Original Scientific Paper
UDC: 004.056(497.115)
DOI: https://doi.org/10.22598/iele.2024.11.1.1

EMPOWERING CYBERSECURITY AWARENESS AMONG THE CITIZENS OF KOSOVO

Enver Buçaj [*]

ABSTRACT

This research paper aims to enhance the awareness of cybersecurity among the citizens of Kosovo, addressing the escalating risks and challenges posed by cyber threats. Employing a robust quantitative methodology involving surveys and interviews, this study delves into citizens' awareness, information, and the formidable barriers they encounter within the cybersecurity domain. The research findings underscore a commendable level of awareness among citizens concerning the perils of cyber threats, coexisting with a noteworthy deficiency in general cybersecurity information. Additionally, citizens identify an array of barriers and challenges that hinder their ability to fortify their defence against cyberattacks. Notably, a correlation analysis unearths a positive relationship between information and awareness, implying that as citizens acquire more knowledge, their cybersecurity awareness tends to thrive. Conversely, barriers and challenges exhibit a negative correlation with awareness, emphasizing the substantial impact these obstacles can have on citizens' preparedness. Moreover, ANOVA - Analysis of Variance provides a comprehensive examination of the influence of information, barriers, and challenges on citizens' overall awareness. Furthermore, hypothesis testing reaffirms the research's core findings: citizens in Kosovo possess a high degree of awareness concerning cyber threats, yet they grapple with a deficiency in general cybersecurity information and confront multifaceted barriers and challenges in safeguarding their digital landscapes. This research paper not only contributes to the fortification of cybersecurity awareness among Kosovo's citizens but also underscores the critical need to address the prevailing challenges in this domain. Through concerted efforts to bolster cybersecurity education, provide accessible information resources, and surmount the barriers that citizens face, Kosovo can stride toward a more cyber-resilient society. By embracing these measures,

[*] Faculty of Law, University "Ukshin Hoti", Prizren, Republic of Kosovo, enver.buqaj@uni-prizren.com

Kosovo positions itself to navigate the complex landscape of cybersecurity threats, ensuring the safety and security of its digital realm in an increasingly interconnected world.

***Key words**: cybersecurity, awareness, Kosovo, correlation analysis, ANOVA analysis.*

1. INTRODUCTION

As the digital revolution progresses, the dichotomy of opportunity and vulnerability becomes evident. The transformative power of the internet, while catalysing advancements in communication, commerce, and governance, has inadvertently birthed a new battleground - the cyber realm. This battleground is fraught with malevolent actors ranging from individual hackers to organized syndicates and even state-backed entities, all wielding the power to disrupt the very fabric of a nation's digital infrastructure.

The Republic of Kosovo, standing at the crossroads of modernization, is a microcosm of this global paradigm. Its efforts to modernize, digitize, and be part of the global digital community make it both a participant and a potential target in this new age warfare. Hence, understanding and investing in cybersecurity isn't just a matter of national security; it's a testament to a nation's commitment to protecting its citizens, its businesses, and its future.

Pivoting towards a digital-first strategy in the Western Balkans brings with it the promise of economic growth, streamlined governance, and societal advancements. Yet, it also means that vulnerabilities, if left unaddressed, can ripple through the socio-economic fabric of these nations. It underscores the necessity of not just technical solutions but also educational endeavours. A populace informed about potential cyber threats becomes the first line of defence against them.

Additionally, fostering regional collaborations and knowledge-sharing can be a force multiplier in this digital age. By sharing best practices, threat intelligence, and resources, countries in the Western Balkans can present a unified front against cyber threats, ensuring that as they progress digitally, they also safeguard their collective digital futures. In the modern era marked by digital ubiquity, understanding the intricacies of cybersecurity becomes paramount. As countries harness the limitless potentials of the digital epoch, they grapple with the concomitant cyber challenges. For the Republic of Kosovo, the call to enhance its cyber defence mechanisms and nurture cybersecurity cognizance among its populace is both timely and visionary.

Cyber threats, with their capability to cross national boundaries, imperil individuals, institutions, and states. The repercussions are manifold, from financial repercussions to jeopardizing national security, pilfering intellectual property, and diminishing public faith. Within this intricate web, the citizens' role in protecting digital commodities and bolstering national cyber defence stands paramount.

In the rapidly digitalizing landscape of Kosovo and the broader Western Balkans, the gravity of cybersecurity looms large. The region's burgeoning dependence on e-governance, digital financial systems, and the synergy of vital infrastructures flags immense repercussions in the event of cyber breaches. A cyber onslaught in the region might culminate in losses upwards of €10 million daily. The transformation of nations into the digital realm increases their dependence on online services and advanced digital financial systems. As highlighted by Radunovic[1], major cyber disruptions have the potential to result in immense daily financial setbacks. The cyber domain plays a crucial role in a nation's prosperity. Cyber strategies extend beyond just the digital sphere, influencing the overall balance and socio-economic advancement of a nation.

Dissecting the Western Balkans' cyber readiness reveals disparities. Kosovo, despite a discernible vacuum in cybersecurity awareness endeavours, has championed cybercrime combat through its dedicated police entities and legislative reforms. Albania parades its dedicated cyber watchdog, ALCIRT, coupled with a defined cyber blueprint. Montenegro, with its national CERT and its overarching 2013-2017 cyber game plan, emerges distinctively. Serbia faces the conundrum of a fragmented cyber leadership, resulting in overlapping jurisdictional entities. While Macedonia might not flaunt an official CERT, its academia's proactive foray into cyber realms heralds promise. Bosnia and Herzegovina, sans a dedicated cyber unit, relies on its Ministry of Security to pioneer its cyber fortification endeavours. These narratives, anchored in Poposka's 2016 observations, underscore the compelling necessity for region-wide, holistic cyber strategies [2,3,4].

In Kosovo's digital frontier, the urgency to pioneer expansive measures and heighten cyber awareness is palpable. Amidst a conspicuous lack of extant research, this investigation aims to bridge this gap, offering nuanced insights

[1] Radunović, V.: DDoS - available weapon of mass disruption. *Proceedings of the 21st Telecommunications Forum Telfor (TELFOR)*, Belgrade: Curran Associates Inc., 2014, pp. 5-8.

[2] Poposka, V.: The Urge for Comprehensive Cyber Security Strategies in the Western Balkans, *Information & Security*, 34(1) 2016, pp. 25-36.

[3] Jica, H.: Cyber Security and National Security Awareness Initiatives in Albania: A Synergy Approach, *Mediterranean Journal of Social Sciences* 4(10) 2013, pp. 614-622.

[4] Nagyfejeo, E., Puello Alfonso, S.: Cybersecurity Capacity Review Bosnia and Herzegovina, *SSRN*, 2019.

to shape policies, strategic blueprints, and pedagogic interventions tailored to Kosovo's unique cyber challenges. This study embarks on a seminal voyage, striving to cultivate a rich cyber-awareness tapestry for Kosovo's populace, preparing them for the ever-evolving cyber challenges, and fostering a resilient digital ethos.

The purpose of this research paper is to delve into the multifaceted realm of cybersecurity in Kosovo. It seeks to examine the current state of cybersecurity awareness, information, and the barriers faced by citizens in safeguarding themselves against cyber threats. Through empirical research and analysis, the study aims to inform policy decisions, educational initiatives, and public awareness campaigns that can collectively enhance the cybersecurity posture of Kosovo.

