Cybersecurity in the Republic of Moldova in the Context of European Integration

Ana-Maria Costea, Natalia Putină, Mircea Brie[1]

Abstract: *The current technological development has brought new opportunities, by reducing the time and transactional costs for several services. Thus, it has increased efficiency in various domains. Yet, at the same time, it has generated new threats and risks that countries need to face in the cyberspace. The unique character of this domain resides in the heterogeneity and multitude of the actors involved. This explains why there are unlimited possibilities for attacks, countless reasons for the attacks to happen, and endless strategies, which make a defence-based strategy futile, if not included within a larger resilience-based perspective. The conception of the state as the sole provider of services for the society no longer stands, as civil society and private actors gradually assume more responsibilities and competences, especially when dealing with the cybersecurity literacy of citizens. This aspect is key since we cannot truly discuss the resilience of a state – and tackle, ipso facto, its security – without taking into consideration the security of its citizens. In order to be protected against cyber threats, citizens need to identify them and find ways to address them. Thus, an adequate knowledge level is fundamental. The present article analyses the way in which the Republic of Moldova, an EU candidate state, is adhering to European norms and values regarding cyber resilience to cope with its cybersecurity threats. Firstly, we examine how its National Cybersecurity Strategy observes the European framework in terms of the state's and civil society's involvement in ensuring the security of the Republic of Moldova and of its citizens through awareness raising activities. Since one of the strategy's objectives is the cooperation with the civil society to increase the citizens' awareness of cyber threats, this research used a questionnaire designed to assess the Moldovan students' current level of knowledge of the cyber landscape and of the relevant European norms in this field. The questionnaire also aims to analyse if and how the Moldovan citizens benefited from the different measures taken by the state, the civil society, or other private actors to address this issue.*

Keywords: *Awareness, civil society, cybersecurity, the EU, Moldova, resilience.*

[1]**Ana-Maria Costea**, PhD, is Associate Professor at the National University of Political Studies and Public Administration (SNSPA), Department of International Relations and European Integration (DRIIE), Romania.
E-mail: anamaria.costea@dri.snspa.ro.
Natalia Putină, PhD, Associate Professor at the Moldova State University, Department of Political and Administrative Sciences, Vice-Dean of Faculty of International Relations, Political and Administrative Sciences, Chișinău, Republic of Moldova.
E-mail: natalia.putina@usm.md.
Mircea Brie, PhD, Professor at the University of Oradea, Department of International Relations and European Studies and PhD supervisor at the Faculty of European Studies of the Babeș-Bolyai University (Romania).
E-mail: mbrie@uoradea.ro.

Introduction

The current technological development came with numerous opportunities for all the levels of the society. Nowadays information travels instantaneously, and production processes are automatic reducing the costs and time constraints, and thus generating higher financial profits. For states, digitalisation has meant not only smart bombs but also integrated fires and greater coordination in the field, thereby improving military capabilities. Additionally, the public institutions digitalised important features of their services to reduce their bureaucratic burden. The critical infrastructure sectors, such as energy, water, health, education, and finance, are all undergoing digitalisation and greater interconnectivity, while individuals have become critically dependent on digital capabilities to run their affairs.

The COVID-19 pandemic emphasised the need for deeper digitalisation, since the majority of the activities were transferred online (for example, education). All these benefits came with a cost, as the cyberspace poses countless threats to states and to individuals. Internationally, due to the pandemic and the fact that the majority of the activities have been carried out online, cybercrime has increased by up to 600%, being estimated to reach $6 trillion in damages in 2021, which represents 1% of the global GDP. The general trend and statistics show that, by 2025, cybercrimes will inflict costs of $10.5 trillion annually (Purplesec, 2024).

The cyber domain is a unique field in which the classical defence strategy does not work due to the wide array of motives behind cyber-attacks and the heterogeneity of the actors involved (states, and non-state actors like organised crime groups, hacktivists, terrorists, hacking groups, individual hackers). The motives range from economic ones – e.g., the case of *Wannacry* (Kaspersky) to political – e.g., *SolarWinds* (Jibilian, Canales, 2021), military – e.g., *Stuxnet* (Collins, McCombie, 2012, pp. 80-91), and social ones – e.g., the Anonymous attacks against Putin (Pitrelli, 2022). Some of the attackers are driven by the desire to acquire international status (Mills, 2012). Therefore, the most suitable policy to address these threats would be one based on a credible and resilient society. Empirically, in the EU, WannaCry was classified as being the result of negligence (ENISA, 2022). Thus, part of these attacks succeeds because the individuals are not aware of the cyberspace vulnerabilities and lack the necessary skills to protect themselves against cyber threats. As mentioned by the European Commission in 2017, "many Europeans still fail to take basic cybersecurity measures: many say they care a lot about their personal data, but then give them away for free on social networks. Data is striking: 90% of the data breaches reported by the 2017 Verizon Data Breach Investigation were the result of phishing" (ENISA, 2022, pg. 4). Hence, it would be practically impossible to have a resilience-based strategy without taking into consideration the citizens' awareness and their knowledge level of the cyber hygiene and the threat landscape. In this regard, the EU organises, among other initiatives that are to be analysed in the following chapters, the *European Cybersecurity Month*, an annual campaign – dedicated to cybersecurity awareness and best practices – during which the Member States, the civil society, and the education providers perform common activities to tackle the aforementioned security issues. But, beyond the EU Member States, are the candidate countries that prepare themselves to be integrated within the European framework. As the cyberspace is one of the most interconnected fields, their

resilience is crucial for the future security of the entire Union. Therefore, this article seeks to analyse the convergence between the Republic of Moldova's cybersecurity strategy and the European principles and activities in the cybersecurity field. Consequently, it will reveal how the Moldovan state is dealing with its citizens' lack of awareness and knowledge of the cyber field. Additionally, we will examine the current status-quo from an empirical point of view, by highlighting the Moldovan students' level of awareness of this issue and their views on the most suitable actors to act in this field: the state or the civil society. Hence, the research questions are:

Q1 - How is the Republic of Moldova integrating itself within the European framework from a strategic cybersecurity perspective?

