ELEKTROTEHNIŠKI VESTNIK 91(1-2): 8-20, 2024
OVERVIEW SCIENTIFIC PAPER

Analyzing Cybersecurity Strategies of the European Union: Challenges and Opportunities for Public Administration

Damjan Fujs [1,*], **Igor Bernik** [2]

[1] *University of Ljubljana, Faculty of Computer and Information Science, Večna pot 113, 1000 Ljubljana, Slovenia*
[2] *University of Maribor, Faculty of Criminal Justice and Security, Kotnikova ulica 8, 1000 Ljubljana, Slovenia*
[*] *E-mail: damjan.fujs@fri.uni-lj.si*

Abstract. Cybersecurity attacks have increased in recent years, both on the EU and global levels, in terms of their number and impact. The public administration sector is particularly at risk, as this is where most cybersecurity attacks take place. It is therefore important to develop comprehensive information security strategies on both the organizational and national level. Strategies help to set up a relatively long-term focus and priorities. The aim of our study is to understand how the EU member countries deal with such challenges. To achieve this, we analyze three indices: the level of penetration (PL), level of digitalization (DL), and global cybersecurity index (GCI). We examine individual national strategies to provide a basis for a comparative analysis which can serve as a reference for improving the long-term cybersecurity in the public administration.

Keywords: information security, cybersecurity, strategy, ENISA, public administration, European Union

Analiza strategij kibernetske varnosti v Evropski uniji: izzivi in priložnosti za javno upravo

Napadi na kibernetsko varnost so se v zadnjih letih močno povečali, tako na ravni EU kot tudi globalno, ne le po številu napadov, temveč tudi po njihovem vplivu. Sektor javne uprave je še posebej ogrožen, saj se zoper le-tega izvrši največ napadov. Zaradi tega je ključnega pomena razviti celovite strategije informacijske varnosti tako na organizacijski kot tudi na nacionalni ravni. Strategije pomagajo določiti relativno dolgoročne usmeritve in prednostne naloge. Cilj te študije je razumeti, kako se države EU spopadajo s takšnimi izzivi. Da bi to dosegli, sočasno analiziramo tri indekse: stopnjo penetracije (PL), stopnjo digitalizacije (DL) in globalni indeks kibernetske varnosti (GCI). Analiziramo tudi posamezne nacionalne strategije držav EU. Študija predstavlja primerjalno analizo držav članic EU, ki lahko služi kot referenca za izboljšanje dolgoročne kibernetske varnosti v javni upravi.

Ključne besede: informacijska varnost, kibernetska varnost, strategija, ENISA, javna uprava, Evropska Unija

1 INTRODUCTION

Attacks on the cybersecurity have increased in recent years, both on the European Union (EU) level and globally, not only in terms of the number of the attacks but also in terms of their impact [1]. Successful cybersecurity attacks can cause various types of the damage, such as a financial damage, reputational damage, unauthorized access to data, etc. In addition, the costs associated with the cybersecurity incidents also increase [2] and the EU is no exception. Moreover, the cybersecurity has become one of the most important security priorities [3]. Due to the increasing number and impact of the cyberattacks, it is important to develop comprehensive information security strategies on both the organizational and national level. Such strategies are essential to effectively manage the risk, protect the critical infrastructure, and ensure the privacy and information security in general. The Strategies are characterized by the fact that they are, like the strategic decisions (as opposed to the operational or tactical decisions), of a long-term nature [4]. It is also essential to review and update cybersecurity documents (such as policies) as threats continue to evolve as new security risks and technologies require flexibility and innovation to protect themselves against attacks [5]. Also to be mentioned is that the organizational cybersecurity strategies are operationally oriented on specific needs of organizations [6]. Thus, the focus of our study is on national cybersecurity strategies. Their advantage is in not needing to be often updated because of their general character [7] and in being planned for a longer period. Our interest is to know how often the EU Member countries update their national cybersecurity strategies. In this context, our first question to be answered is:

RQ1: How often do the EU countries update their cybersecurity strategies?

The EU plays an important role in shaping cybersecurity strategies (and policies) in its member countries [8]. As the cybersecurity threats become more sophisticated and pervasive, examining the EU cybersecurity strategies from a public administration perspective is of a great importance. The public administration sector is particularly at risk, as this is where most incidents of the cyberattacks occur, leading to a disruption of services and breaches of personal data [1]. Our study examines some aspects of the EU

Received 14 December 2023
Accepted 5 March 2024

cybersecurity strategies in the context of the public administration. It highlights the potential benefits for policymakers, public administrations, and the overall digital resilience of the member countries. It is known that a high level of digitalization is associated with a higher level of penetration [9]. Besides that, we are particularly interested in the relationship between the level of the cybersecurity (GCI), the level of penetration (PL) and digitalization (DL). DL measures the degree to which governments provide digital public services while PL measures the level of internet usage by individuals when interacting with public authorities [9]. Following the above, our next research questions are:

RQ2: What is the state of digitalization and the extent of using government services in the EU countries?

RQ3: What is the state of the cybersecurity in the EU countries?

As a society becomes more dependent on the technology and the internet, the prevalence of the various cyberattacks also increases [10]. Coppolino et al. [11] have a similar view. According to them the increase in the intensity of the cyber-attacks is accompanied by an increasing number of interconnected devices, as well as a significant increase in virtualization and the use of public cloud services. In this context, our fourth research question is:

RQ4: Can the high level of the cybersecurity in the EU countries be attributed to the extent of digitalization and government service utilization?

The paper provides an analysis of the EU cybersecurity strategies and their potential impact on selected aspects of the public administration. Although few studies specifically address this issue, our study fills this gap by examining the EU cybersecurity policies in relation to the indices (level of digitalization, level of penetration and national cybersecurity index). Some aspects of the cybersecurity strategies have been researched, but there is no aggregated overview of all cybersecurity strategies and their relation to the public administration. Drawing on a range of sources, including the academic literature, governmental reports and publications of international organizations, we examine the interconnectedness between the EU cybersecurity strategies and public administration practices, with a particular focus on digital transformation, cybersecurity governance, and capacity-building efforts. Our research aims to provide a deeper understanding of the relationship between the EU cybersecurity strategies and public administrations and to provide insights and recommendations to policymakers, public administrations, and other stakeholders on how to strengthen the cybersecurity resilience in the digital age. By filling this gap, our study contributes to the field of the cybersecurity governance and public administration by highlighting the importance of aligning the cybersecurity strategies with the specific needs and challenges of the public administration in the EU.