To guide our exploration, this study formulates the following research hypotheses:

- *There is a high level of awareness among the citizens of the Republic of Kosovo regarding cyberattacks and cyber threats.*
- *A deficiency of general information about cybersecurity is present among the citizens of Kosovo.*
- *Citizens confront various barriers and challenges when it comes to defence against cyberattacks.*

This research paper is structured as follows: it commences with an introduction, providing context and outlining the study's objectives. The subsequent section presents a comprehensive literature review, grounding the study in existing scholarship. The methodology section elucidates the research approach and data collection methods, while the results section is subdivided into multiple subsections, addressing demographic data, citizens' cybersecurity awareness, information levels, barriers, and challenges, followed by statistical analyses. A dedicated discussion section interprets and contextualizes the findings, leading to a conclusive summary in the conclusion. Recommendations are proposed to enhance cybersecurity awareness among Kosovo's citizens, and the paper concludes with a comprehensive bibliography - reference list. This structured approach ensures a coherent exploration of the study's facets, facilitating a holistic understanding of the subject matter.

2. LITERATURE REVIEW

In today's digitally connected world, cybersecurity awareness is of paramount importance to individuals, organizations, and nations. The emergence of cyber threats and attacks has highlighted the need for comprehensive cybersecurity strategies and the cultivation of a cybersecurity-conscious society.[5] Cybersecurity awareness is a multifaceted endeavour that demands attention to gender-specific behaviour, national capacity assessments, regional dynamics, psychological factors, legislation, international cooperation, and educational challenges. The case of Kosovo, situated in the Western Balkans, presents both unique opportunities and challenges in cultivating a cybersecurity-conscious society. This literature review, based on a diverse range of research and regional insights, lays the foundation for informed and context-specific cybersecurity awareness initiatives in Kosovo. The collaboration of stakeholders, including government, academia, and international partners, is crucial in empowering the citizens of Kosovo to navigate the digital landscape securely. As cyber threats evolve, so must the strategies for awareness and protection.

Cybersecurity awareness constitutes a multifaceted domain, fusing theoretical constructs with empirical evaluations, thereby constructing a robust foundation for comprehending the intricacies of this critical field. Theoretical dimensions, exemplified by gender disparities, privacy concerns, and behavioural determinants, collectively serve as pillars upon which cybersecurity awareness is built. In tandem, empirical investigations contribute pragmatic insights into a nation's state of readiness against cyber threats, its areas of vulnerability, and the efficacy of implemented awareness initiatives. Consequently, adopting a holistic approach, one that encompasses the deployment of comprehensive strategies, educational endeavours, and international collaboration, assumes paramount significance in mitigating the escalating intricacy and recurrence rates of cyber threats, a stance underscored by seminal works in this field[6, 7]. In the realm of theoretical foundations, gender differences in cybersecurity behaviour are a critical area of research. Understanding these distinctions is essential for tailoring awareness programs to different demographic groups and promoting inclusive cybersecurity practices. Research by Anwar et al.[8] demonstrates that there are gender-specific patterns in cybersecurity behaviour, with female employees often exhibiting greater caution than their male counterparts. This highlights the importance of gender-sensitive approaches in cybersecurity awareness campaigns.

[5] Mori, S., Goto, A.: Reviewing national cybersecurity strategies, *Journal of disaster research*, 13(5) 2018, pp. 957-966.

[6] Bada, M.: Cybersecurity Capacity Assessment of the Republic of Kosovo, *SSRN,* 2015.

[7] Ganin, A. A. et al.: Multicriteria decision framework for cybersecurity risk assessment and management, *Risk Analysis*, 40(1) 2017, pp. 183-199.

[8] Anwar, M. et al.: Gender difference and employees' cybersecurity behaviors, *Computers in Human Behavior*, 69 2017, pp. 437-443.

The Concern for Information Privacy (CFIP) instrument, introduced by Stewart, K. A. et al.[9], measures individuals' privacy concerns. This instrument aids in assessing concerns related to phishing threats, enabling more targeted awareness efforts. Studies using CFIP reveal that individuals with higher privacy concerns tend to be more cautious online, displaying increased awareness of potential threats and a greater propensity to adopt protective measures. Behavioural aspects play a pivotal role in cybersecurity awareness, as evident from Mark[10] study analyzing factors influencing phishing threat avoidance behaviour. His research underscores that individuals with greater cybersecurity knowledge and skills are more adept at recognizing phishing attempts and taking appropriate action. Furthermore, the study highlights that individuals previously targeted by phishing attacks tend to exhibit heightened vigilance and awareness, emphasizing the experiential dimension of cybersecurity behaviour.

Empirical investigations into national cybersecurity readiness assume a central role in assessing tangible preparedness within the cyber domain. Such inquiries prove indispensable for evaluating a nation's ability to confront and mitigate the myriad threats and vulnerabilities that characterize the contemporary digital landscape. Cybersecurity capacity assessments yield a comprehensive assessment of a nation's cyber strengths and weaknesses, often culminating in actionable recommendations for fortifying cybersecurity infrastructure, refining policies, and orchestrating awareness campaigns.

The cybersecurity landscape of any country requires a comprehensive assessment to identify strengths, weaknesses, and areas of improvement. Bada[11] conducted a cybersecurity capacity assessment of the Republic of Kosovo. This assessment serves as a foundational document for understanding Kosovo's readiness in addressing cybersecurity challenges. Such assessments provide valuable insights into the specific needs and priorities of the nation, forming the basis for tailored cybersecurity awareness initiatives.[12]

[9] Stewart, K. A., Segars, A. H.: An empirical examination of the concern for information privacy instrument, *Information systems research,* 13(1) 2002, pp. 36-49.

[10] Mark, M. S.: *An analysis of factors influencing phishing threat avoidance behavior: a quantitative study*, School of Business and Technology, doctoral dissertation, Capella University, March 2021.

[11] Bada, M.: Cybersecurity Capacity Assessment of the Republic of Kosovo. *Global Cyber Security Capacity Centre,* 2015.

[12] Maraj, A., Sutherland, C., Butler, W.: The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo, in Eze, T., Speakman, L., Onwubiko, C. (eds.) *Proceeding 20th European Conference on Cyber Warfare and Security*, Chester: University of Chester, 2021.

The importance of national cybersecurity awareness programs is evident not only in Kosovo but also across the world. The United Nations Office on Drugs and Crime conducted a comprehensive study on cybercrime, shedding light on the multifaceted nature of cyber threats. While the study is not specific to Kosovo, it underscores the global nature of cyber threats. Kosovo's awareness efforts must align with the evolving landscape of cybercrime to effectively protect its citizens and infrastructure.[13]

Proximity and regional dynamics often influence the cybersecurity landscape of neighboring countries. Fotescu et al.[14] explored Albania's cybersecurity pivot, navigating between Western architectures and great power competition. Understanding the geopolitical dynamics shaping a country's cybersecurity posture is essential for Kosovo. It highlights the need for a balanced approach that considers both regional and international cybersecurity frameworks. Bahiti, R. et al. [15] and Moci[16] also examined the case of Albania and its efforts towards a more resilient cyberspace. The research provides valuable insights into the challenges and initiatives in a neighboring country that may have relevance to Kosovo. Cross-border cooperation and knowledge sharing can be essential in strengthening cybersecurity awareness. Bada et al.[17] conducted an empirical study reviewing national cybersecurity awareness in Africa. The findings emphasize the need for coordinated and effective awareness campaigns to mitigate cybersecurity risks. While this study focuses on Africa, its insights can be valuable for Kosovo, highlighting the significance of cohesive awareness efforts. Phishing scams remain a prevalent threat in cyberspace, targeting individuals and organizations worldwide. Butavicius et al.[18] investigated factors influencing people's vulnerability to phishing scams. Their study underscores the importance of time pressure and deception cues in phishing detection. Understanding these psychological factors can inform the design of cybersecurity

[13] Malby, S. et al.: Comprehensive study on cybercrime, New York: United Nations, 2013.

