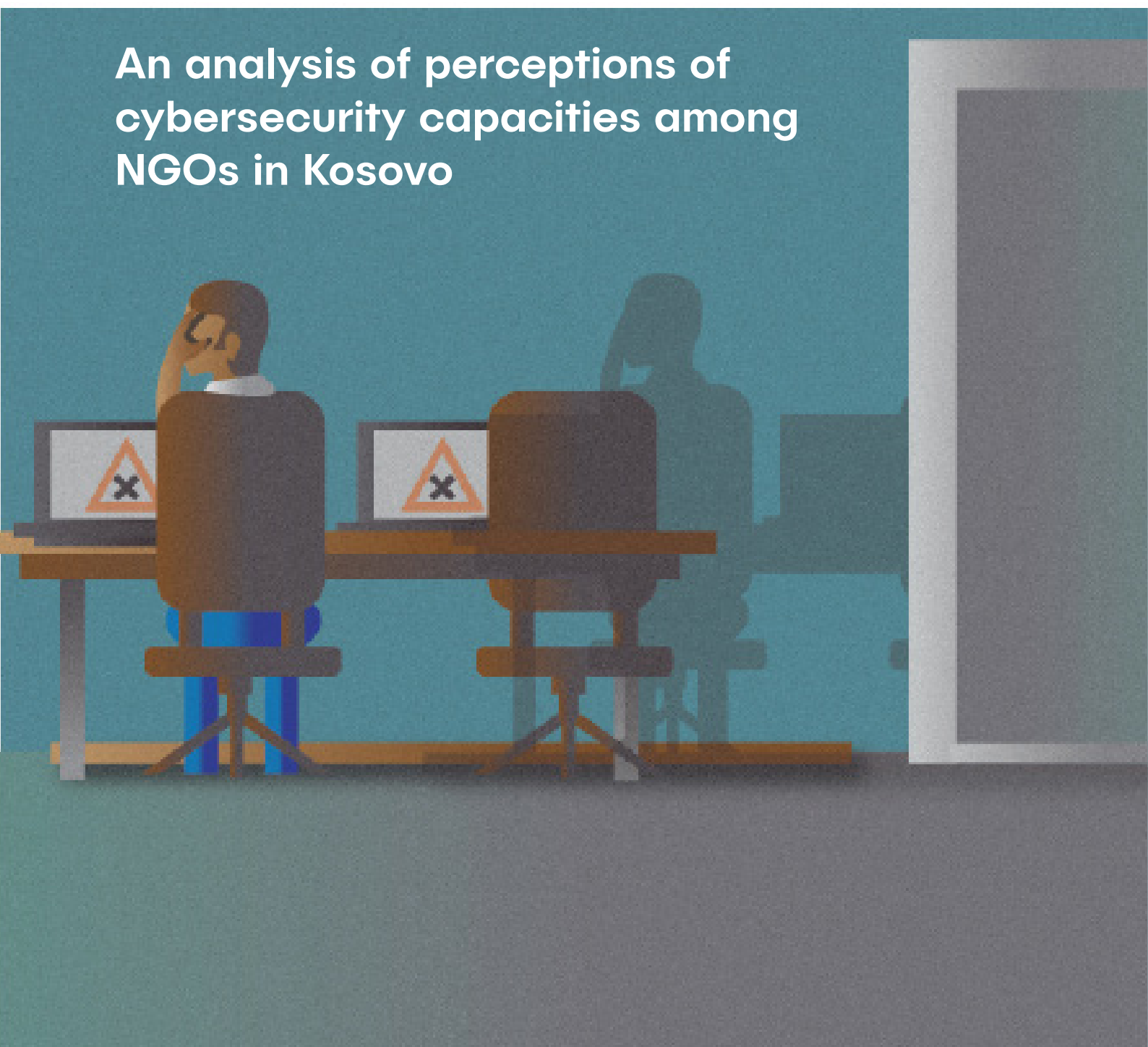
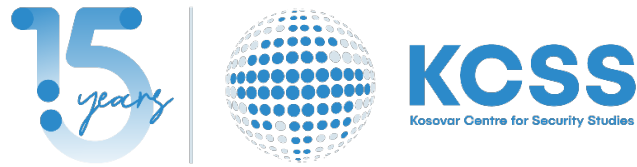


ARE NON-GOVERNMENTAL ORGANIZATIONS PREPARED TO DEAL WITH CYBERTHREATS?