Q2 - What is the level of knowledge among the Moldovan students regarding the European and national cyber threat landscapes and the ways to mitigate them?

Q3 - How should the Moldovan civil society involve itself in the cyber field?

From a methodological point of view, this article is structured in four sections aiming to answer the aforementioned questions. The first section is the introduction. The second section offers an overview of the existing literature on the concepts of 'resilience' and 'civil society' because a resilience-based strategy would be the most appropriate to deal with an ever-evolving security landscape. In the third section, we analyse the EU's strategies and activities related to the cyberspace and, more concretely, its ways of constructing a resilient European society through awareness campaigns, educational activities, and private-public partnerships. In the fourth one, we examine the Moldovan cybersecurity strategy to see if it follows the European principles and we analyse the concrete actions taken in this direction. We have conducted empirical research to evaluate the Moldovan students' level of awareness regarding the European and the national initiatives, as well as their knowledge of concepts such as 'cyber hygiene' and 'the security landscape of the online world'. In terms of research methods, for the first part of our paper we have used the document analysis instrument, as we have drawn upon a wide variety of strategic documents adopted at the EU level (e.g., European Commission reports on the results of the activities conducted under the framework of the *European Cybersecurity Month*) or in the Republic of Moldova. Additionally, statistical data was used to assess recent developments regarding internet coverage in the Republic of Moldova, and the citizens' awareness of online threats. Moreover, a questionnaire was sent to Moldovan students – enrolled in bachelor's (BA) and master's (MA) degree programmes – who specialise in international relations and/or public administration. Based on that survey, we provide a comprehensive overview of the Moldovan students' current awareness and knowledge level of the cyberspace and of the norms, initiatives, threats, and actors responsible for dealing with the vulnerabilities in this field. From a procedural point of view, the questionnaire was available online from December 2023 till January 2024, and 103 responses were generated.

Conceptual analysis. Literature review

Given the evolving security landscape, it is obvious that it would be practically impossible to employ classical defence strategies in the cyberspace. Firstly, there is a multitude of actors involved in the cyberspace, and they use a very wide spectrum of

strategies. As mentioned before, the cyber actors can be driven by economic, political, military-strategic, social, or irrational motives. Secondly, the accountability in the cyberspace is among the most difficult elements to address. Thirdly, the technology is developing at an incredible speed, making it difficult to establish a defence policy against shifting threats. Lastly, in terms of costs, a large-scale cyberattack is not necessarily expensive. That is why the number of potential attackers is higher than in the case of classical physical large-scale military attacks (Costea, 2023, pp. 111-127). It would therefore be counterproductive to defend yourself against a threat that is changing by the minute. Consequently, states need to develop resilient systems. One of the first definitions of 'resilience' was produced in the '70s by Holling, who saw it as a measure to absorb changes and disturbances, while maintaining unaltered the relationship between the state's institutions and the population (Holling, 1973). Although the concept is not new, it gained momentum in 2010, when several states (e.g., Canada) developed security strategies for the resilience of their systems and/or of their society (Svitkováa, 2017, pp. 24-26). Walker and Salt (2012, pg. 3) refer to resilience as being a system's capacity to continuously evolve and adapt to deviations, while preserving its core functions and structure. The EU is defining it as "the ability not only to withstand and cope with challenges but also to undergo transitions, in a sustainable, fair, and democratic manner" (European Commission. EU Science Hub). For a system to do that, we need to consider more than the management level (in this case, the states). The concept of resilience sparks debates about the monopoly that states tend to have over security matters as security providers for their citizens. Since we can have financial, economic, social, environmental, industrial, or terrorist incidents, the state cannot be the only one that responds to security threats (Fjäder, 2014). In fact, resilience refers to the "strong social compact between the state and society on their respective and mutual roles and responsibilities" (Metre, 2016, pg. 1). In the cyberspace, it is even more crucial to involve non-state actors, since the systems are so interconnected. As mentioned earlier, one of the biggest cyberattacks in our modern era was *WannaCry* and its success was due not only to the negligence (ENISA, 2022) of the states, but also of the critical infrastructure operators and of individuals. Thus, it is vital to develop a resilient society in which private actors and individuals do their due diligence. To this end, each state should seek, together with the civil society and private actors, to increase the citizens' level of awareness of the online dangers, as well as their ability to mitigate them. In this framework, the civil society organisations (CSOs) become essential actors in the democratisation process, as they are the main partners of the public authorities (Mărcuț, Chiriac 2023, pg. 264; Polgár, 2023), especially when it comes to conducting awareness raising campaigns. Without an active and independent civil society, we cannot have a democracy (Popovenciuc, 2022, pg. 26; Brie, Putină, 2023, pp. 172-174; Brie, Costea, Petrila, 2023, pp. 108-109). Hence, the civil society should be involved in relevant activities, including in conflict management (Brie, Horga, 2014, pp. 207-211) and international cooperation (Brie, 2021, pp. 10-16; Brie, Jusufi, Polgár, 2022, pp. 186-192), at all levels, from local and regional to national and international levels (Zakota, Nemeth, 2022; Brie, Mărcuț, Polgár, 2022, pg. 73; Brie, Jusufi, Polgár, 2023, pp. 58-60; Jusufi, Polgár, 2023, pp. 130-135).

The European Union's approach - norms, strategies and results

The EU is among the top international leaders in the cybersecurity domain. Strategically, it adopted in 2021 the 2030 Digital Compass: the European way for the Digital Decade (European Commission, 2021). In 2022, the level of internet connectivity within the EU was approximately 90%, as the gap between rural and urban areas had been decreasing significantly since 2007 (Statica, 2024). This high level of connectivity opened the door for equally high and diverse online threats. To mitigate the vulnerabilities of the digital infrastructures, the EU adopted its Strategic Compass for Security and Defence (2022) that reveals its strategic emphasis on the security of the entire Union. Among the top threats that the EU is facing, the European decision-makers have highlighted the threats that come from the cyber domain, and they have proposed the development of the EU Cyber Defence Policy (*A Strategic Compass for Security and Defence*, 2022). Additionally, in December 2022, the EU decision-makers adopted the NIS 2 Directive, a document "that aims to achieve a high common level of cybersecurity across the European Union" (*NIS 2 Directive*, 2022).

