches, servers.	TCP UDP FTP DNS, etc.	Malware	Sony Pictures (2014), Netflix, ABC and HBO (2015). Unauthorized posting of media products in the public environment reduces the income of the production companies, because the public can access them for free, without having to go to cinemas or pay monthly subscriptions to gain access.
5.	Critical infrastructure	Network devices: routers, switches, servers; and network services	All network protocols	DDoS Malware	In June 2022, Hackers targeted Lithuania's state railway, airports, media companies, and government ministries with DDoS attacks [6]. The target of these attacks is oriented toward the interruption of critical national services.

So, where the target of cyber-attacks is information, the terms cyber security and information security can be used interchangeably. In the case of cyber-attacks targeting: IoT equipment, organizational business processes or critical state infrastructure, people or actions leading to financial harm (as in the case of digital media), cyber security is a different term. In the case of information printed and stored in physical format, the protection of this information relates to information security, but not to cyber security, as it is not a cyber asset.

To present how widely used the terms information security and cyber security are, as well as other terms such as network security, infrastructure security, or computer security, the Google Trends tool was used to analyze internationally, in the period 10.01.2004-10.01.2022, the results can be analyzed in figure 2.

From figure 2 it can be seen that Google searches show a line with an increasing trend for the term cyber security, especially since 2009, when it was used by the ex-president of the USA, Barack Obama, in his press release referring to the importance of cyber security [25]. Trend lines are used to reflect the total number of searches for a term compared to other terms. The other terms proposed for analysis, including information security, have negative trend lines.

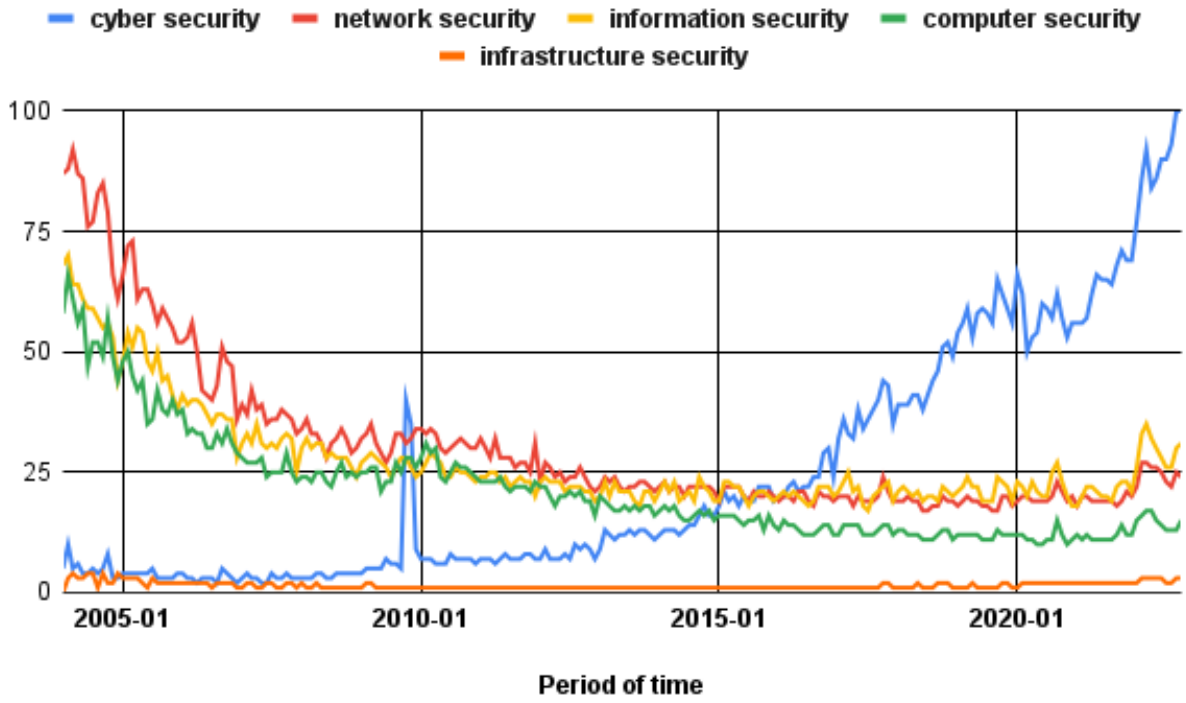

Figure 2. Google search trends for security terms 2004-2022 [35].

These results are indicative but important to identify trends [36]; but also, to present further proof of the hypothesis that cyber security represents an umbrella term for several types of security.

4. Conclusions

With the outbreak of the war in Ukraine, but also before, with the Covid-19 pandemic and the shift to remote work, cyber-attacks have steadily increased, with targets ranging from information and devices to people. Until now, states have each defined a strategy to be implemented to defend against cyber-attacks, where the terms information security and cyber security are used interchangeably.

But as discussed in this article, these two terms can be used in this way when the target of the attacks is information, when the target is various infrastructure services, cyber assets, or people, as a constituent part of cyberspace, they can no longer use the term information security, but rather the term cyber security. Several definitions have been presented, in order to be able to define these two terms as comprehensively as possible and to improve the knowledge base in this field, international trends can be used as an additional argument to justify the use of the term cyber security, as a term that covers more technological issues than information security.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Ghamdi, M.I. Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings* 2021. DOI: 10.1016/J.MATPR.2021.04.098.
2. Edgar, T.W.; Manz, D.O. *Research Methods for Cyber Security*. 1st ed., Elsevier, United States, 2017, 402 p.