[14] Fotescu, A. Chihaia, M. S.: Albania's cybersecurity pivot: Between Western architectures and great power competition, in Scott N. R., Mary M. (eds.): *Routledge Companion to Global Cyber-Security Strategy*, London: Routledge, 2021, pp. 26-35.

[15] Bahiti, R., Josifi, J.: Towards a more resilient cyberspace: the case of Albania, *Information & Security: An International Journal*, 32 2015, pp. 120-130.

[16] Moci, E.: Cybersecurity Awareness in Albania, *European Journal of Social Science Education and Research*, 8(3) 2021, pp. 112-117.

[17] Bada, M., Solms, B. V., Agrafiotis, I.: Reviewing national cybersecurity awareness in Africa: an empirical study, *Apollo - University of Cambridge Repository*, 2019.

[18] Butavicius, M. A., Taib, R., Han, S. J.: Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails, *Computers & Security*, 123 2022, pp. 102937.

awareness campaigns that effectively educate individuals on recognizing and avoiding phishing attempts.

The legal and regulatory framework plays a crucial role in enhancing cybersecurity. Cesarec[19] examined cybersecurity legislation and implementation in Southeast European (SEE) countries, offering an overview of the policy landscape. While the study focuses on SEE, the relevance of cybersecurity legislation is evident for Kosovo. Robust legal frameworks are essential in fostering a culture of cybersecurity awareness and compliance. International support and collaboration are vital in strengthening cybersecurity capacities. The European Union's support for cybersecurity capacity building in the Western Balkans is a testament to the recognition of regional cybersecurity challenges. This support can serve as a model for cooperation and resource mobilization in Kosovo's pursuit of enhanced cybersecurity awareness.[20]

Maraj et al. [21] explored the challenges to cybersecurity education in developing countries, using Kosovo as a case study. The findings highlight the need for tailored educational approaches to address specific challenges. Additionally, they studied the factors encouraging girls in cybersecurity, emphasizing the importance of inclusivity and diversity in cybersecurity awareness and education. The proliferation of Internet of Things (IoT) devices introduces new cybersecurity challenges. Mikko et al [22] discussed the vulnerabilities associated with IoT devices. As Kosovo embraces digital transformation, it must consider the security implications of IoT adoption. This research serves as a reminder of the evolving nature of cybersecurity threats.

Minović et al.[23] examined cybersecurity in the Western Balkans, identifying policy gaps and cooperation opportunities. Kosovo's integration into regional

[19] Cesarec, I.: Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment–Overview of Cyber-security legislation and implementation in SEE Countries, *Annals of Disaster Risk Sciences: ADRS*, 3(1) 2020.

[20] European Commission: Instrument for pre-accession assistance (IPA II) 2014-2020, multi-country: EU support to cybersecurity capacity building in the Western Balkans, Brussels 2019.

[21] Maraj, A., Sutherland, C., Butler, W.: The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo, in Eze, T., Speakman, L., Onwubiko, C. (eds.) *Proceeding 20th European Conference on Cyber Warfare and Security*, Chester: University of Chester, 2021, p. 260.

[22] Mikko, H., Nyman, L.: The internet of (vulnerable) things: On hypponen's law, security engineering, and IoT legislation, *Technology Innovation Management Review*, 7(4) 2017, pp. 5-11.

[23] Minović, A. et al.: Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, Geneva: DiploFoundation, 2016.

cybersecurity efforts is essential for collective resilience. The study provides insights into the broader regional context of cybersecurity. Tasevski[24] discussed Macedonia's path towards cybersecurity, offering lessons and parallels for Kosovo. Cross-country experiences in the Western Balkans can inform Kosovo's cybersecurity strategy and awareness campaigns.

Tasevski[25] delved into the importance of IT and cybersecurity awareness-raising campaigns. The study emphasizes the role of education and awareness initiatives in building a cyber-resilient society. Kosovo can draw upon such insights to design effective awareness campaigns. William et al.[26] provided a macro perspective on cybersecurity capacity in African countries. While Kosovo is not in Africa, this research underscores the importance of evaluating a nation's capacity comprehensively. Kosovo's cybersecurity awareness efforts should align with its capacity-building initiatives.

Shappie et al. [27] researched how personality traits can predict cybersecurity behaviour. Understanding the role of individual psychology in cybersecurity awareness can aid in tailoring awareness campaigns to resonate with different personality types. Moreover, the role of education in cybersecurity awareness cannot be overstated. Khader et al.[28] proposed a cybersecurity awareness framework for academia. This framework can provide valuable insights into designing educational programs that equip students with the necessary cybersecurity knowledge and skills. Additionally, addressing the specific threat of phishing scams is crucial in any cybersecurity awareness initiative.

3. DATA AND METHODOLOGY

To investigate the role of cybersecurity awareness among citizens, a quantitative or numerical methodology was employed. This type of methodology is applicable for studying psychological, social, and economic processes through the exploration of numerical models. Quantitative research gathers a range of

[24] Tasevski, P.: Macedonian Path Towards Cybersecurity, *Information & Security*, 32(2) 2015, pp. 1-10.

[25] Tasevski, P.: IT and cyber security awareness-raising campaigns, *Information & Security*, 34(1) 2016, pp. 7-22.

[26] William, D.H. et al.: Cybersecurity capacity: does it matter?, *Journal of Information Policy*, 9 2019, pp. 280-306.

[27] Shappie, A. T., Dawson, C. A., Debb, S. M.: Personality as a predictor of cybersecurity behaviour, *Psychology of Popular Media*, 9(4) 2020, pp. 475.

[28] Khader, M., Karam, M., Fares, H.: Cybersecurity awareness framework for academia, *Information*, 12(10) 2021, pp. 417.

numerical data, with some of the numerical data being quantitative, while in other cases, numerical structures are created by the researcher (e.g., on a scale from 1 to 5). To carry out this research, surveys were used, and the process of sample selection, data collection instrument, and statistical analysis is explained below.

The primary data for this research was obtained through a structured survey conducted among a representative sample of Kosovo citizens. The survey sought to elicit comprehensive insights into citizens' cybersecurity awareness, knowledge, and practices. Additionally, existing datasets and reports related to cybersecurity and awareness in Kosovo were consulted to provide context and reinforce the analysis.

4. RESEARCH INSTRUMENT

A meticulously crafted survey questionnaire was administered to respondents. This questionnaire was developed based on established cybersecurity awareness and knowledge assessment frameworks. It featured a mix of closed-ended and open-ended questions to encompass a wide range of responses and insights. The survey instrument underwent a pilot phase to ensure clarity and relevance.

In parallel with the survey, semi-structured interviews were conducted with key stakeholders in the field of cybersecurity in Kosovo. These interviews aimed to acquire qualitative insights and context regarding the challenges and opportunities associated with cybersecurity awareness in the country.