The rest of the paper is structured as follows. In the next section, we provide an overview of the literature on the cybersecurity strategies, public administration, and their interplay where we discuss the limited research specifically focused on the EU cybersecurity strategies within the context of the public administration, highlighting the need for a comprehensive analysis. In the *Research Methodology and Interpretation of Results* section, we present the methodological approach employed in our study and interpretation of the results. Section *Comparing the EU strategies and their implications on the public administration* presents an additional argumentation and public administration aspects addressed in the national cybersecurity strategies. In the *Discussion* section, we answer the research questions and discuss the results. In the last section, we draw conclusions of our work and present directions for a further study and limitations of the presented one.

2 Literature review

The strategy is defined as a document that determines the desired direction for a business and formulates the most effective course of action to achieve that goal [6]. When dealing with national cybersecurity strategies, it is important to consider a bigger picture, as we are dealing with a larger entity. Thus, a national cybersecurity strategy is one of the most essential documents for formulating cybersecurity policies [12]. For example, the European Commission [13] has published the EU Cybersecurity Strategy for the Digital Decade, which sets out the main strategic orientations for the future cybersecurity. The 2020 adopted Berlin Declaration [14] highlights the importance of digital transformation in the public administration. Besides the EU strategy, there are also cybersecurity strategies of individual EU member countries [15]. The national cybersecurity strategies are often highlighted in the literature. For example, Štitilis et al. [12] present a comparative analysis between the EU countries on some aspects of the cybersecurity strategies, Górka [16] analyzes the cybersecurity strategies of the Visegrad group countries, Jacuch [17] provides a comparative analysis of the EU cybersecurity strategies with a particular focus on Poland.

Previous studies in the cybersecurity in relation to the public administration mainly focused on different operational activities. For example, Ubowska and Królikowski [18] suggest that the cybersecurity culture should be built on the basis of the user awareness, which can reduce the number of incidents in the public administration. Romanovská and Pitner [10] compare the Belgian and Australian strategies, paying no regard to the regional or community accountability. They claim that involving lower levels of the government in the strategies would be helpful, as this potentially provide an even better cybersecurity (at the regional level). Subban and Jarbandhan [19] describe the future and the role of the public administration in the context of the cybersecurity.

In doing so, they highlight several recommendations to improve the policies, such as updating the cybersecurity measures, training staff, simplifying procedures, etc. Yanakiev and Polimirova [20] conduct a survey among experts urging them to ensure a long-term nature of strategies and emphasizing the need to establish procedures for reviewing and updating the strategies. Coppolino et al. [11] review the cybersecurity threats in the local public administration sector, highlighting the importance of the risk assessment, threat intelligence and advanced security monitoring techniques to improve the cybersecurity levels. Nagy-Takács and Berényi [21] give an overview of the state of the field and the most important elements of the information security in the public administration in Hungary, also mentioning the national cybersecurity strategy. Alvarez-Rodriguez et al. [22] analyze the best practices of the Spanish interoperability framework, which allows the public administration to share the public information faster and easier, thus reaching the digital maturity faster. They find it important that countries rely on the European initiatives and policies. Crahay et al. [23] explore the Berlin Declaration signed by the 27 EU member countries in December 2020 to highlight the importance of digital public services, as digitalization plays a key role in shaping the EU digital decade. Maglaras et al. [24] examine the progress of Greek national cybersecurity strategy and highlight the positive impact of the strategic guidelines on shaping the online security.

When addressing the impact of certain factors on the cybersecurity (direct or/and indirect), our focus is on two factors (i.e., indices), namely PL and DL. PL reflects the degree of how much users interact with public authorities through the internet, while DL measures the degree to which governments provide digital public services [9]. Both concepts are relatively well explored in the literature. In recent years in particular, much attention has been paid to digitalization (and technological advances) as an important contributor to the economic growth [25] and to other sectors and areas at a local, regional and global level. As the number of the devices [26] and the internet users increases [27], the use of digital public services is expected to grow, making it particularly important that public administrations know how to ensure a robust cybersecurity.

To get an insight into the situation in the field of the cybersecurity, we can refer to one of the established indices, i.e., the Global Cybersecurity Index (GCI). GCI was established by the International Telecommunication Union [28]. GCI is one of the most comprehensive indicators to measure the commitment to the cybersecurity [29]. Its aim is to help countries identify areas for improvement and inspire them to act by raising awareness of the global cybersecurity landscape. GCI presents an overall score based on five dimensions [28]: legal, technical, organizational, capacity development and cooperation measures. Bruggemann et al. [30] analyze 11 countries with the highest GCI ranking and address specific pillars focusing on small-and medium-sized enterprises. Chen et al. [31] explore some socioeconomic factors to predict the cybercrime, noting that political efforts decrease the cybercrime occurrence to some extent. From our research perspective, this is an important finding as politicians play a vital role in adopting policies (including the cybersecurity). Onumo et al. [32] propose a research model to find additional (significant) dimensions that affect GCI. One of their hypotheses is that countries with a long-term orientation tend to have high levels of the cybersecurity development. Koniagina et al. [29] analyze GCI in relation with the legislation of the Russian Federation imposed on the Internet of Things. Similarly, Nehrey et al. [33] analyze the top ten countries according to GCI and analyze the situation in detail and give advice on how to improve cybersecurity in Ukraine.

The focus of our study is on individual dimensions. GCI is used as a whole score to determine the given country cybersecurity state. Our focus is on the EU countries, whereas previous studies have focused on the global state of the cybersecurity [30], [33] or on individual countries [29], [33].

3 Research Methodology and Interpretation of the Results

In our study, we use a mixed-methods research approach, i.e., a combination of a qualitative and quantitative research approach [34]. The study is divided into two analytical parts. The first part refers to a quantitative analysis of the cybersecurity strategy releases and exploration of certain indicators, while the second part refers to a qualitative analysis of national cybersecurity strategies in the EU with a focus on the public administration. The study includes all the 27 EU member countries in a sample analysis. The analytical part comprises several steps. First, we examine the dynamics of the updates of the national cybersecurity strategies of the EU member countries. Second, we compare the different indices of the EU countries (e.g., DL, PL and GCI). Third, we provide an aggregated analysis of all countries against the indices to get a more comprehensive overview of the current state of DL, PL and GCI. Our analysis is divided into two parts for a better understanding of the graphs. The