As regards resilience, in 2015 the EU took the first major step by organising the high-level conference called "Building a Resilient Europe in a Globalised World". In 2016 the Research Network for the Measurement of Resilience was established, and four years later "the 2020 Strategic Foresight Report announced resilience as a new compass for EU policies" (European Commission. EU Science Hub). Moreover, in 2022, the EU adopted its Cyber Resilience Act (European Commission, 2022). Among the issues that the EU has to deal with, we would like to emphasise the "insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner" (European Commission, 2022). This lack of understanding, awareness and cyber hygiene represent key elements in the EU's cybersecurity strategy (European Commission, 2020a). To mitigate this vulnerability and to reach a credible societal resilience, the EU has developed several strategies designed to increase its citizens' level of knowledge and awareness. One of these is the GDPR. This regulation is unique at the international level and it has made the EU a normative power in the cyber domain. In a nutshell, the main purpose of this piece of legislation is to protect the EU citizens against the way in which the private and the public authorities are using their data. Through the GDPR, an individual has access to their own data, can demand its erasure from the archives of the provider, and is informed on how their data is going to be used (Regulation (EU) 2016/679). At the empirical level, the new European Cybersecurity Competence Centre (ECCC) was developed to work together with a Network of National Coordination Centres (NCCs) in order to increase the cybersecurity level across the EU (ECCC, 2021).

From an institutional point of view, in 2019 the EU adopted the regulation that established the development of ENISA, the European Union Agency for Cybersecurity (ENISA, 2024). Among the activities that this agency is carrying out, we would like to highlight the European Cybersecurity Month (ECSM), an annual event that started in 2012 and is intended to promote awareness of the cybersecurity risks and threats and to provide solutions to vulnerabilities in the cyberspace. The target groups for these events are EU citizens, schools, and universities. The activities take the form of awareness raising campaigns and the sharing of good practices through

public-private partnerships (European Cybersecurity Month). The ECSM started by hosting pilot projects in less than half of the EU Member States, but in 2013, when the EU Cybersecurity Strategy (2013) was adopted, it called on all EU Member States to participate. It even went beyond the boundaries of the EU, having states like the Republic of Moldova participate and organise events under European umbrella. In 2021, the ECSM organised an event on the topic of thinking twice before clicking a specific website or attachment, for example. The target audience of the campaigns were the young people (21+ years old) since they spend a lot of time online and using social media platforms. In terms of tangible results, the campaign reached an audience of over 20 million people (over twice the 8.8 million figure reached in 2020). Additionally, more than 70% of the EU Member States consider that the campaigns had a positive impact, visible in the reduction of the cyber incidents (ENISA, 2021).

Through ENISA, the EU also engages in educational activities related to digital literacy. According to the Digital Education Action Plan for 2021-2027 (European Commission, 2020b), the second priority of the EU is to enhance the digital skills and competences all around the Union through educational programmes. Concretely, a report published by ENISA in December 2022 reveals that all EU Member States have developed educational activities for their citizens. The providers of such educational services include states like Romania (which involves governmental institutions in the process), Croatia (which implements them through the Ministry of Interior), Ireland, Finland and Estonia that develop partnerships with universities, or countries like France, Sweden and Malta that provide these training programmes through partnerships with the civil society (ENISA, 2022, pp. 9-21).

Thus, the EU is a very active party in the regional endeavours to raise the level of digital knowledge and people's awareness of cybersecurity issues. These activities are essential in creating a resilient society, since statistically "in 2022, 96% of young people in the EU made daily use of the internet, compared with 84% for the whole population" (Eurostat, 2023). In terms of digital skills, in 2021 "young people between the age of 16 and 29 report[ed] basic or above basic overall digital skills. Country shares range[d] from 93% in Finland, 92% in Malta, 89% in Croatia and 87% in Greece and the Netherlands to 49% and 46% in Bulgaria and Romania" (Eurostat, 2023).

Although the cybersecurity policy is not a supranational policy of the European Union, the Member States approach it in a concerted manner, adopting its principles and values, and developing a common ground. From this point of view, and considering that the cyberspace interconnects various domains, it is critical for EU's candidate states and partner countries to adopt the same approach. That is why we chose to analyse the Republic of Moldova's approach to the cyberspace, especially since the onset of the ongoing Ukrainian war, and in light of the cyber-attacks that occurred in the region.

The Republic of Moldova's approach - norms, strategies and results

In June 2022, the Republic of Moldova became a candidate state of the EU, and the accession negotiations officially started on June 25, 2024. Hence, it is important to know which is the status quo regarding the convergence of different Moldovan policies

and the European acquis. From a security perspective, the EU enlargement towards the East will bring crucial changes, as in the East the EU will have a large direct border with one of its strategic competitors, namely the Russian Federation. As far as cybersecurity is concerned, the Republic of Moldova adopted its first Information Security Strategy in November 2018 for the period of 2019-2024. According to it, an important factor that affects the national security of the country is represented by the general public's lack of awareness of the online risks, especially those related to misinformation campaigns (The Parliament of Moldova, 2018a, pg. 15). To tackle this issue, the Moldovan authorities proposed the development of the resilience capabilities and know-how of private and public authorities and individuals through awareness campaigns, trainings, exercises, simulations, and the development of new curricula in the field (The Parliament of Moldova, 2018a, pp. 20-21). Additionally, the strategy emphasises the importance of cooperation between the state and the civil society (The Parliament of Moldova, 2018a, pg. 22), the latter being seen as a necessary partner in raising the Moldovan citizens' level of awareness of the online threats and of the ways to mitigate them (The Parliament of Moldova, 2018b, pg. 27). Another strategic document is the Republic of Moldova's Digital Transformation Strategy 2023-2030. One foundational element of the Moldovan digital architecture is the idea that the general public needs to go through a process of digital literacy and competences development (The Government of the Republic of Moldova and the Ministry of Economic Development and Digitalization, pg. 6).