Data collection occurred over a designated timeframe, during which survey questionnaires were distributed electronically and in person. The research team collaborated closely with local partners and organizations to secure a diverse and representative sample of participants, encompassing different demographics, regions, and educational backgrounds.

The data garnered from the survey and interviews underwent rigorous analysis to address the research hypotheses and objectives. The following analytical techniques were employed:

1. *Descriptive Analysis*: Descriptive statistics were harnessed to summarize and present key findings regarding citizens' cybersecurity awareness, knowledge, and practices.

2. *Inferential Analysis*: Inferential statistics, encompassing correlation analysis and ANOVA testing, were utilized to investigate relationships among variables and to evaluate the research hypotheses. These statistical analyses facilitated the assessment of the significance of factors influencing cybersecurity awareness.
3. *Qualitative Analysis*: Qualitative data derived from open-ended survey questions and interviews underwent content analysis. This process entailed identifying recurring themes, patterns, and qualitative insights pertaining to the barriers and challenges associated with promoting cybersecurity awareness.

5. ETHICAL CONSIDERATIONS

The research adhered unwaveringly to ethical guidelines and upheld the privacy and anonymity of survey respondents. Informed consent was meticulously secured from all participants, and their data was treated with utmost confidentiality.

By adopting a mixed-methods approach that seamlessly integrates quantitative and qualitative data, this research aspired to furnish a full comprehension of the landscape of cybersecurity awareness among Kosovo citizens. Moreover, it endeavored to proffer actionable recommendations for fortifying cybersecurity education and readiness within the region.

6. RESEARCH RESULTS

6.1. DEMOGRAPHIC DATA

The demographic data provides a detailed profile of the survey participants, encompassing factors such as age, gender, education, and geographic location (Place of Residence). These demographics offer valuable insights into the composition of the study’s sample and facilitate the identification of potential variations in cybersecurity awareness among different population segments.

Table 1. Demographic Data of Participants

Question	**Frequency**	**Percentage**
Gender	**N**	**%**
Female	68	45.3
Male	82	54.7
Age Group	**N**	**%**
18-30	52	34.7
31-40	77	51.3
41-50	19	12.7
>60	2	1.3
Educational Level	**N**	**%**
High School	32	21.3
Bachelor's Degree	60	40.0
Master's Degree	44	29.3
Doctorate	14	9.3
Place of Residence	**N**	**%**
Rural	48	32.0
Urban	102	68.0

Source: Authors' calculation

Table 1 provides an overview of the demographic characteristics of the research participants. As indicated in the Table 1, the study exhibits a predominantly male participation rate, with 82 individuals, accounting for 54.7% of the total respondents. Furthermore, a substantial portion of the participants, comprising 77 individuals or 51.3%, falls within the age range between 31 and 40. Regarding educational background, the results illustrate that the majority of respondents have attained a Bachelor's degree, with 60 individuals, representing 40% of the sample population, reporting this level of education. Additionally, the surveyed participants predominantly originate from urban areas, with 102 respondents, constituting 68% of the research sample from urban locales.

6.2. CITIZENS' AWARENESS OF CYBERSECURITY

This subsection delves into the outcomes of the statements administered to the research participants concerning their awareness of cybersecurity. Specifically, participants were presented with four statements, and the ensuing tables provide a summary of the results associated with these statements.

Table 2. Need for Cybersecurity Education Programs

Statement (Question)	Frequency	Percentage (%)	Mean	Standard Deviation
The creation of cybersecurity education programs through schools and higher education institutions is necessary to increase citizens' awareness and sensitivity to cyber threats.				
Strongly Disagree	0	0.0	3.17	0.497
Disagree	8	5.3		
Agree	109	72.7		
Strongly Agree	33	22.0		
The preparation and updating of educational materials for cybersecurity are necessary, adapting them for the specific audience of citizens and making them accessible and attractive				
Strongly Disagree	2	1.3	3.14	0.531
Disagree	4	3.0		
Agree	114	75.0		
Strongly Agree	31	20.7		

Source: Authors' calculation

Table 2 displays the outcomes related to citizens' awareness of cybersecurity, with a particular focus on the statement addressing the need for cybersecurity education programs. In the first statement, which reads, "The creation of cybersecurity education programs through schools and higher education institutions is necessary to increase citizens' awareness and sensitivity to cyber threats," an overwhelming majority of study participants (94.7%) expressed agreement with this assertion. Similarly, in the second statement, "The preparation and updating of educational materials for cybersecurity are necessary, adapting them for the specific audience of citizens and making them accessible and attractive," the majority of respondents (93.7%) also concurred with this statement.

Hence, based on the results of the two aforementioned statements, it is evident that citizens in the Republic of Kosovo highly endorse the necessity of establishing cybersecurity education programs, with an emphasis on their provision by educational institutions. Furthermore, respondents recognize the importance of keeping educational materials up-to-date to effectively address the rapidly evolving nature of cybersecurity.

Table 3. Promotion and Campaigns Regarding Cybersecurity

Statement (Question)	Frequency	Percentage (%)	Mean	Standard Deviation
Promoting cybersecurity awareness through information campaigns and public campaigns to encourage citizens to take necessary measures to protect themselves from cyber threats is necessary.				
Strongly Disagree	2	1.3	3.25	0.422
Disagree	2	1.3		
Agree	115	76.7		
Strongly Agree	31	20.7		
It is essential to create online platforms and informative resources to provide practical guidance and advice on cybersecurity that citizens can research and consult to enhance their knowledge and applicability.				
Strongly Disagree	2	1.3	3.07	0.506
Disagree	8	5.3		
Agree	117	78.0		
Strongly Agree	23	15.3		

Source: Authors' calculation

Table 3 displays the outcomes related to citizens' awareness of cybersecurity, with a specific focus on the results concerning the statement about the establishment of online platforms and informative resources to promote cybersecurity. In the first statement, "Promoting cybersecurity awareness through information campaigns and public campaigns to encourage citizens to take necessary measures to protect themselves from cyber threats is necessary," an overwhelming majority of participants (97.4%) express agreement with this statement. In the second statement, "It is essential to create online platforms and informative resources to provide practical guidance and advice on cybersecurity that citizens can research and consult to enhance their knowledge and applicability," a substantial majority (93.3%) also concur.

Based on the outcomes of these two statements, it is evident that the citizens of the Republic of Kosovo consider the promotion of cybersecurity awareness to be of utmost importance. This promotion should be carefully planned by relevant institutions and encompass diverse campaigns with extensive citizen involvement. Furthermore, the development of readily accessible online platforms for cybersecurity advice and guidance is deemed crucial to assist citizens in addressing cybersecurity threats effectively.

6.3. PUBLIC KNOWLEDGE REGARDING CYBERSECURITY

After presenting the results of citizens' awareness of cybersecurity, this section focuses on citizens' level of knowledge about cybersecurity. Four statements were presented to gauge citizens' understanding of this domain, and the ensuing tables provide a summary of these results.