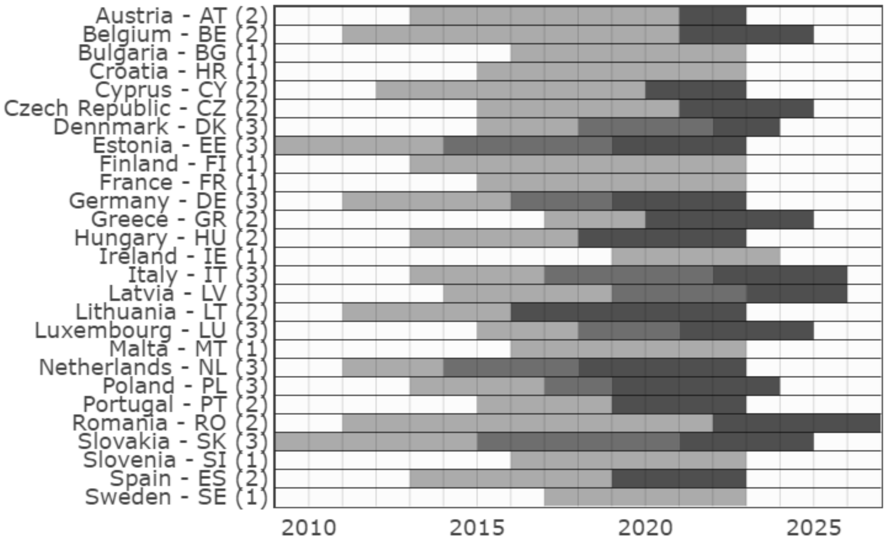

Figure 1. Timeline plot showing the change between the sets of the date data points. A comparison of the cybersecurity strategies by the number of document releases. Values on the Y-axis represent countries with the name and international country code and the number of versions (in parentheses). Values on the X-axis indicate the years. Note: the numbers in brackets for each country represent the total number of the strategy releases.

first part (Figure 2) shows the DL, GCI and PL situation over countries with below-average GCI scores. The second part (Figure 3) shows the DL, GCI and PL situation over countries with above-average GCI scores. The average of the 27 EU member countries in terms of GCI is 91.26%. The DL and PL indices for the countries are from [9] and the GCI one is from [28]. The following symbols are used to interpret the average values: x is the sample mean average and μ is the population mean average (the average of the 27 EU member countries).

In the second part, we present our findings concerning the public administrations in national cybersecurity strategies. We use a qualitative analysis of the available cybersecurity strategies of the EU member countries and look for contexts in which the term public administration is used. The strategies which are written in English are analyzed in detail in terms of their cybersecurity strategy objectives. The data used are taken from the ENISA database [35]. A descriptive statistics is used for the quantitative analysis of the indices (PL, DL and GCI) and the document analysis (e.g., the adoption occurrence and objectives of cybersecurity strategies of individual EU

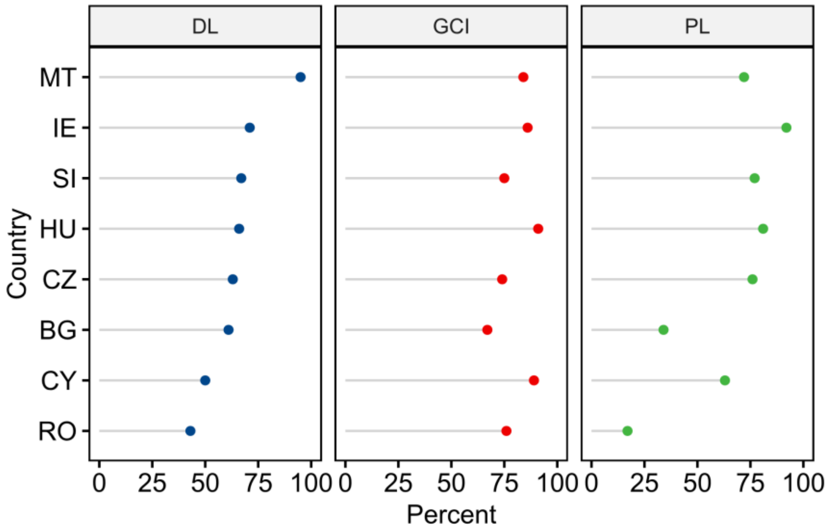

Figure 2. Chart diagram showing the DL, GCI and PL indices of the countries, with the below-average GCI values (the total average is 91.26%). Instead of a full list of the country names, abbreviations according to the ISO codes are used. DL is the level of digitalization, GCI is the global cybersecurity index and PL is the level of penetration. The data are arranged in a descending order of DL.

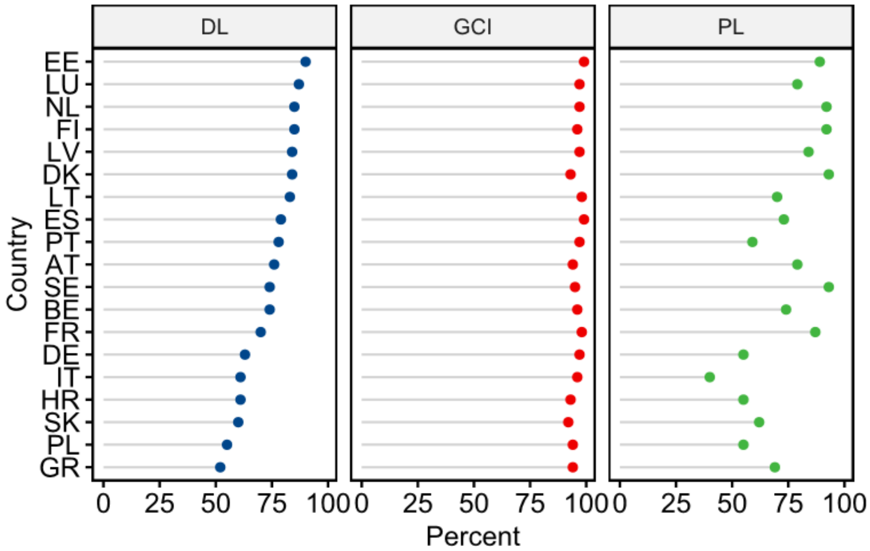

Figure 3. Chart diagram showing the DL, GCI and PL indices of the countries, with the above-average GCI values (the total average is 91.26%). Instead of the a list of country names, abbreviations according to the ISO codes are used. DL is the level of digitalization, GCI is the global cybersecurity index and PL is the level of penetration. The data are arranged in descending order of DL.

member states). The collected data are analyzed and visualized using the R programming statistical software. We use R (version 4.3.1) and the software RStudio (version 2022.07.1 - "Spotted Wakerobin" release). The results of the analysis are presented below.

First, we want to answer the question how often the EU member countries update their strategies. According to Subban and Jarbandhan [19], the frequency of the document releases is one of the four indicators of a good governance. The others are an accountability, predictability and participation. Transparency is also an important aspect of an effective cybersecurity governance. A higher number of releases may indicate a greater transparency which promotes the stakeholder trust and allows for a better scrutiny of the cybersecurity efforts. Comparing the cybersecurity strategies by quantifying the document releases provides a valuable framework for a comparative analysis. Moreover, by examining variations in the document releases, researchers and policymakers can identify trends, assess progress, and learn from countries with more comprehensive strategies.