"Moldova is among the top 10 countries in the world in terms of accessibility and cost convenient access to Gigabit Internet" (The Government of the Republic of Moldova and the Ministry of Economic Development and Digitalization, pg. 10). Therefore, it is crucial to have an educated population in this field. Internationally, the EU is among Moldova's most important strategic partners. It is in the common interest of Chisinau and Brussels to develop a resilient Republic of Moldova that can handle external threats, especially in the context of the war in Ukraine. For example, as part of the European Peace Facility Assistance on Cyber Defence in Moldova, the EU sent capacity-building military actors to help Moldovan decision-makers develop resilient and robust security systems (e-Governance Academy, 2023b).

At the institutional level, the National Agency for Cybersecurity was created in December 2023 (The Government of the Republic of Moldova, 2023). Legally speaking, according to the European norms, the Republic of Moldova adopted a new legislation addressing the cyberspace that will enter into force in 2025 with EU's support (Delegation of the European Union to the Republic of Moldova, 2023a). In terms of concrete activities funded by the EU, in 2023 the Republic of Moldova held a three-day cybersecurity exercise in order to enhance its resilience against cyber threats (Delegation of the European Union to the Republic of Moldova, 2023b). It also took part in the European Cybersecurity Month organised in October 2023 (E-governance Agency, 2023a).

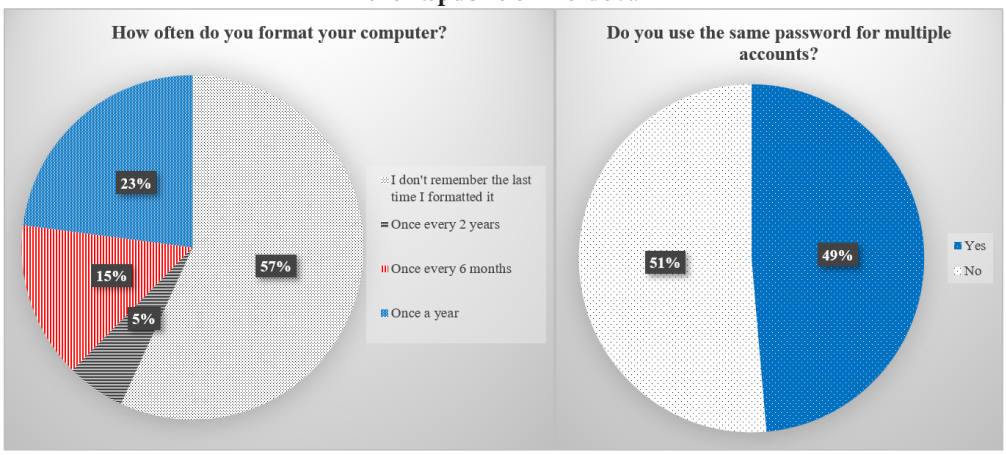
Those actions were necessary, but not sufficient. As already mentioned, the concept of resilience relates to a system. Thus, we cannot realistically speak about a country's resilience without taking into consideration relevant features of its society. According to statistical data, in 2021 approximately 80% of the Moldovan population

had access to the internet. 82% of the individuals that participated in the 2021 poll were aged between 15 and 59 (The Government of the Republic of Moldova and the Ministry of Economic Development and Digitalization, pg. 10). Hence, we can infer that the active population and the young people are among the most connected to the internet and, thus, the most vulnerable in the cyberspace.

To assess the levels of awareness, we have studied the young population from the Republic of Moldova, by applying an in-depth questionnaire designed to assess their knowledge of the connectivity level, the vulnerabilities of the cyberspace, the ways to mitigate those threats, the EU's measures and values, the state's activities, and their views on the Moldovan civil society and its role in this field. The questionnaire was applied to 103 students from Moldova State University (the biggest public university in the Republic of Moldova) that specialise in Public Administration, Political Science, International Relations, European Studies, and Law. The questionnaire was available from December 2023 until January 2024. We have chosen these specializations because they do not have a major in the field of cybersecurity, although cybersecurity has a direct impact on their everyday life. Also, given their majors, their future chances of working in the public administration sector are rather high. If civil servants do not possess the necessary competences in the fields of cybersecurity and resilience, this may affect the state's resilience in the medium and long terms. The questionnaire was targeted at the active population, hence there were 57 respondents aged 18-25 years, 28 aged 26-40 years, and 18 aged 40-60 years. As far as the gender of the respondents is concerned, 58% of them (i.e., 63 respondents) were women and 42% (i.e., 46 respondents) were men. Moreover, 58% of the respondents were students at MA level, and 42% at BA level (*Authors' own research*).

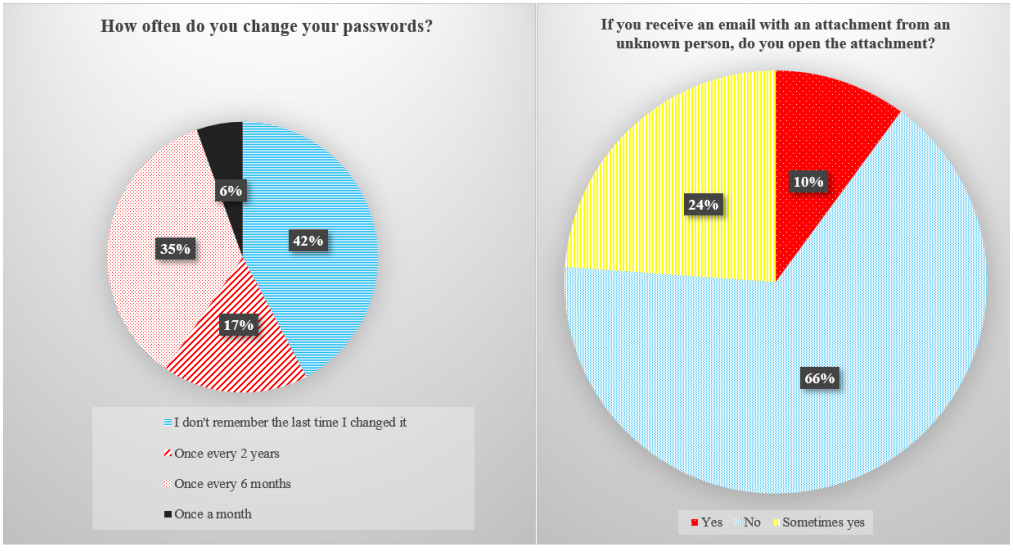
To reach a suitable level in terms of resilience (as defined in the second chapter), firstly you need to know the potential threats and the necessary steps to ensure a system's protection. Only then will you have greater chances to identify the attack and stop it, while the system is recovering. Thus, the cyber hygiene is required of all internet users. When asked what cyber hygiene is, 50 out of 103 respondents answered that they do not know or have never heard that term before. When asked when they last formatted their computer, 57% did not remember, while only 15% declared that they are doing it on a regular basis, once every 6 months (*Chart 1*). Additionally, 49% of the respondents use the same password for multiple accounts (*Chart 2*) and 42% of them did not remember the last time they have changed their passwords (*Chart 3*). Lastly, 34% of the respondents answered that they would open an email attachment from an unknown person (*Chart 4*). These results are illustrated in the charts below (*Authors' own research*).