Table 4. Proficiency in Cybersecurity Knowledge

Statement (Question)	**Frequency**	**Percentage (%)**	**Mean**	**Standard Deviation**
There are skills among the citizens of Kosovo in basic cybersecurity knowledge, such as creating secure passwords, identifying hidden threats, and knowing how to report cyber incidents.				
Strongly Disagree	18	12.0	2.48	0.721
Disagree	44	29.3		
Agree	86	57.3		
Strongly Agree	2	1.3		
There is knowledge among citizens about general cybersecurity risks such as phishing attacks, malware, and online identity theft.	**N**	**%**	**Mean**	**Std.Dev**
Strongly Disagree	28	18.7	2.19	0.772
Disagree	71	47.3		
Agree	46	30.7		
Strongly Agree	5	3.3		

Source: Authors' calculation

Table 4 presents the outcomes related to citizens' comprehension of cybersecurity, with a specific focus on their knowledge of secure passwords, phishing, malware, and other related concepts. In the first statement, “There are skills among the citizens of Kosovo in basic cybersecurity knowledge, such as creating secure passwords, identifying hidden threats, and knowing how to report cyber incidents,” only 58.6% of participants in the study agree with this statement. Respondents were also presented with the statement “Citizens know general cyber threats such as phishing attacks, malware, and identity abuse on the internet,” where, according to the data presented in the table above, only 34% of participants in the research sample agree with the presented statement.

Therefore, based on the results of the two statements presented above, citizens of the Republic of Kosovo do not possess extensive knowledge about secure passwords and the proper way to report various cyber incidents. They also have limited knowledge about cyber threats such as phishing and malware.

Table 5. Understanding Cybersecurity Best Practices and Incident Response

Statement (Question)	Frequency	Percentage (%)	Mean	Standard Deviation
Citizens have information about good cybersecurity practices such as using antivirus programs and keeping the operating system up to date.				
Strongly Disagree	27	18.0	2.11	0.71
Disagree	82	54.7		
Agree	38	25.3		
Strongly Agree	3	2.0		
There is a high level of preparedness among citizens to deal with cyber incidents and protect their personal and financial data in the digital environment.				
Strongly Disagree	29	19.3	2.2	0.819
Disagree	71	47.3		
Agree	41	27.3		
Strongly Agree	9	6.0		

Source: Authors’ calculation

Table 5 offers insights into citizens’ familiarity with cybersecurity best practices and their readiness to tackle cyber incidents. It centers on their awareness of risk reduction practices and their preparedness for dealing with cyberattacks.

Surprisingly, only 27.3% of the research sample agreed with the first statement: *"Citizens possess knowledge about cybersecurity best practices, such as the utilization of antivirus programs and regular system updates."* Similarly, only 33.3% of respondents concurred with the second statement: "There is a high level of preparedness among citizens to address cyber incidents and safeguard their personal and financial digital assets.". These outcomes underscore a significant deficit in citizens' understanding of essential cybersecurity best practices, such as antivirus software usage.

6.4. IDENTIFYING BARRIERS AND CHALLENGES IN CYBERSECURITY

In this section, we delve into the barriers and challenges that citizens face in the realm of cybersecurity. We have presented the results of four specific statements designed to uncover these hurdles, and their corresponding outcomes are detailed in the tables below.

Table 6. Lack of Resources and Materials on Cybersecurity

Statement (Question)	Frequency	Percentage (%)	Mean	Standard Deviation
There is a lack of awareness and understanding of the risks of cyber threats on the part of citizens, which can be addressed through continuous information and education campaigns.				
Strongly Disagree	7	4.7	2.8	0.531
Disagree	18	12.0		
Agree	123	82.0		
Strongly Agree	2	1.3		
There is a lack of appropriate educational resources and materials to encourage and assist citizens in taking measures for cybersecurity.				
Strongly Disagree	2	1.3	2.93	0.473
Disagree	16	10.7		
Agree	122	81.3		
Strongly Agree	10	6.7		

Source: Authors' calculation

Table 6 provides insights into citizens' perspectives regarding barriers and challenges related to cybersecurity. This table encapsulates the findings of statements concerning cyber threats awareness and the availability of educational materials. In the first statement, "The lack of awareness and understanding of cyber threat risks among citizens, which can be addressed through continuous awareness and educational campaigns," a significant majority (83.3%) of respondents agreed with this assertion. The second statement, "There is a deficiency in suitable educational resources and materials to motivate and guide citizens in taking cybersecurity precautions," also garnered concurrence from the majority (88%) of respondents.

Hence, the results from these two statements underscore the considerable risks that citizens in the Republic of Kosovo perceive from cyber threats, alongside substantial challenges related to the accessibility of suitable resources and educational materials aimed at encouraging cybersecurity measures.

Table 7. Lack of institutional support and citizen response

Statement (Question)	**Frequency**	**Percentage (%)**	**Mean**	**Standard Deviation**
There is a noticeable lack of collaboration and effective coordination among government institutions, non-governmental organizations, and the private sector to address cybersecurity challenges and promote widespread awareness.				
Strongly Disagree	2	1.3	3	0.384
Disagree	5	3.3		
Agree	134	89.3		
Strongly Agree	9	6.0		
There is a lack of emphasized sensitivity and responsiveness of citizens to cyber incidents.				
*Strongly Disagre*e	9	6.0	2.97	0.649
Disagree	7	4.7		
Agree	114	76.0		
Strongly Agree	20	13.3		

Table 7 furnishes insights into citizens' views on the obstacles and issues associated with institutional support and citizen response in cybersecurity. The table encapsulates the results of statements concerning collaboration among government bodies, non-governmental organizations, and the private sector, as well as citizens' sensitivity and responsiveness to cyber incidents.

In the first statement, "There is a pronounced lack of collaboration and meaningful coordination among government institutions, non-governmental organizations, and the private sector to address cybersecurity challenges and promote widespread awareness," an overwhelming majority (95.3%) of respondents concurred. The second statement, "There is a noticeable lack of sensitivity and responsiveness among citizens to cyber incidents," also resonated with a significant majority (89.3%) of respondents.

Therefore, based on the outcomes of these two statements, citizens of the Republic of Kosovo believe that there is a notable dearth of collaborative efforts among cybersecurity-related institutions and a noticeable deficit in citizen responsiveness to cyber incidents.

6.5. COMPARATIVE ANALYSIS OF INDICATORS

Following the presentation of results from the three core indicators (Awareness, Information, and Challenges), we proceed to compare these indicators to discern their relative strengths.

Figure 1. Comparative Analysis of Indicators

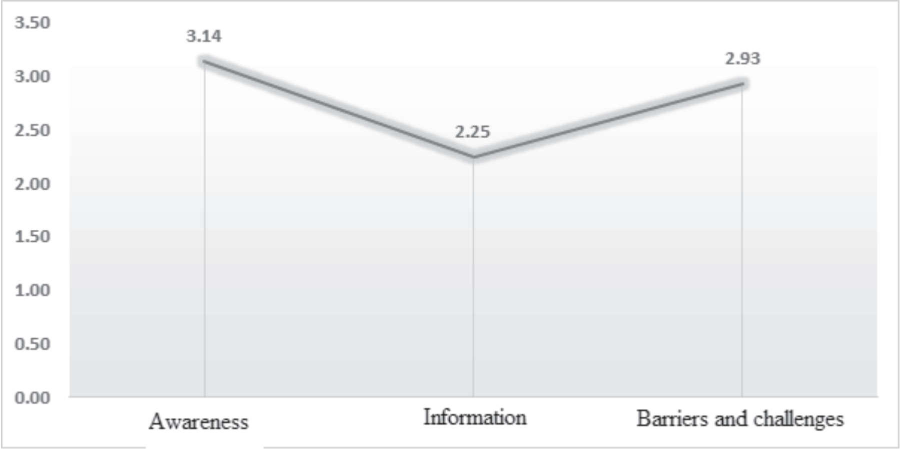

Figure 1, as displayed above, offers a comparative overview of the three indicators. The figure indicates that the citizens' awareness indicator boasts the highest value (3.14), followed by the barriers and challenges indicator (2.93), while the information indicator lags behind with the lowest value (2.25). This comparison provides valuable insights into the relative standing of these indicators. To further elucidate their relationships, we present a correlation matrix analysis in the subsequent section.