Figure 1 shows that eight EU countries have only the first release of the strategy, ten countries have the second and nine countries the third release. The Scandinavian countries are interesting in terms of RQ1. Finland, for

example, is a country that has only one release of the strategy. It took place in 2013. Denmark has three releases of its strategy. The first took place in 2015 and the last in 2022. On average, Denmark releases a new strategy every three years. Sweden, too, has only one release of its strategy. It took place in 2017. Our comparison between countries with below-average (Figure 2) and above-average (Figure 3) GCI shows that countries with a below-average GCI released the first version of their strategy on average two years later than the countries with an above-average GCI.

Figure 2 shows a dot chart diagram presenting the DL, GCI and PL indices over countries with the below-average GCI values (x_{below} = 80.25%, μ = 91.26%). It is interesting to note that Romania and Bulgaria are the countries with the lowest average level of PL and at the same time with the lowest level of GCI. In this context, the fact that Romania is one of the few countries whose national cybersecurity strategy covers almost all 21 objectives is particularly interesting (see Table 1). We would however expect GCI to be higher as it covers all the essential aspects of the cybersecurity management. However, we cannot comment on the strategy content as it is not available in the English language. Since the strategies are of a long-term character, we may not expect their new releases on a short-term basis. Moreover, an interesting observation is that none of the countries that fall below the GCI average has three releases of their strategy, they have just one (i.e., BG, IE, MT and SI) or at most two (CY, CZ, HU and RO).

Figure 3 shows a dot chart diagram presenting the DL, GCI and PL indices for the countries with the above-average GCI values (x_above = 95.89%, μ = 91.26%). Here, some interesting differences between the countries are less noticeable. For example, there is a divergence noted in how the targets are addressed in the strategies. For example, Croatia and the Netherlands have in their cybersecurity strategies only seven objectives, while they achieve an above-average GCI. A similar case are Germany and Latvia. They cover only nine objectives but achieve an above-average GCI. Also interesting is that the median number of the objectives of the countries with an above-average GCI is 12, while in the countries with a below-average GCI it is 14. We would expect that the

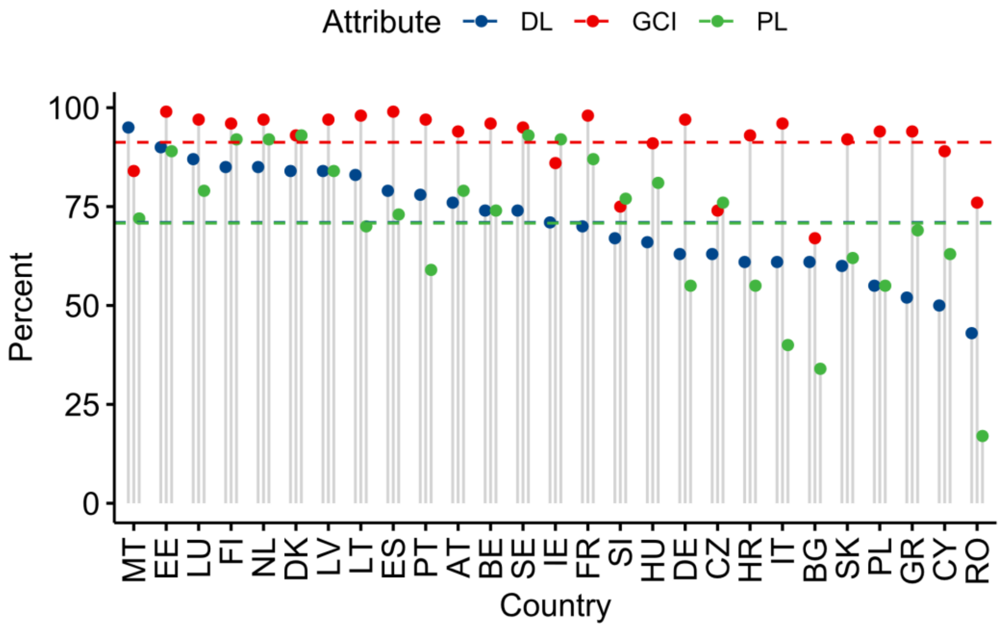

Figure 4. Lollipop diagram with an aggregate display of all the 27 EU countries. The red dashed line shows the average GCI. The green dashed line shows the average PL. The blue dashed line (DL average) is not visible as it is overlapped by PL. Instead of the full list of country names, abbreviations according to the ISO codes are shown (as in Table 1). DL is the level of digitalization, GCI is the global cybersecurity index and PL is the level of penetration. The data are arranged in a descending order of DL.

countries addressing more objectives would achieve a higher GCI, which cannot be determined by comparing the medians. Among the mentioned countries, it is only Germany that often addresses "public administration" in its strategy.

Figure 4 presents a lollipop diagram of the aggregated DL, GCI and PL. It shows the countries that are below/above the average in terms of DL, GCI and PL. The countries are in a descending order according to DL. The ideal state is the one that stands out from the average of all the indices (above the dashed lines). As seen, one of the interesting outliers is Malta. It has the highest score of DL, but below the average in terms of GCI compared to the other countries. The most marked decline is in the countries following Sweden. Speaking in terms of DL, and the divergence in terms of PL and GCI, there is no pattern indicating some general conclusions. It seems that each country is unique and that many factors need to be considered when assessing the cybersecurity and that the indices alone are insufficient. This finding is in some way not surprising as the cybersecurity is a broad concept [36] involving numerous variables. Malta [37], for example, does not address the public administration in its strategy while the Swedish cybersecurity strategy [38] points out that the stakeholders whose cybersecurity is inferior, thus likely to jeopardize the security of others, particularly the public administration, specifically when sharing sensitive information within the public administration. Also, they promote the development of the national framework for systematic cybersecurity efforts to enable a more effective monitoring of the cybersecurity efforts in the public administration.

4 Comparing the EU strategies and their implications on the public administration

Table 1 summarizes our comparison of the cybersecurity strategies of the EU member countries. The countries that address most of the objectives (over 19) are: Italy, the Czech Republic, Greece, Romania and Slovakia. The countries with the fewest objectives are also of a particular interest (top three countries with the least exposed objectives). These countries are Malta, Croatia and the Netherlands.

Below we describe some findings related to the occurrence of the notion of the public administration in the national cybersecurity strategies. The Greek, Romanian, Lithuanian, and Finnish strategies do not even mention the concept of the public administration in their strategies. On the contrary, Austria, Belgium and Portugal use the term public administration, but no specific treatment can be identified in their strategies. The Danish strategy [39] is also specific. It does not use the "public administration« but uses the term "public authorities”. The same applies to the French strategy. The Irish strategy [40] is specific in this respect as it uses many terms such as the "public authority", "public sector" and also "public services". However, the Irish strategy find the public sector data particularly important, e.g., for electoral processes and military infrastructure, so it is important to ensure the security of both processes and the infrastructure. Ireland is particularly vulnerable. According to their strategy [40], more than 30% of all the data in the EU is hosted in Ireland. A somehow a worrying fact is that judging by GCI, Ireland is below the EU average. The Luxembourg strategy addresses besides "public sector" and "public service", also the “public body”. It claims that the public body should issue the cybersecurity certificates compliable with the European cybersecurity certification scheme. It is not clear, however, whether this concerns the public administration in general or only the small-and medium-sized enterprises.