Chart 1 and chart 2 – Questionnaire applied to the active population (18-60 years old) of the Republic of Moldova



Source: Authors' own research.

Chart 3 and chart 4 – Questionnaire applied to the active population (18-60 years old) of the Republic of Moldova



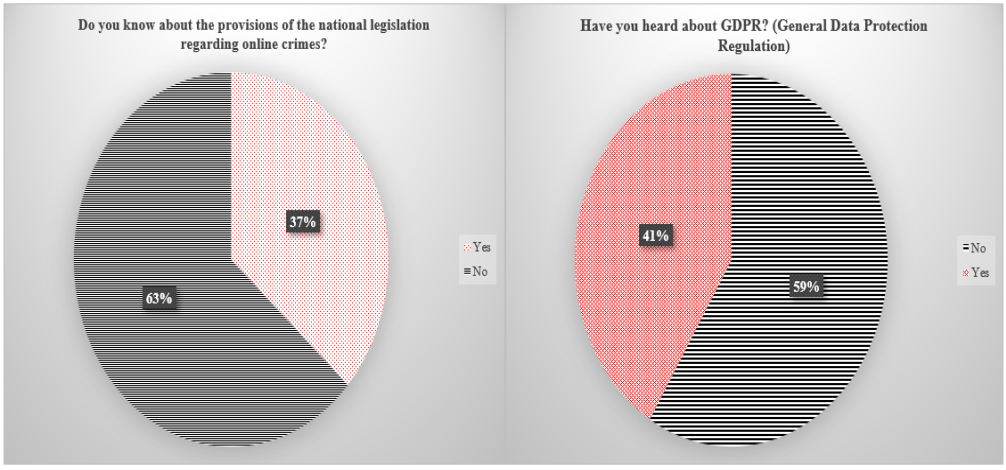
Source: Authors' own research.

Unfortunately, these results depict a very negative situation of the Moldovan society's resilience in the cyberspace. Although the target group was formed of educated individuals who spend a significant amount of time online, it came out that even they lack the basic knowledge of the current cybersecurity landscape. According to some 2023 statistics (AAG, 2024), phishing is still seen as the most common form of cybercrime, with 3.4 billion spam emails sent daily. Thus, opening an attachment from an unknown sender is highly problematic. The results of the questionnaire are

confirmed by the statistics published in December 2023 by the National Cybersecurity Index, according to which the Republic of Moldova recorded a score of 2 out of 10 in what concerns the education and professional development at the undergraduate level of cybersecurity. The statistics offer as well a bleak picture of the graduate cybersecurity education sector, which received a score of 3 out of 10 (e-Governance Academy Foundation, 2023b, pg. 1). As regards the indicators 'public cybersecurity awareness resources' and 'cybersecurity awareness raising coordination', Moldova maintained the score of 3 out of 10 (e-Governance Academy Foundation, 2023b, pg. 2).

The results of the questionnaire demonstrate that the respondents' knowledge of the national legislation in the cyber domain remains minimal. Only 37% of them declared that they know about such provisions (*Chart 5*). Since the Republic of Moldova is an EU candidate state, the recorded level of knowledge about European norms is more positive, i.e. 41% of the students who took part in the poll (*Chart 6*) declared having heard of the European General Data Protection Regulation (GDPR) (*Authors' own research*).

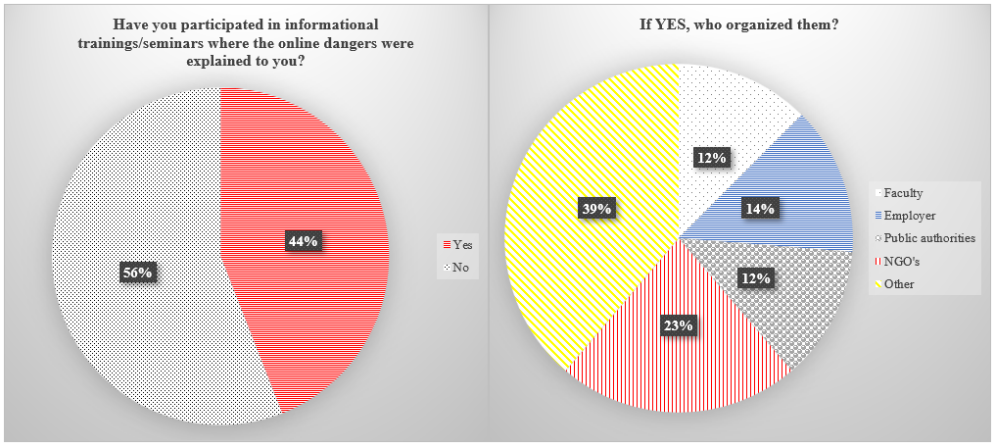
Chart 5 and chart 6 – Questionnaire applied to the active population (18-60 years old) of the Republic of Moldova



Source: Authors' own research.