6.6. CORRELATION ANALYSIS

In this section, we conduct a correlation analysis to explore the relationships between the variables under study. Correlation is a statistical tool used to assess the associations between two or more variables, which can be positive, negative, or negligible. A positive correlation implies that two variables change in the same direction, meaning that as one variable increases, the other also increases. Conversely, a negative correlation suggests that two variables move in opposite directions, where an increase in one leads to a decrease in the other. To quantify the degree of correlation, we employ the Pearson correlation coefficient, which ranges from -1 to 1. Values close to -1 indicate a strong negative correlation, values near 1 indicate a strong positive correlation, while a value of 0 indicates a lack of linear correlation between the variables.[29]

Table 8. Correlation Matrix

		Awareness	**Information**	**Barriers and Challenges**
Awareness	Pearson Correlation	1	.095	-.208*
	Sig. (2-tailed)		.245	.011
	N	150	150	150
Information	Pearson Correlation	.095	1	-.048
	Sig. (2-tailed)	-.245		.557
	N	150	150	150
Barriers and Challenges	Pearson Correlation	-.208*	.048	1
	Sig. (2-tailed)	.011	.557	
	N	150	150	150
*. Correlation is significant at the 0.05 level (2-tailed).				

The findings displayed in Table 8 reveal important correlations between the variables or indicators. Specifically:

- There is a positive correlation (r = 0.095) between citizens' awareness and their level of information. In simpler terms, as citizens' awareness increas-

[29] Gogtay, N.J., Thatte, U.M.: Principles of correlation analysis. Journal of the Association of Physicians of India 65 (3) 2017, pp. 78-81.

es, so does their level of information. Additionally, this positive correlation indicates that increased awareness is associated with fewer challenges and barriers when it comes to dealing with cyber threats.

- Conversely, there is a negative correlation (r = -0.208) between citizens' awareness and the barriers and challenges they face. In essence, higher awareness levels are linked to a reduction in perceived challenges and barriers regarding cyber threats.
- Furthermore, a negative correlation (r = -0.048) is between citizens' level of information and the challenges and barriers they encounter. This signifies that as citizens acquire more information about cyber threats, they tend to perceive fewer challenges and barriers in addressing these threats.

The results indicate that promoting citizens' awareness and delivering comprehensive information about cyber threats may lead to a reduction in the perceived challenges and barriers they face. This, in turn, has the potential to bolster their capacity to respond effectively to cyber threats.

6.7. ANALYSIS OF VARIANCE (ANOVA)

Following the correlation analysis, we proceed with an Analysis of Variance (ANOVA) to delve deeper into the significance of the variables and their interrelationships.

Table 9. Summary of ANOVA Results

Model Summary[b]						
	Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	
1		.425[a]	.551	.038	.42392	
ANOVA[a]						
	Model	Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	1.407	2	.703	3.913	.022[b]
	Residual	26.417	147	.180		
	Total	27.823	149			
Coefficients[a]						
	Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.320	.294		7.897	.000
	Informacionet	.059	.055	.086	4.064	.009
	Barrierat dhe Sfidat	-.234	.092	.204	2.533	.012
a) Dependent Variable: Awareness						

Figure 2. Regression Data Plot

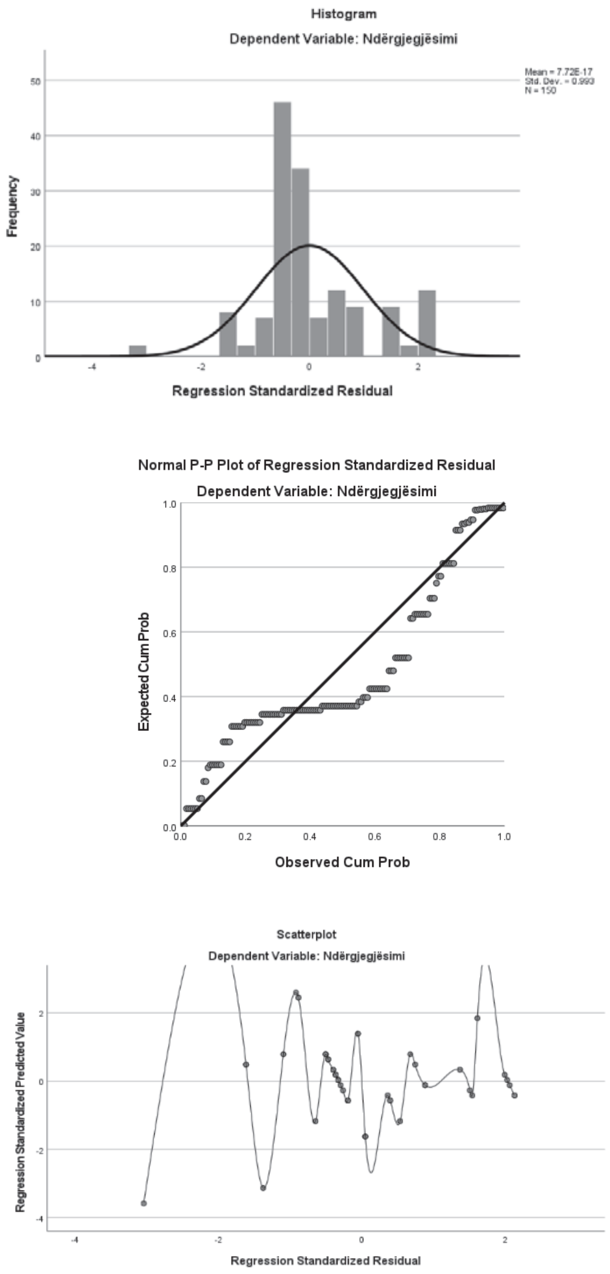

Table 9 provides an analysis of the ANOVA regression, based on the coefficient of determination (R-squared=0.551). We conclude that information, barriers, and challenges account for 55.1% of the variation in citizens' awareness, while the remaining portion is attributed to other variables affecting awareness but not included in the model. The regression is statistically significant, as indicated by the F-statistic of 3.91 and a P-value of 0.022. Consequently, the results presented in the regression analysis are both valid and reliable. We offer an interpretation of these findings below.

Information has a positive impact on citizens' awareness (B=0.059), signifying that for every 1 unit increase in the information variable, awareness increases by an average of 0.059 units. This coefficient is statistically significant, with a P-value (0.000) lower than the critical P-value (0.05).

Conversely, challenges and barriers have a negative impact on citizens' awareness (B= -0.234), indicating that for every 1 unit increase in the challenges and barriers variable, awareness decreases by an average of 0.234 units. This coefficient is also statistically significant, with a P-value (0.009) lower than the critical P-value (0.05).

As illustrated in Figure 2, the dependent variable of the study (awareness) exhibits a normal distribution of data, as depicted in the first section of the figure using a histogram.

6.8. HYPOTHESIS TESTING

H1: There is a high awareness among the citizens of the Republic of Kosovo regarding cyberattacks and cyber threats. – This hypothesis is accepted, given the high level of agreement with the four statements presented by citizens regarding their awareness. Additionally, the average of this indicator (3.14) was higher compared to the other indicators.