For example, the Czech strategy addresses the role of civil servants to make public administration more resilient to cyber threats [41]. Similarly, the Slovakian strategy assumes that recruitment and development of the staff possessing the related competencies are important to ensure the information security objectives [42]. The Italian strategy [43] emphasizes that establishing robust cybersecurity capabilities within the Public Administration is of a paramount importance in securing a successful national digital transition. This critical step is instrumental in safeguarding the integrity and confidentiality of the citizens data and services at the highest security level. Estonia, as a country with a highly digitized public administration, proposes in its strategy [44] to integrate different sectors (e.g., private sector, science and technology) for being crucial in achieving the cybersecurity. The Polish strategy [45] finds it important to standardize and lay down the requirements in terms of the cybersecurity, as their development is beneficial for the private sector or citizens. The Spanish strategy [46] is one of the few that addresses the artificial intelligence in connection with the public administration and finds the new technology to have already become part of the everyday life. The Hungarian strategy [47] sees the necessity to ensure a safe and reliable environment for the public administration while promoting the innovative and cutting-edge development of public services. However, this record appears in the 2013 version. The new version (2018) is not available in English.

Germany [48] in its 2030 Network Strategy addresses the importance of the security requirements. Germany is thus the only country among mentioned countries to realize the importance of the public administration protection. Other countries which also address the public administration do not give it as much importance as Germany. The Croatian strategy [49] only proposes the "State School for Public Administration" and some other institutions to be connected to universities without argumenting. The Dutch strategy [50] addresses the public administration as part of the public-private partnership. One of its important tasks is the measure of a special act (Digital Government Act), which also deals with the information security in the public administration. The Latvian strategy [51] explains how their salary reform in the public administration assures positive results as it provides competitiveness and better payment for the hired cybersecurity experts. The Slovak strategy [42] takes similar steps except that it only emphasizes the importance of motivational and reward tools for professionals in the public administration which indirectly implies that there is a gap between the conditions of the public administration and the private sector. Following the above, the most important aspects may be the provision of competitive working conditions (i.e., the salary or financing in general). Italy is also aware of the financial aspect and highlights [43] its plan to improve the cyber resilience of the public administration and the financial contribution.

In the future, special attention and support must be paid to organizations that manage the cybersecurity in countries with the lowest GCI scores (e.g., Bulgaria, the Czech Republic and Slovenia). Even though the Czech strategy [41] addresses many objectives, it achieves one of the lowest GCIs in the EU. Of course, one has to take into account that the strategy was implemented in 2021 and the results are not yet to be seen. In the Czech strategy, the importance of the digitalization of the public administration and the concern for its resilience is very clearly highlighted as a stand-alone subsection. The Bulgarian strategy is not studied for not being available in the English language. Interestingly, the Slovenian strategy [52] addresses "SIGOV-CERT" as an independent response center for its public administration information systems. Specialized CERTs for the public administration sector are likely to provide an added value in terms of the priority treatment and personalized support. Since the information systems supporting the public administration are generally specific as they may be part of the critical infrastructure (e.g., hospital information systems, taxation information systems, etc.).

Table 1: EU cybersecurity strategies objectives. Countries are shown on the X-axis. Objectives are shown on the Y-axis. The green color at the top of the table represents countries that achieve an above-average GCI. The red color represents the countries that are below the average.

Country (code):	AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	GR	HU	IE	IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE
Cybersecurity strategy objective																											
Address cyber crime	X	X	X	X	X	X	X	X	X	X	X	X	▨	▨	X	X	X	X	X	X	X	X	X	X	X	X	X
Adopt Information Security Standards	▨	▨	▨	▨	X	X	▨	X	▨	▨	▨	X	▨	X	X	▨	X	▨	▨	▨	▨	▨	X	X	▨	▨	▨
Balance security with privacy	▨	▨	X	X	X	X	▨	X	X	X	▨	X	▨	X	X	X	▨	▨	▨	▨	▨	X	X	X	X	X	X
Critical Information Infrastructure Protection	X	X	▨	▨	X	X	X	X	X	X	X	X	X	X	X	X	X	X	▨	X	X	X	X	X	X	X	X
Citizen awareness	▨	X	X	▨	X	X	X	X	X	X	X	X	▨	X	X	X	X	X	X	▨	X	X	X	X	X	X	X
Develop national cyber contingency plans	X	▨	▨	▨	X	X	X	X	X	X	X	X	X	X	X	X	X	X	▨	▨	X	▨	X	X	▨	X	X
Engage in international cooperation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Establish a public-private partnership	X	X	▨	▨	X	X	▨	X	X	▨	▨	X	▨	X	X	▨	X	X	▨	X	X	▨	X	X	▨	X	X
Establish an incident response capability	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	▨
Establish an institutionalised form of cooperation between public agencies	X	X	▨	▨	X	X	▨	X	▨	X	X	X	X	X	X	▨	▨	X	▨	▨	X	X	X	X	X	X	X
Establish and implement policies and regulation capabilities	▨	▨	▨	▨	X	X	▨	▨	▨	▨	▨	X	▨	X	X	▨	X	▨	▨	▨	▨	▨	X	X	▨	▨	▨
Establish baseline security requirements	X	▨	▨	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	▨	X	X	X	X	X	▨	X	▨
Establish incident reporting mechanisms	X	X	X	X	X	X	X	X	X	X	▨	X	X	X	X	▨	▨	X	X	▨	X	X	X	X	X	X	▨
Establish trusted information-sharing mechanisms	▨	▨	▨	▨	X	X	▨	X	▨	▨	▨	X	▨	X	X	▨	▨	▨	▨	▨	▨	▨	X	X	▨	▨	▨
Foster R&D	X	X	X	X	X	X	X	X	X	X	X	X	▨	X	X	▨	X	▨	▨	▨	X	X	X	X	▨	X	X
Organise cyber security exercises	X	X	▨	▨	X	X	X	X	X	X	▨	X	X	X	X	▨	X	X	▨	▨	X	X	X	X	X	X	X
Provide incentives for the private sector to invest in security measures	▨	▨	▨	▨	X		▨	▨	X	▨	▨	X	▨	X	X	▨	▨	▨	▨	▨	▨	▨	X	X	▨	X	▨
Risk assessment approach	▨	▨	▨	▨	X	X	▨	X	▨	▨	▨	X	▨	X	X	▨	X	▨	▨	▨	▨	▨	X	X	▨	▨	▨
Set a clear governance structure	▨	▨	▨	▨	X	X	▨	▨	▨	▨	▨	X	▨	X	X	▨	▨	▨	▨	▨	▨	▨	▨	X	▨	▨	▨
Strengthen training and educational programmes	X	X	X	▨	X	X	X	X	X	X	▨	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	▨
Improve the cybersecurity of the supply chain	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	X	▨	▨	▨	▨	▨	▨	▨	X	▨	▨	▨	▨
Count:	12	11	8	7	20	19	11	17	14	13	9	20	9	19	21	9	14	12	6	7	13	12	20	20	10	15	10
English language	X	X	▨	X	▨	X	X	X	X	X	X	▨	X*	X	X	X	X	X	X	X	X	X	▨	X	X	X	X

Note: ISO 3166 (alpha-2 code) codes are used for country representation (available here: https://www.iso.org/obp/ui/#search), X indicates Yes, and grey color indicates No.