These results could be explained by the students' limited access to trainings or awareness campaigns on all these topics. When asked about this aspect, only 44% of them confirmed having participated in informational trainings/seminars where the online dangers are presented (*Chart 7*). The state and the NGOs are among the top providers of such services (*Chart 8*), proving the necessity of developing partnerships between the public authorities and the civil society (*Authors' own research*).

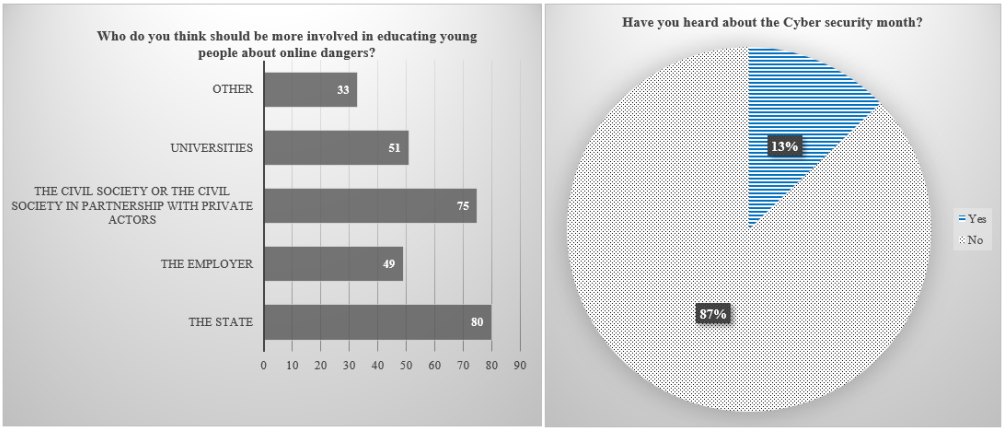
Chart 7 and chart 8 – Questionnaire applied to the active population (18-60 years old) of the Republic of Moldova



Source: Authors' own research.

As regards the issue of the most suitable actors to provide these types of trainings and awareness campaigns, the respondents had a multiple-choice question. The majority of them (80 out of 103) declared that the state should the first provider of such services, followed closely by the civil society (75 out of 103) (*Chart 9*). Here the civil society was viewed as an actor that acts on his own or in cooperation with private actors. In what concerns the visibility of EU's annual event titled "Cyber Security month", 87% of the respondents stated that they had not heard about it (*Chart 10*), although, as previously mentioned, it is organised at the European level since 2012, and the Republic of Moldova itself organised it in 2023. (*Authors' own research*).

Chart 9 and chart 10 – Questionnaire applied to the active population (18-60 years old) of the Republic of Moldova

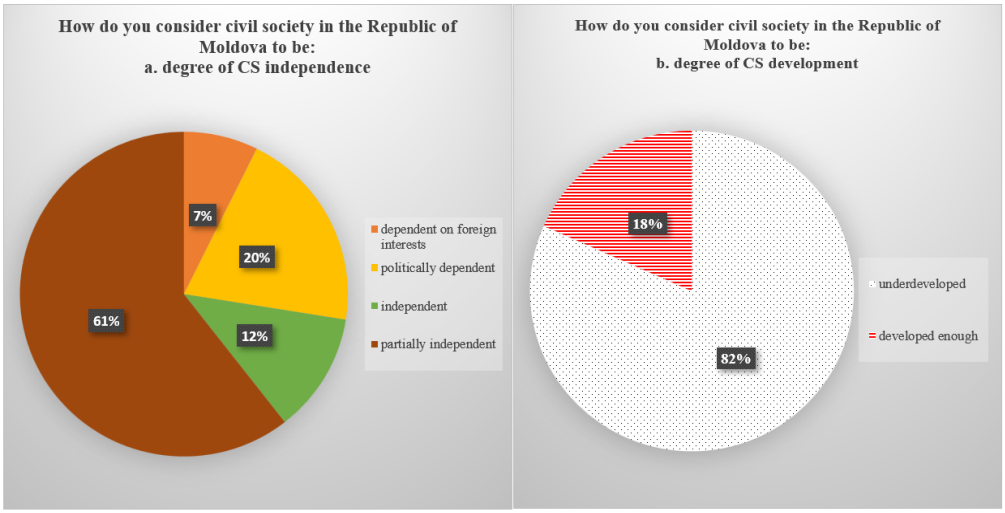


Source: Authors' own research.

Additionally, the majority of the respondents, i.e. 61%, see the Moldovan civil society partially independent, while 20% view it as politically dependent, 7% consider

it dependent on foreign interests, and only 12% see it as independent (*Chart 11*). Furthermore, when asked about the civil society's development level, the majority of the respondents, namely 82%, said that they view it as underdeveloped (*Chart 12*).

Chart 11 and chart 12 – Questionnaire applied to the active population (18-60 years old) of the Republic of Moldova



Source: Authors' own research.

These results match the European Commission's recent assessment, which concludes that the Moldovan civil society still lacks the necessary tools to engage more in policy dialogues (European Commission, 2023, pp. 16, 86). Thus, we cannot claim that the Republic of Moldova is a resilient state. However, based on relevant statistics and strategic documents analysed herein, we can conclude that the Moldovan civil society wants to become resilient. To achieve this goal, it must develop a resilient society by initially harnessing the power of information and education.