H2: There is a lack of general information about cybersecurity among citizens. – This hypothesis is accepted. As based on the presented statements, there is a high level of agreement in the research sample that there is a lack of information among citizens about cybersecurity. Additionally, the average of the information variable is the lowest (2.25) compared to the other presented variables.

H3: Citizens face numerous barriers and challenges in protecting themselves from cyberattacks. – This hypothesis is also accepted. In the presented statements, more than 80% of respondents agree that there are many challenges and barriers they face in terms of security and risks from various cyberattacks.

6.9. CONSISTENCY WITH FINDINGS FROM PREVIOUS RESEARCH

Our study's findings both align with and extend the existing body of research in the field of cybersecurity awareness, providing a deeper and more context-specific understanding of the unique setting of Kosovo. Our research echoes the perspective emphasized by Anwar et al.[30] on the importance of gender-sensitive approaches in cybersecurity awareness campaigns. Although gender-specific patterns were not our primary focus, our findings reveal variations in cybersecurity awareness and knowledge levels among different demographic groups. This underscores the need for tailored awareness programs to cater to the diverse needs and preferences of different population segments. The recognition of gender disparities in cybersecurity behaviour is consistent with the broader research landscape.

Our study aligns with the insights of Maraj et al.[31], who explored the challenges of cybersecurity education in developing countries, including Kosovo. We emphasize the necessity for tailored educational approaches and inclusivity in cybersecurity awareness and education. These findings underscore the pivotal role of educational initiatives in fostering a cyber-resilient society, which resonates with prior research.

Building on Bada[32], who placed emphasis on cybersecurity capacity assessments in evaluating a nation's readiness to address cyber threats, our research conducts such an assessment within the context of Kosovo. Our findings reveal specific challenges and priorities for the nation, underscoring the need for tailored cybersecurity awareness initiatives. This aligns with the broader recognition of national assessments as significant in the realm of cybersecurity research.

Acknowledging the impact of regional dynamics on a country's cybersecurity posture, as explored by Fotescu et al.[33], our research underscores the relevance of regional and international cybersecurity frameworks, especially within the Western Balkans context. This study recognizes the importance of a balanced

[30] Anwar, M. et al.: Gender difference and employees' cybersecurity behaviors, *Computers in Human Behavior*, 69 2017, pp. 437-443.

[31] Maraj, A., Sutherland, C., Butler, W.: The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo, in Eze, T., Speakman, L., Onwubiko, C. (eds.) *Proceeding 20th European Conference on Cyber Warfare and Security*, Chester: University of Chester, 2021, p. 260.

[32] Bada, M.: Cybersecurity Capacity Assessment of the Republic of Kosovo, *SSRN*, 2015.

[33] Fotescu, A., Chihaia, M. S.: Albania's cybersecurity pivot: Between Western architectures and great power competition, in Scott N. R., Mary M. (eds.): *Routledge Companion to Global Cyber-Security Strategy*, Routledge, London, 2021, pp. 26-35.

approach that considers both regional and global cybersecurity initiatives. These insights are consistent with the emphasis on international cooperation evident in previous research.

Drawing parallels with Dawson[34] and Shappie et al.[35] research on the role of personality traits in predicting cybersecurity behaviour, our study highlights the relationship between citizens' awareness and their effectiveness in responding to cyber threats. These findings underscore the significance of addressing psychological factors in cybersecurity awareness campaigns, aligning with the insights of previous research.

In alignment with Cesarec's[36] examination of cybersecurity legislation in Southeast European countries, our research recognizes the pivotal role of robust legal frameworks in fostering a culture of cybersecurity awareness and compliance. The consistency of these findings reinforces the significance of legal aspects in the domain of cybersecurity research.

7. CONCLUSION, LIMITATIONS AND FUTURE DIRECTIONS

This study provides valuable insights into the landscape of cybersecurity awareness among citizens in the Republic of Kosovo, utilizing a quantitative methodology to explore various dimensions of this critical domain. The research aimed to illuminate citizens' awareness, knowledge, and challenges related to cybersecurity, with the ultimate goal of enhancing cybersecurity education and preparedness.

The findings of this research have revealed several significant insights. The study identified a high level of awareness among citizens regarding cyber threats and the necessity of cybersecurity education programs, underscoring the relevance of cybersecurity in the digital age. However, there remains room for improvement in specific areas of knowledge and best practices. Variations in cybersecurity awareness and knowledge across different demographic groups were observed, emphasizing the need for tailored awareness programs to address the diverse needs and preferences of various population segments.

[34] Dawson, M.: *Hyper-connectivity: Intricacies of national and international cyber securities*, doctoral dissertation, London: London Metropolitan University, 2017.

[35] Shappie, A. T., Dawson, C. A., Debb, S. M.: Personality as a predictor of cybersecurity behaviour, *Psychology of Popular Media*, 9(4) 2020, pp. 475.

[36] Cesarec, I.: Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment–Overview of Cyber-security legislation and implementation in SEE Countries, *Annals of Disaster Risk Sciences: ADRS*, 3(1) 2020.

Kosovo's citizens encounter various challenges and barriers in safeguarding themselves against cyber threats, including a lack of awareness and understanding of cyber risks, limited access to educational resources, and insufficient institutional collaboration. Addressing these challenges is pivotal for strengthening cybersecurity awareness and resilience. The research highlights the crucial role of educational initiatives in nurturing a cyber-resilient society, advocating for tailored approaches, inclusivity, and continuous awareness campaigns as essential components of effective cybersecurity education. Furthermore, recognizing the influence of regional dynamics and international frameworks, particularly within the Western Balkans context, underscores the importance of a balanced approach that considers both regional and global cybersecurity initiatives. Robust legal frameworks play an indispensable role in fostering a culture of cybersecurity awareness and compliance, making cybersecurity legislation development and enforcement vital for enhancing cybersecurity practices and safeguarding digital assets.

Based on these findings, several implications and recommendations emerge. It is imperative to develop customized cybersecurity awareness programs that accommodate the diverse needs of different demographic groups to ensure inclusivity and efficacy. Educational materials on cybersecurity should be made readily accessible and engaging, with a focus on offering practical guidance and advice to citizens. Promoting collaboration among government institutions, non-governmental organizations, and the private sector is essential to effectively address cybersecurity challenges. Integrating psychological factors into cybersecurity awareness campaigns can effectively address citizens' attitudes and behaviour regarding cybersecurity. Continuously strengthening legal frameworks related to cybersecurity is critical to ensure compliance and effectively protect digital assets. This research advances the understanding of cybersecurity awareness in Kosovo and outlines areas for improvement. By addressing the identified challenges and implementing the recommended strategies, Kosovo can work towards building a more cyber-resilient society and contribute to global efforts to ensure a secure digital environment.

While this research contributes to the understanding of cybersecurity awareness in Kosovo, several limitations should be acknowledged. The study primarily focused on quantitative data, with limited exploration of qualitative insights, potentially limiting the depth of understanding. The research sample may not fully represent the diversity of the population, which could impact the generalizability of the findings. Furthermore, the cross-sectional design of the study provides a snapshot of awareness at a specific point in time, limiting the ability to capture changes and trends over time. Despite efforts to ensure a diverse sample, there may still be unexamined factors contributing to demographic variations in awareness. Recognizing these limitations is crucial for accurately interpreting the study's findings and guiding future research endeavors in the field of cybersecurity awareness.