An analysis of perceptions of cybersecurity capacities among NGOs in Kosovo





Author: Donika Elshani

The following report is published in the framework of the “Greater Internet Freedom” project, implemented by Internews and BIRN Hub, with the support of the United States Agency for International Development (USAID).

Supported by:



**Emerging
Threats
Programme**

ARE NON-GOVERNMENTAL ORGANIZATIONS PREPARED TO DEAL WITH CYBERTHREATS?

**AN ANALYSIS OF PERCEPTIONS OF CYBERSECURITY
CAPACITIES AMONG NGOs IN KOSOVO**

August, 2023

TABLE OF CONTENTS

ABOUT PROGRAMME 1

EXECUTIVE SUMMARY 2

INTRODUCTION 3

METHODOLOGY 4

 Cybersecurity Indicators for CSOs 5

BACKGROUND 7

MAIN FINDINGS 9

RECOMMENDATIONS 15

ANNEX 1..... 16

ENDNOTES..... 23

ABOUT THE PROGRAMME:

The Emerging Threats Programme has been designed as a response to evolving domestic, regional, and international security threats. Its primary aim is to consolidate and provide a better understanding of emerging threats that consistently move away from traditional conceptualizations of security challenges. Given the extent of evolving threats related to cybersecurity and disinformation, this programme seeks to build upon internal organizational capacities to provide evidence-based expertise to operationalize institutional responses to these challenges. Evidence-based research in relation to the Emerging Threats Programme focuses on: critical infrastructure, cybersecurity, disinformation and hybrid security challenges. While needs assessment(s), monitoring and research remain fundamental actions to be developed in the programme, KCSS aims to utilize expertise generated to directly enhance the capacities of executive institutions and agencies to respond effectively to cybersecurity challenges and disinformation. The programme will be developed through:

- **State of the art evidence-based research related to emerging threats such as cybersecurity, critical infrastructure protection, hybrid threats and disinformation;**
- **Awareness-raising campaigns and targeted advocacy to improve the level of understanding of challenges related to cybersecurity, critical infrastructure protection, hybrid threats and disinformation in Kosovo;**
- **Awareness-raising campaigns and targeted advocacy to improve the level of understanding of challenges related to cybersecurity, critical infrastructure protection, hybrid threats and disinformation in Kosovo.**

EXECUTIVE SUMMARY

NGOs in Kosovo are increasingly relying on digital tools to conduct their work. From online correspondence via different applications, storing important organizational data on electronic devices and establishing an online presence through social media accounts, they are leveraging technology to streamline processes, improve communication, and engage with stakeholders. However, with the benefits of these digital tools come certain challenges and risks that, if left unaddressed, can undermine the effectiveness and security of NGOs and potentially even threaten their very existence. Malign actors are increasingly using the online sphere to perpetrate malicious activities, including stealing sensitive data, committing financial crimes, spreading falsehoods and hate speech, to name but a few.

The aim of this report is to provide a analysis of perceptions of key digital threats and digital capacity-building needs of the non-governmental sector in Kosovo. It seeks to fill the existing data gap by conducting an initial assessment of the key challenges faced by NGOs in terms of digital security and identifying their specific needs for enhancing their digital capacity.