Conclusions

The purpose of this article was to assess the Moldovan society's resilience in the face of cyber threats, by taking into account the European norms and strategies. Firstly, we conducted an analysis of the main strategic cybersecurity documents adopted by the EU and the Moldovan authorities. Secondly, we analysed the institutional and legal frameworks by using statistical data. We highlighted, among others, the importance of measuring the internet connectivity and the digital literacy levels. At the macro level, the Republic of Moldova is just beginning to implement the EU legislation on cybersecurity. Thus, we cannot discuss yet about the convergence of the European and Moldovan legislations in this field, since the latter will enter into force in 2025. Lastly, the survey we carried out focused especially on the young Moldovans' level of awareness of cyber threats. More than 100 Moldovan students responded to a questionnaire to assess their level of awareness of cyber threats. Our poll was targeted at young people (students) because they are the most active online. Additionally, we selected many students with a major in international relations since these ones are certainly more familiar with the European dynamics. Results show that although the authorities in Chisinau have taken

important steps to develop the country's resilience in the cyberspace – by providing the necessary legislation and institutional framework, in partnership with the EU, and we refer especially to the National Information Security Strategy, and the Digital Transformation Strategy 2023-2030 – , their medium- and long-term impacts remain to be seen. Currently, the Moldovan civil society and young Moldovans in general still lack basic knowledge of the cyber hygiene required to protect themselves online. Although the Republic of Moldova is an EU candidate country, its population is not well versed in the European cyber initiatives. The civil society is viewed as an important player, but remains underdeveloped there and partially dependent on political affiliations. It is in its initial stages of development. Thus, we cannot label the Moldovan state as being resilient in front of the current cyber threats. It remains to be seen how steadfast and efficient the decision-makers will be in stepping up the resilience of their country.

References:

- AAG, (2024). "The Latest 2023 Cyber Crime Statistics" (updated January 2024). Available at: https://aag-it.com/the-latest-cyber-crime-statistics/. Accessed on: January 10, 2024.
- Brie, M., Horga, I., (2014). "The European Borders - Expressions of Identity", *Transylvanian Review*, Vol. XXIII, supplement No.1, pp. 202-216.
- Brie, M., Putină, N., (2023). "The Development and Role of Civil Society in the Republic of Moldova in the Framework of the Eastern Partnership (2009–2021)", *Civil Szemle*, Vol. XX, No. 4, pp. 167-185.
- Brie, M., (2021). "Comparative Conceptual Perspectives on Identity Borders in the Republic of Moldova", *Europolity. Continuity and Change in European Governance*, Vol. 15, No. 2, pp. 5-29.
- Brie, M., Costea, A.-M., and Petrila, L., (2023). "Perceptions of civil society in Armenia and Azerbaijan in the context of the Nagorno-Karabakh conflict", *Civil Szemle*, XX, No. 2, pp. 99-118.
- Brie, M., Islam, J., and Polgár I., (2023). "North Macedonia's Internal and External Identity Disputes. Role and Implication for the Civil Society", *Civil Szemle*, XX, No. 2, pp. 69-98.
- Brie, M., Islam J., and Polgár, I., (2022). "Is Inclusivity Necessary for Legitimacy of New Regionalism? Unpacking Open Balkan Initiative Negotiations", *Transylvanian Review*, Vol. 31, Supplement No. 2, pp. 185-208.
- Brie, M., Mărcuţ, M., and Polgár, I., (2022). "Developing International Cooperation Capabilities to Boost Local Development and Social Responsibility. Case study: Bihor County", *Civil Szemle,* Vol. XIX, No. 4, Budapesta, pp. 133-151.
- Collins, S., McCombie, S., (2012). "Stuxnet: The Emergence of a New Cyber Weapon and its Implications", *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, pp. 80-91.

- Costea, A-M., (2023). "Private-Public Partnerships in Cyber Space as Deterrence Tools. The Trans-Atlantic View", *Europolity. Continuity and Change in European Governance*, Vol. 17, No. 2, pp. 111-134. Available at: http://europolity.eu/wp-content/uploads/2023/12/4.-Costea_compressed.pdf. Accessed on: August 15, 2024.
- Delegation of the European Union to the Republic of Moldova, (2023a). *Moldova adopted the EU-backed Cybersecurity Law.* Available at: https://www.eeas.europa.eu/delegations/moldova/moldova-adopted-eu-backed-cybersecurity-law_en?s=223. Accessed on: August 10, 2024.
- Delegation of the European Union to the Republic of Moldova, (2023b). *Cybersecurity exercise enhances Moldova's resilience against cyber threats*. Available at: https://www.eeas.europa.eu/delegations/moldova/cybersecurity-exercise-enhances-moldova%E2%80%99s-resilience-against-cyber-threats_en. Accessed on: August 10, 2024.
- e-Governance Academy Foundation, (2023b). *The National Cyber Security Index. Moldova*. Available at: https://ncsi.ega.ee/country/md/?pdfReport=1. Accessed on: August 10, 2024.
- e-Governance Academy. *European Peace Facility Assistance on Cyber Defence in Moldova*, Moldova. Available at: https://ega.ee/project/european-peace-facility-moldova/. Accessed on: August 10, 2024.
- e-Governance Agency, (2023a). *October – Cybersecurity Awareness Month*. Available at: https://egov.md/en/node/40107. Accessed on: August 10, 2024.
- ECCC, (2021). *Cyber policy*. Available at: https://ecs-org.eu/european-cybersecurity-competence-centre-launches-its-website/. Accessed on: September 20, 2024.
- ENISA, (2021). *European Cybersecurity Month 2021 - Deployment report.* https://www.enisa.europa.eu/publications/european-cybersecurity-month-2021-deployment-report. Accessed on: January 10, 2024.
- ENISA, (2022). *Cybersecurity Education Initiatives in the EU Member States.* Available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states. Accessed on: August 15, 2024.
- ENISA, (2024). *About ENISA*. Available at: https://www.enisa.europa.eu/about-enisa/regulatory-framework. Accessed on: January 10, 2024.
- EUR-Lex, (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001. Accessed on: August 10, 2024.
- European Commission, (2020a). *The EU's Cybersecurity Strategy for the Digital Decade*. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. Accessed on: August 15, 2024.