Looking ahead, several promising avenues for future research in the realm of cybersecurity awareness among citizens in Kosovo emerge. Longitudinal studies can track the evolution of cybersecurity awareness over time, providing insights into the effectiveness of awareness programs and educational initiatives. Deeper demographic analysis can delve into variations in awareness among different population segments, uncovering underlying factors. Behavioural studies can bridge the gap between awareness and actual cybersecurity practices, identifying implementation barriers. Comparative studies with neighboring countries can offer insights into regional dynamics, fostering cross-border collaboration. Evaluating the impact of specific educational programs and campaigns can guide evidence-based strategies. Exploring the influence of emerging technological trends and psychological factors on cybersecurity behaviour is warranted. Additionally, investigating international collaboration opportunities, analyzing cybersecurity policies, assessing economic impacts, and examining public-private partnerships will contribute to a more comprehensive understanding of cybersecurity awareness in Kosovo.

LITERATURE

1. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L.: Gender difference and employees' cybersecurity behaviors, *Computers in Human Behavior,* 69 2017, pp. 437-443.
   - DOI: https://doi.org/10.1016/j.chb.2016.12.040
2. Bada, M.: Cybersecurity Capacity Assessment of the Republic of Kosovo. *SSRN,* 2015.
   - DOI: https://doi.org/10.2139/ssrn.3658214
3. Bada, M., Solms, B. V., Agrafiotis, I.: Reviewing national cybersecurity awareness in Africa: an empirical study, *Apollo - University of Cambridge Repository*, 2019.
   - DOI: https://doi.org/10.17863/cam.40856
4. Bahiti, R., Josifi, J.: Towards a more resilient cyberspace: the case of Albania, *Information & Security: An International Journal*, 32 2015, pp. 120-130.
   - DOI: https://doi.org/10.11610/isij.3210
5. Butavicius, M. A., Taib, R., Han, S. J.: Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails, *Computers & Security,* 123 2022, pp. 102937.
   - DOI: https://doi.org/10.1016/j.cose.2022.102937

6. Cesarec, I.: Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment–Overview of Cyber-security legislation and implementation in SEE Countries. *Annals of Disaster Risk Sciences: ADRS*, 3(1) 2020.
   – DOI: https://doi.org/10.51381/adrs.v3i1.45
7. Dawson, M.: *Hyper-connectivity: Intricacies of national and international cyber securities*, doctoral dissertation, London: London Metropolitan University, 2017, https://repository.londonmet.ac.uk/id/eprint/1282.
8. European Commission: Instrument for pre-accession assistance (IPA II) 2014-2020, multi-country: EU support to cybersecurity capacity building in the Western Balkans, Brussels 2019, https://neighbourhood-enlargement.ec.europa.eu/document/download/1fb8ced5-0608-4083-a2cf-39d87426e302_en.
9. Fotescu, A., Chihaia, M. S.: Albania's cybersecurity pivot: Between Western architectures and great power competition, in Scott N. R., Mary M. (eds.): *Routledge Companion to Global Cyber-Security Strategy*, London: Routledge, 2021, pp. 26-35.
   – DOI: https://doi.org/10.4324/9780429399718
10. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., Linkov, I.: Multicriteria decision framework for cybersecurity risk assessment and management, *Risk Analysis*, 40(1) 2017, pp. 183-199.
    – DOI: https://doi.org/10.1111/risa.12891
11. Gogtay, N. J., Thatte, U. M.: Principles of correlation analysis, *Journal of the Association of Physicians of India*, 65(3) 2017, pp. 78-81.
12. Jica, H.: Cyber Security and National Security Awareness Initiatives in Albania: A Synergy Approach, *Mediterranean Journal of Social Sciences*, 4(10) 2013, pp. 614-622.
    – DOI: https://doi.org/10.5901/mjss.2013.v4n10p614
13. Khader, M., Karam, M., Fares, H.: Cybersecurity awareness framework for academia, *Information* 12(10) 2021, pp. 417.
    – DOI: https://doi.org/10.3390/info12100417
14. Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., Ignatuschtschenko, E.: Comprehensive study on cybercrime, New York: United Nations, 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
15. Maraj, A., Sutherland, C., Butler, W.: The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo, in Eze, T., Speakman, L., Onwubiko, C. (eds.) *Proceeding 20th European Conference on Cyber Warfare and Security*, Chester: University of Chester, 2021.
    – DOI: https://doi.org/10.34190/EWS.21.003
16. Mark, M. S.: *An analysis of factors influencing phishing threat avoidance behavior: a quantitative study, School of Business and Technology*, doctoral dissertation, Capella University, March 2021.

17. Mikko, H., Nyman, L.: The internet of (vulnerable) things: On hypponen's law, security engineering, and IoT legislation, *Technology Innovation Management Review*, 7(4) 2017, pp. 5-11.
    – DOI: https://doi.org/10.22215/timreview/1066

18. Minović, A., Abusara, A., Begaj, E., Erceg, V., Tasevski, P., Radunović, V., Klopfer, F.: Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, Geneva*:* DiploFoundation,, 2016.

19. Moci, E.: Cybersecurity Awareness in Albania. *European Journal of Social Science Education and Research*, 8(3) 2021, pp. 112-117.
    – DOI: https://doi.org/10.26417/778wjv40q

20. Mori, S., Goto, A.: Reviewing national cybersecurity strategies, *Journal of disaster research*, 13(5) 2018, pp. 957-966.
    – DOI: https://doi.org/10.20965/jdr.2018.p0957

21. Nagyfejeo, E., Puello Alfonso, S.: Cybersecurity Capacity Review Bosnia and Herzegovina, *SSRN*, 2019.
    – DOI: https://doi.org/10.2139/ssrn.3658404

22. Poposka, V.: The Urge for Comprehensive Cyber Security Strategies in the Western Balkans, *Information & Security,* 34(1) 2016, pp. 25-36.
    – DOI: https://doi.org/10.11610/isij.3402

23. Radunović, V.: DDoS - available weapon of mass disruption. *Proceedings of the 21st Telecommunications Forum Telfor (TELFOR)*, Belgrade: Curran Associates Inc., 2014, pp. 5-8.
    – DOI: https://doi.org/10.1109/TELFOR.2013.6716157

24. Shappie, A. T., Dawson, C. A., Debb, S. M.: Personality as a predictor of cybersecurity behaviour, *Psychology of Popular Media*, 9(4) 2020, pp. 475.
    – DOI: https://doi.org/10.1037/ppm0000247

25. Stewart, K. A., Segars, A. H.: An empirical examination of the concern for information privacy instrument, *Information systems research,* 13(1) 2002, pp. 36-49.
    – DOI: https://doi.org/10.1287/isre.13.1.36.97

26. Tasevski, P.: Macedonian Path Towards Cybersecurity, *Information & Security,* 32(2) 2015, pp. 1-10.
    – DOI: https://doi.org/10.11610/isij.3204

27. Tasevski, P.: IT and cyber security awareness-raising campaigns, *Information & Security*, 34(1) 2016, pp. 7-22.
    – DOI: https://doi.org/10.11610/isij.3401

28. William, D. H., Creese, S., Shillair, S., Bada, M.: Cybersecurity capacity: does it matter?, *Journal of Information Policy*, 9 2019, pp. 280-306.
    – DOI: 10.5325/jinfopoli.9.2019.0280