5 Discussion

Considering that eight EU member countries have one release, ten countries two releases, and nine countries three releases of their cybersecurity strategy means that on average they have two releases of their national of cybersecurity strategy.

This answers *RQ1* (*how often do the EU countries release/update their cybersecurity strategy?*).

Speaking in terms of the frequency of releases, we can observe that the cybersecurity strategy in the EU countries remains in force for five years (median value). One of the interesting observations is that none of the countries below the average of each of the three indices GCI, DL and PL (these are: RO, CY and BG) or below the average of GCI and at the same time above the average of PL and/or DL (these are the countries: MT, IE, HU, SI and CZ) have more than two releases of their cybersecurity strategy. This observation may suggest that countries with the above average GCI scores tend to have more cybersecurity strategy releases compared to the countries with lower average GCI scores. Specifically, countries with the above-average GCI scores tend to have more than two cybersecurity strategy releases, while the below-average countries typically have either one or two releases. This somehow suggests a positive correlation between the country's cybersecurity preparedness, as reflected in their GCI score, and the frequency of releasing their cybersecurity strategy. On one hand, the countries with higher GCI scores may be more proactive in addressing the cybersecurity challenges, as reflected in the higher number of the cybersecurity strategy releases. They are likely to recognize the importance of a continuous updating and improving their response to the evolving cyber threats. On the other hand, the countries with lower GCI scores may be relatively less proactive in addressing the cybersecurity issues, leading to a smaller number of their strategy releases. This might indicate that these countries could improve their cybersecurity policies and practices. It is important to note that there are exceptions where some countries with the above-average GCI scores still have less than three cybersecurity strategy releases (i.e., FI, ES, AT, BE, SE, LT, PT, FR, HR and GR). This may be due to many factors, such as differences in the government structures, availability of resources, or other national priorities that affect the development and release of the cybersecurity strategies.

Overall, the findings highlight the importance of a robust cybersecurity strategy and the need for a continuous effort to adapt and strengthen the cybersecurity measures in response to the evolving threat landscape. Policymakers and stakeholders in the countries with lower GCI scores may use this information to compare their strategies with those of the better-performing countries and identify opportunities to improve their cybersecurity preparedness.

To answer RQ2, we analyzed DL and PL of all the 27 EU member countries. 16 countries achieve an above-average PL and 11 countries achieve below-average PL (total average of all the 27 EU countries = 70.81 %). Moreover, 13 countries achieve an above-average DL and 14 countries achieve a below-average DL (the total average of all the 27 EU countries is 71.00 %).

This answers RQ2 (*what is the state of digitalization and the extent of using government services in the EU countries?*)

To answer RQ3, we analyze GCI of each of the 27 EU member countries. Eight EU countries achieve a below-average GCI and 19 EU countries achieve an above-average GCI (the total average of all the 27 EU countries is 91.26 %). It can be concluded that slightly more than a third of the EU member countries do not meet the GCI average. Nevertheless, it can be observed that the situation is satisfactory since most countries are above the average.

This answers RQ3 (*what is the state of the cybersecurity in the EU countries?*)

Based on the data (both on DL and PL), it cannot be argued that the degree of digitalization is related to GCI. For example, ten EU countries achieve the above-average values for PL, DL and GCI (EE, LU, FI, NL, DK, LV, ES, AT, BE and SE). But there are also countries that achieve an above-average GCI and at the same time a below-average PL and/or DL (there are nine such countries, i.e. LT, PT, FR, DE, HR, IT, SK, PL and GR). However, there are also five countries that achieve an above-average PL and/or DL and a below-average GCI (MT, IE, HU, SI and CZ). Three countries achieve below-average values for PL, DL and GCI (RO, CY and BG). We would expect that this kind of the difference is more obvious, because we may speculate that the more digitalization there is, the more cybersecurity risks there are. Indirectly, this thesis can also be seen in the literature, as there are some academic efforts that find that countries with a better technological and ICT infrastructure are more likely to be targets of attacks. They also find that countries with a higher gross domestic product (GDP) per capita are more likely to be targets of cybercrime attacks [31]. However, our study does not show a clear connection between the fact that countries that are more digitalized and that have highly digitalized public administration services achieve higher/lower levels of the cybersecurity. Based on the analyzed data, it is not evident that the cybersecurity level may be attributed to DL or PL.

This answers RQ4 (*can the high level of the cybersecurity in the EU countries be attributed to the extent of digitalization and government service utilization*?).

6 CONCLUSION

The paper examines 27 EU member countries in terms of their cybersecurity strategies and indices such as GCI, DL and PL. A particular attention is paid to the public administration, as this type of the sector is particularly vulnerable to cyberattacks. By looking at the DL, PL and GCI indices simultaneously and examining cybersecurity strategies, we shed light on a new analytical angle. Our study provides the following contributions:

- Firstly, examining the cybersecurity strategies in the 27 EU countries offers an insight into the different approaches used to combat the cyber threats. Each country operates in a unique socio-political context, resulting in different strategies and priorities. By examining this diversity, researchers and policymakers gain a broader perspective that allows for the identification of innovative ideas and alternative solutions that could be applicable in different contexts.

- Secondly, our study contributes to understanding of the cybersecurity practices and enables a mutual exchange of ideas and the development of a comprehensive understanding of the EU cybersecurity strategies. The EU consists of 27 member countries with carious degrees of digitalization, cybersecurity maturity and internet use by individuals when interacting with public authorities. The study of the EU cybersecurity strategies also highlights the opportunities for regional cooperation within the EU. Cooperation and knowledge sharing between the EU countries promote the exchange of best practices, sharing of threat intelligence and coordinated response mechanisms. A comprehensive study of these strategies can identify successful cooperation initiatives and foster cross-border partnerships that strengthen cybersecurity defenses on regional and global levels.