- European Commission, (2020b). *Digital Education Action Plan (2021-2027)*. Available at: https://education.ec.europa.eu/focus-topics/digital-education/action-plan. Accessed on: August 10, 2024.
- European Commission, (2021). *2030 Digital Compass: the European way for the Digital Decade*. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118. Accessed on: August 15, 2024.
- European Commission, (2022). *Cyber Resilience Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. Accessed on: August 15, 2024.
- European Commission, (2023). *SWD (2023) 698 final. Republic of Moldova 2023 Report. 2023 Communication on EU Enlargement policy.* Available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_698%20Moldova%20report.pdf. Accessed on: August 10, 2024.
- European Commission | EU Science Hub, (n.d.). *Resilience*. Available at: https://joint-research-centre.ec.europa.eu/scientific-activities-z/resilience_en. Accessed on: 15 August 2024.
- *European Cybersecurity month*, (n.d.). Available at: https://cybersecuritymonth.eu/about-ecsm/. Accessed on: August 20, 2024.
- European Union, (2022). *A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security.* Available at: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf. Accessed on: August 15, 2024.
- Eurostat, (2023). *Being young in Europe today - digital world.* Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Being_young_in_Europe_today_-_digital_world&oldid=564756. Accessed on: August 10, 2024.
- EUR-Lex, (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data*. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html. Accessed on: August 20, 2024.
- Fjäder, C., (2014). "The nation-state, national security and resilience in the age of globalization". *Resilience: International Policies, Practices and Discourses*. Vol. 2, No. 2, pp. 114-129.
- Holling, C.S., (1973). "Resilience and Stability of Ecological Systems", *Annual Review of Ecology and Systematics*, Vol. 4, pp. 1–23. Available at: http://www.jstor.org/stable/2096802. Accessed on: August 10, 2024.
- Jibilian, I., Canales, K., (2021). *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal.* Available at: https://

www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12. Accessed on: August 15, 2024.

- Jusufi, I., Polgár I.-J., (2023). "The Interaction between the Level of Democracy and the Perception of the Civil Society. The Case of Albania and North Macedonia (2010–2022)", *Civil Szemle*, Vol. XX, Budapest, No. 4, pp.127-150.
- Kaspersky, (n.d.). *What is WannaCry ransomware?* Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Accessed on: August 15, 2024.
- Mărcuț, M., Chiriac, C., (2023). "Assessing TikTok's Potential for Civil Society in Europe: A Literature Review", *Civil Szemle*, Vol. XX, No. 4, Budapest, pp. 263-278.
- Mills, E., (2012). "Romanian arrested on Pentagon, NASA hacking charges", *CNET*, January 31. Available at: https://www.cnet.com/news/privacy/romanian-arrested-on-pentagon-nasa-hacking-charges/. Accessed on: August 15, 2024.
- Official Journal of the European Union, (2022). *The NISS 2 Directive*. Available at: https://www.nis-2-directive.com/. Accessed on: September 15, 2024.
- Pitrelli, M., (2022). "Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia", *CNBC*, July 28. Available at: https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html. Accessed on: August 15, 2024.
- Polgár, I.J., (2023). "The Role of Civil Society Organisations in Migration Management. Cooperation between Public Authorities and Civil Society Actors at the EU's South Eastern Borders", *Civil Szemle*, Vol. XX, No. 4, Budapest, pp. 27-40.
- Popoveniuc, B., (2022). *"Moral-Democratic Competence as a pillar of Civil Society"*, *Civil Szemle*, Special issue, pp. 19-41.
- Purplesec, (2024). *Cybersecurity Statistics. The Ultimate List of Cybersecurity Stats Data, & Trends.* Available at: https://purplesec.us/resources/cyber-security-statistics/#Cybercrime. Accessed on: January 15, 2024.
- Putină, N., Brie, M., (2023). "Civil Society Development and Democratization in the Republic of Moldova", *Civil Szemle*, Vol. XX, No. 4, Budapest, pp. 79-108.
- Statica, (2024). *Annual level of internet access among households in cities, towns & suburbs, and rural areas in the European Union from 2007 to 2022.* Available at: https://www.statista.com/statistics/1370388/eu-digitalization-level-household-internet-access-rural-urban/#statisticContainer. Accessed on: August 15, 2024.
- Svitková, K., (2017). "Resilience in the National Security Discourse", *Obrana a Strategie [Defence & Strategy]*, Vol. 17, No. 1, pp. 21-42. DOI: 10.3849/1802-7199.17.2017.01.021-042.

- The Government of the Republic of Moldova, (2023). *În Republica Moldova va fi creată Agenția Națională pentru Securitate Cibernetică [The National Cyber Security Agency will be created in the Republic of Moldova]*. Available at: https://gov.md/ro/content/republica-moldova-va-fi-creata-agentia-nationala-pentru-securitate-cibernetica. Accessed on: August 16, 2024.
- The Government of the Republic of Moldova, the Ministry of Economic Development and Digitalization, and the UNDP. *Republica Moldova – Strategia de transformare digitală 2023–2030 [Republic of Moldova's Digital Transformation Strategy 2023-2030]*. Available at: https://mded.gov.md/wp-content/uploads/2023/11/STD_RO.pdf. Accessed on: August 16, 2024.
- The Parliament of Moldova, (2018a). *Decision No. 257. Hotărâre privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia [Decision on the approval of the Information Security Strategy of the Republic of Moldova for the years 2019–2024 and the Action Plan for its implementation]*. Available at: https://www.parlament.md/LegislationDocument.aspx?Id=b9a17a8f-da13-41b6-ae7d-ba1d7b96f0aa. Accessed on: August 16, 2024.
- The Parliament of Moldova, (2018b). *Decision No. 257. Annex No. 2: Plan de Acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 [The Action Plan for the implementation of the Information Security Strategy of the Republic of Moldova for the years 2019–2024]*. Available at: https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro. Accessed on: August 16, 2024.
- Van Metre, L. (2016). "Fragility and Resilience", FSG Policy Brief No. 2, September, *US Institute of Peace, Carnegie Endowment for International Peace, and Center for a New American Security.* Available at: https://www.usip.org/publications/2016/09/fragility-and-resilience. Accessed on: August 16, 2024.
- Walker, B., Salt, D., (2012). *Resilience Practice: Building Capacity to Absorb Disturbance and Maintain Function*, London: Island Press.
- Zakota, Z., and Németh, I.P., (2022). "Civil Society and Education in the European Union". *Civil Szemle*, Special issue, pp. 293-305.