3 Enisa Threat Landscape 2021. Available online: https://www.enisa. europa. eu/publications/ enisa-threat-landscape-2021 (accessed on 05.09.2022).
4. Cost of a Data Breach Report 2022. Available online: https://www.ibm. com /downloads/cas/3R8N1DZJ (accessed on 06.09.2022).
5. Enisa Threat Landscape for Ransomware Attacks. Available online: https:// www.enisa. europa.eu/ publications/enisa-threat-landscape-for-ransomware-attacks (accessed on 05.09.2022).
6. Center for Strategic and International Studies (CSIS). Significant Cyber Incidents. 2022. Available online: https://www.csis.org/programs (accessed on 12.09.2022).
7. Check Point Research. Cyber Security Report. 2022. Available online: https://www.checkpoint.com (accessed on 20.10.2022).
8. Encyclopedia Britannica. Available online: https://www.britannica.com/topic/ cryptology (accessed on 06.09. 2022).
9. Bay, M. What is cybersecurity? *French Journal for Media Research* 2016, 6, pp 1-28. ISSN 2264-4733.
10. ISO/IEC 27001: Information Security Management, International Organization for Standardization, Geneva, Switzerland, 2013. Available online: https://www.iso.org/isoiec-27001-information -security.html (accessed on 02.09.2022).
11. Bragaru, T; Briceag, V; Malcoci, V; Galaicu, V. Information Security vis-à-vis Informational Security. *Studia Universitatis Moldaviae* 2019, 2 (122), pp. 38–47. [in Romanian].
12. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Computer Security* 2013, 38, pp. 97–102. DOI: 10.1016/j.cose.2013.04.004.
13. Horne, C.A; Ahmad, A; Maynard, S.B. A Theory on Information Security. In: *The 27th Australasian Conference on Information Systems*, Wollongong, Australia, 2016.
14. Whitman, M. E.; Mattord, H.J. *Principles of Information Security*. 7th ed., Cengage Learning, 2021; p. 658.
15. Ogbanufe, O. Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computer Security* 2021, 108, pp. 102340. DOI: 10.1016/ J.COSE. 2021.102340.
16. SANS Institute. Information Security Resources. Available online: https://www. sans.org/information-security (accessed on 06.09.2022).
17. Cooke, I. Doing More with Less. *ISACA* 2017, 5, pp. 6-9.
18. Wiener, N. *Cybernetics; or control and communication in the animal and the machine*. John Wiley, USA, 1948; 231 p.
19. Merriam-Webster.com Dictionary. Available online: https://www.merriam-webster.com/dictionary/steersman (accessed on 10.09.2022).
20. National Institute of Standards and Technology. Information Security. Available online: https://csrc.nist.gov/ glossary/term/cyberspace (accessed on 10.09.2022).
21. Ware, W. H. *Security controls for computer systems*. Rand Corp Santa Monica CA, USA, 1970, 80 p.
22. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* 2021, 7, pp. 8176–8186. DOI: 10.1016/J.EGYR.2021.08.126.
23. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences* 2014, 80 (5), pp. 973–993. DOI: 10.1016/j.jcss.2014.02.005.
24. Alam, S. *Cybersecurity: Past, Present and Future*. Lambert Academic Publishing, Germany, 2022; pp. 2-8. DOI: https://doi.org/10.48550/arXiv.2207. 01227.
25. Schatz, D.; Bashroush, R.; Wall, J. Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law* 2017, 12(2), pp. 53-74. DOI: 10.15394/jdfsl. 2017.1476.
26. ITU-T X.1205. Overview of cybersecurity. Available online: https:// www.itu.int/ en/ITU-T/study groups/com (accessed on 10.09.2022).
27. ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary, "International Organization for Standardization," Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard /73906 (accessed on 22.09.2022).
28. National Cybersecurity Strategies. European Network and Information Security Agency. Available online: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide (accessed on 04.09.2022).
29. Abouzakhar, N. Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. In: *12th European Conference on Cyber Warfare and Security* 2013, pp. 1–10.

30. Al-Fedaghi, S.; Alsumait, O. Towards a conceptual foundation for physical security: Case study of an IT department. *International Journal of Safety and Security Engineering* 2019, 9 (2), pp. 137–156. DOI: 10.2495/SAFE-V9-N2-137-156.
31. Farah, A.; Saida, B.; Mourad, O. C. On the security of business processes: classification of approaches, comparison, and research directions. In: *International Conference on Networking and Advanced Systems (ICNAS)*, 2021, pp. 1–8. DOI: 10.1109/ICNAS53565.2021.9628908.
32. Bullock, J. A.; Haddow, G. D.; Coppola, D. P. *Cybersecurity and critical infrastructure protection. Introduction to Homeland Security*. Butterworth-Heinemann, 2021; pp. 425–497. DOI: 10.1016/B978-0-12-817137-0.00008-0. ISBN: 978-0-12-817137-0.
33. Alexei, A.; Alexei, A. Analysis of IoT security issues used in Higher Education Institutions. *International Journal of Mathematics and Computer Research* 2021, 9 (5), pp. 2277-2286. DOI: 10.47191/ijmcr/v9i5.01.
34. Enisa Threat Landscape Botnet 2020. Available online: https://www.enisa. europa. eu/ topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-botnet (accessed on 12.09.2022).
35. Data source: Google Trends. Available online: https://trends.google.com/trends/explore?date=all&q=cyber%20security,network%20security,information%20security,computer%20security,infrastructure%20security (accessed on 20.09.2022).
36. Choi, H.; Varian, H. Predicting the Present with Google Trends. *Economic Record* 2012, 88, pp. 2–9. DOI: 10.1111/j.1475-4932.2012.00809.x.

Citation: Alexei, A.; Alexei, A. The difference between cyber security vs information security. *Journal of Engineering Science* 2022, 29(4), pp. 72-83. https://doi.org/10.52326/jes.utm.2022.29(4).08.

Submission of manuscripts: jes@meridian.utm.md