- Thirdly, the analysis of the indices such as GCI, DL and PL can facilitate cooperation between the EU countries to share best practices and threat intelligence and to strengthen joint efforts to combat cyber threats and attacks.

- Fourthly, by comparing the numbers of the cybersecurity strategy releases, we can quickly grasp the scope and extent of each country effort in formulating and publicizing their cybersecurity strategies. Thus, a visual representation can make a complex information more accessible and appealing, and it also allows for transparency and comparative benchmarking between the EU countries.

As with any study, there are some limitations and opportunities for improvement in our study that the reader should consider. In analyzing and interpreting the data, we have relied on the composite indices. This may be a limitation as it does not necessarily provide a clear insight into the studied situation. For example, DL consists of four sub-categories (i.e., user-centricity, transparency, key enablers and cross-border services) (The European Commission, 2022). Similarly, GCI is also a composite index. For future studies, it may be useful to focus on individual aspects that make up GCI (e.g., legal measures, technical measures, organizational measures, capacity development and cooperative measures). In this way, we could get an additional aspect of where countries are ahead or behind compared to the EU average. Most of the research was conducted in the first half of 2023. This means that countries may have issued new strategies during this time.

ACKNOWLEDGMENTS

The authors would like to thank the President of the World Federation of Scientists, Prof. Antonino Zichichi, for awarding a scholarship to support the completion of the author's doctoral studies (Damjan Fujs). The authors would also like to thank the anonymous reviewers for their insightful comments which have helped them to improve the study.

DISCLOSURE STATEMENT

The authors report no potential conflict of interest.

FUNDING

This work was supported by the Slovenian Research and Innovation Agency (ARIS) under the Grant number P2-0426.

REFERENCES

[1] ENISA, ‘ENISA Threat Landscape 2022’, European Union Agency for Cybersecurity. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[2] F. Schlackl, N. Link, and H. Hoehle, ‘Antecedents and consequences of data breaches: A systematic review’, *Information and Management*, vol. 59, no. 4, p. 103638, 2022, doi: 10.1016/j.im.2022.103638.

[3] S. Backman, ‘Risk vs. threat-based cybersecurity: the case of the EU’, *European Security*, vol. 32, no. 1, pp. 85–103, 2023, doi: 10.1080/09662839.2022.2069464.

[4] J. Rees, S. Bandyopadhyay, and E. H. Spafford, ‘PFIRES: A Policy Framework for Information Security’, *Commun ACM*, vol. 46, no. 7, pp. 101–106, 2003.

[5] CR-T, ‘When is it Time to Update Your Cybersecurity Policy?’, CR-T: Calculated Research and Technology. [Online]. Available: https://www.cr-t.com/blog/when-is-it-time-to-update-your-cybersecurity-policy/

[6] A. Ahmad, S. B. Maynard, and S. Park, ‘Information security strategies: towards an organizational multi-strategy perspective’, *J Intell Manuf*, vol. 25, no. 2, pp. 357–370, Apr. 2014, doi: 10.1007/s10845-012-0683-0.

[7] M. Gercke, ‘Cybersecurity Strategy’, *Computer Law Review International*, vol. 14, no. 5, pp. 136–142, Jan. 2013, doi: 10.9785/ovs-cri-2013-136.

[8] L. K. Ilves, T. J. Evans, F. J. Cilluffo, and A. Alec, ‘European Union and NATO Global Cybersecurity Challenges: A Way Forward’, *Prism*, vol. 6, no. 2, pp. 126–141, 2016.

[9] The European Commission, *eGovernment Benchmark 2022 Background Report: Synchronising Digital Governments*, 1st editio. Luxembourg: Publications Office of the European Union, 2022. doi: 10.2759/204448.

[10] F. Romanovská and T. Pitner, ‘Multi-Level Cybersecurity Governance Frameworks for Public Administration’, *IDIMT 2022 - Digitalization of Society, Business and Management in a Pandemic: 30th Interdisciplinary Information Management Talks*, pp. 277–284, 2022, doi: 10.35011/IDIMT-2022-277.

[11] L. Coppolino, S. D’Antonio, G. Mazzeo, L. Romano, and L. Sgaglione, ‘How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project’, in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, IEEE, May 2018, pp. 573–578. doi: 10.1109/WAINA.2018.00147.

[12] D. Štitilis, P. Pakutinskas, and I. Malinauskaitė, ‘EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis’, *Security Journal*, vol. 30, no. 4, pp. 1151–1168, Oct. 2017, doi: 10.1057/s41284-016-0083-9.

[13] European Commission, ‘Joint Communication to the European Parliament and the Council: The EU’s Cybersecurity Strategy for the Digital Decade’, *Join(2020)*, pp. 1–28, 2020.

[14] German Presidency of the Council of the EU, ‘Berlin Declaration on Digital Society and Value-Based Digital Government’. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

[15] ENISA, ‘National Cybersecurity Strategies’. Accessed: Jul. 07, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[16] M. Górka, ‘The cybersecurity strategy of the visegrad group countries’, *Politics in Central Europe*, vol. 14, no. 2, pp. 75–98, 2018, doi: 10.2478/pce-2018-0010.

[17] A. Jacuch, ‘Comparative Analysis of Cybersecurity Strategies.European Union Strategy and Policies. Polish and Selected Countries Strategies’, *Online Journal Modelling the New Europe*, no. 37, pp. 102–120, 2021, doi: 10.24193/OJMNE.2021.37.06.

[18] A. Ubowska and T. Królikowski, ‘Building a cybersecurity culture of public administration system in Poland’, *Procedia Comput Sci*, vol. 207, pp. 1242–1250, 2022, doi: 10.1016/j.procs.2022.09.180.

[19] M. Subban and V. Jarbandhan, ‘Good Governance Perspectives in Public Administration and Cybersecurity’, *Administratio Publica*, vol. 27, no. 4, pp. 134–157, 2019.

[20] Y. Yanakiev and D. Polimirova, ‘Exploring the Role of the Human Factor in Cybersecurity : Results from an Expert Survey in Bulgaria’, *Journal of Information & Security*, vol. 44, pp. 39–50, 2020.

[21] V. Nagy-Takács and L. Berényi, ‘Information Security Management System Standards in Hungarian Public Administration’, *ACM International Conference Proceeding Series*, pp. 112–117, 2022, doi: 10.1145/3551504.3551554.

[22] M. Alvarez-Rodriguez, V. Kalogirou, F. Chiarelli, A. Crahay, N. Custers, and E. Miscenà, ‘National and sub-national approaches towards the creation of an interoperability framework – the case of Spain’, in *Proceedings of the 24th Annual International Conference on Digital Government Research*, New York, NY, USA: ACM, Jul. 2023, pp. 388–394. doi: 10.1145/3598469.3598513.

[23] A. Crahay *et al.*, ‘The Berlin Declaration monitoring mechanism’, in *15th International Conference on Theory and Practice of Electronic Governance*, New York, NY, USA: ACM, Oct. 2022, pp. 325–330. doi: 10.1145/3560107.3560305.

[24] L. Maglaras, G. Drivas, N. Chouliaras, E. Boiten, C. Lambrinoudakis, and S. Ioannidis, ‘Cybersecurity in the Era of Digital Transformation: The case of Greece’, *2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020*, no. September 2017, pp. 0–4, 2020, doi: 10.1109/ITIA50152.2020.9312297.

[25] L. Marti and R. Puertas, ‘Analysis of European competitiveness based on its innovative capacity and digitalization level’, *Technol Soc*, vol. 72, no. October 2022, p. 102206, 2023, doi: 10.1016/j.techsoc.2023.102206.

[26] K. Dubey, S. C. Sharma, and M. Kumar, ‘A Secure IoT Applications Allocation Framework for Integrated Fog-Cloud Environment’, *J Grid Comput*, vol. 20, no. 1, 2022, doi: 10.1007/s10723-021-09591-x.

[27] H. Liu, Z. Liu, D. Sun, and Y. Liu, ‘Python Java joint implementation of internet-based public opinion information collection’, *Soft comput*, vol. 5, no. Pavan 2017, Jun. 2023, doi: 10.1007/s00500-023-08652-5.

[28] International Telecommunication Union, ‘Global Cybersecurity Index 2020: Measuring commitment to cybersecurity’, Geneva, Switzerland, 2021.

[29] M. Koniagina, D. Belotserkovich, L. Vorona-Slivinskaya, and N. Pronkin, ‘Measures to Ensure

Cybersecurity and Regulation of the Internet of Things in the Russian Federation: Effectiveness Assessment', *J Econ Issues*, vol. 57, no. 1, pp. 257–274, Jan. 2023, doi: 10.1080/00213624.2023.2170136.

[30] R. Bruggemann, P. Koppatz, M. Scholl, and R. Schuktomow, 'Global Cybersecurity Index (GCI) and the Role of its 5 Pillars', *Soc Indic Res*, vol. 159, no. 1, pp. 125–143, 2022, doi: 10.1007/s11205-021-02739-y.

[31] S. Chen *et al.*, 'Exploring the global geography of cybercrime and its driving forces', *Humanit Soc Sci Commun*, vol. 10, no. 1, p. 71, Feb. 2023, doi: 10.1057/s41599-023-01560-x.

[32] A. Onumo, A. Cullen, and I. Ullah-Awan, 'An Empirical Study of Cultural Dimensions and Cybersecurity Development', in *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, IEEE, Aug. 2017, pp. 70–76. doi: 10.1109/FiCloud.2017.41.

[33] M. Nehrey, I. Voronenko, and A.-B. M. Salem, 'Cybersecurity Assessment: World and Ukrainian Experience', in *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)*, IEEE, Sep. 2022, pp. 335–340. doi: 10.1109/ACIT54803.2022.9913081.

[34] S. Terrell, 'Mixed-Methods Research Methodologies', *The Qualitative Report*, vol. 17, no. 1, pp. 254–280, Jan. 2015, doi: 10.46743/2160-3715/2012.1819.

[35] ENISA, 'National Cyber Security Strategies - Interactive Map'. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

[36] M. Sexton, 'U.K. cybersecurity strategy and active cyber defence – issues and risks', *Journal of Cyber Policy*, vol. 1, no. 2, pp. 222–242, Jul. 2016, doi: 10.1080/23738871.2016.1243140.

[37] MITA, 'Malta Cyber Security Strategy 2016', Valletta, Malta, 2016. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta

[38] GOS, 'A national cyber security strategy: Skr. 2016/17:213', Stockholm, Sweden, 2016.

[39] DIGST, 'The Danish National Strategy for Cyber and Information Security', Copenhagen, Denmark, 2021.

[40] GOVIE, 'National Cyber Security Strategy: 2019-2024', Dublin, Ireland, 2019. Accessed: Oct. 12, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Ireland

[41] NUKIB, 'National Cyber Security Strategy of The Czech Republic', Prague, Czech Republic, 2021. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Czech%20Republic

[42] NBU, 'The National Cybersecurity strategy 2021 - 2025', Bratislava, Slovakia, 2021. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Slovakia

[43] ACN, 'National Cybersecurity Strategy: 2022 - 2026', Rome, Italy, 2022. Accessed: Oct. 12, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Italy

[44] MKM, 'Cybersecurity Strategy: Republic of Estonia', Tallinn, Estonia, 2019. Accessed: Oct. 12, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

[45] MC, 'Cybersecurity Strategy of the Republic of Poland for 2019 - 2024', Warsaw, Poland, 2019. Accessed: Oct. 12, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Poland

[46] DSN, 'National Cybersecurity Strategy', Madrid, Spain, 2019. Accessed: Oct. 13, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Spain

[47] HUGOV, 'National Cyber Security Strategy of Hungary', Budapest, Hungary, 2013.

[48] BMI, 'Cyber Security Strategy for Germany 2021', Berlin, Germany, 2021. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

[49] MUP, 'The national cyber security strategy of the republic of Croatia', Zagreb, Croatia, 2015. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Croatia

[50] NCTV, 'National Cyber Security Agenda: A cyber secure Netherlands', Amsterdam, Netherlands, 2018. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Netherlands

[51] MOD, 'The Cybersecurity Strategy of Latvia 2023-2026', Riga, Latvia, 2023. Accessed: Oct. 11, 2023. [Online]. Available: https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf

[52] MJU, 'Cyber Security Strategy: Establishing a System to Ensure a High Level of Cyber Security', Ljubljana, Slovenia, 2016. Accessed: Oct. 11, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Slovenia

Damjan Fujs received his Ph.D. degree from the Faculty of Computer and Information Science, University of Ljubljana, Slovenia in 2024. He is a teaching assistant at the same university. His research interests include cybersecurity, security requirements engineering, software development methodologies and informatics. His work has been published in a range of scientific journals such as Computers & Security, Computers & Education, IEEE Access, Journal of Universal Computer Science, etc. Currently, he is or has been a member of the program committee of the Dnevi Slovenske Informatike (DSI 2021-2024), International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2021-2024), and European Interdisciplinary Cybersecurity Conference (EICC 2023, 2024). He is currently a member of the editorial board of the International Journal on Advances in Security.

Igor Bernik is a Professor of Information Security and Dean at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research interests include cybercrime, cyberwarfare, cybernetics, decision support systems, and information security. He is the author and co-author of numerous scientific papers published in renowned international journals and conferences, and the author of the book Cybercrime and Cyberwarfare, published in 2014 by Wiley.