The report draws on a quantitative survey conducted among 48 NGOs to assess their cybersecurity landscape. The findings reveal that NGOs in Kosovo face significant challenges in terms of their capacity to identify, mitigate, and respond to cyber threats. The analysis highlights a lack of adequate resources, expertise, and cybersecurity measures within these organizations to effectively tackle potential digital threats in the future. The lack of procedures and regulations to help guide and govern the management and prevention of cyber incidents and lack of incident response mechanisms, coupled with the fact that most survey respondents had never conducted any form of risk assessment relating to digital threats, leaves NGOs in Kosovo completely exposed to a myriad of risks and vulnerabilities associated with the online sphere.

The findings from this report show that NGOs in Kosovo face significant challenges in terms of their capacity to identify, mitigate, and respond to cyber threats. The analysis highlights a lack of adequate resources, expertise, and cybersecurity measures within these organizations to effectively tackle potential digital threats in the future. While NGOs appear to perceive cyber threats to be a real threat to their wellbeing, they are not proactively engaged in addressing and mitigating these risks. The findings from this analysis indicate a lack of security culture within the sector. The lack of procedures and regulations to help guide and govern the management and prevention of cyber incidents, coupled with the fact that most survey respondents have never conducted any form of risk assessment relating to digital threats, leaves NGOs in Kosovo completely exposed to a myriad of risks and vulnerabilities associated with the online sphere. Without a concrete incident response plan in place and without designated persons within the organization that are responsible for monitoring and responding to threats, these NGOs are left largely unprepared to handle potential breaches, which is likely to lead to delays, confusion, and inadequate response to cyber incidents. Finally, the lack of awareness among staff, which is exacerbated by the absence of training and awareness-raising campaigns, increases the risk that these individuals become victims of various cyberattacks. This not only causes damage to the organization but also affects the emotional and psychological wellbeing of the staff members themselves.

INTRODUCTION

As digital space becomes an ever-more integral element of contemporary modern societies, critical societal infrastructure, governmental services, the security sector, and citizens at large are increasingly dependent on interconnectivity and the global online network. Kosovo has one of the largest internet penetration rates in Europe.¹ In March 2023, Kosovo connected its last remaining village to high-speed broadband internet.² According to a 2022 report by the Kosovo Agency of Statistics, 98 percent of households in Kosovo have access to the internet, with internet usage being almost equally distributed across most age groups.³ Consequently, the majority of people's everyday activities, such as communication, information access, business transactions, and, to some extent, government services, have transitioned to the online realm.

Much like any other public or private entity nowadays, NGOs continuously exploit digital technologies and platforms to conduct a range of activities related to their work, including information sharing, community building, capacity and stakeholder engagements, advocacy, and resource mobilization.⁴ In this regard, NGOs in Kosovo constitute no exception. Organizations that have yet to establish an online presence, either through a dedicated organizational website or active social media pages, are scarce. The latter especially have become the main digital tools through which NGOs in Kosovo connect with their target audiences, disseminate information, and engage in meaningful dialogue.

However, as organizations rely increasingly on new digital tools to conduct their daily operations, their digital footprint grows and with it grows the digital risk they are prone to face. Cyberthreats affecting NGOs, including digital hacks aimed at causing operational disruptions, stealing data or disseminating disinformation, not only hinder daily organizational operations and target staff members, but also endanger NGOs' relationship with the communities they are involved in.⁵ This is especially critical when considering NGOs that work with marginalized individuals and groups, such as women and girls, children, torture and trauma victims/survivors, people with disabilities, members of the LGBTIQ+ community, ethnic minorities and individuals with mental health issues, among others. Any disruption to their operations or compromise of sensitive data can have severe consequences for the individuals who rely on their services and support.⁶

The digital threat landscape in Kosovo is evolving and comprises various risks and challenges that affect citizens, organizations, and the state apparatus. Kosovo has witnessed a series of cyberattacks that have had significant impacts on multiple sectors. Recently, Kosovo Telecom, the country's telecommunications provider, experienced a targeted cyberattack, resulting in disruptions to internet services for both mobile and landline users.⁷ Additionally, there have been instances of cyberattacks targeting government services, leading to challenges in internet connectivity and restricted access to certain government websites.⁸ The online realm has also turned into fertile ground for spreading hateful content. Digital spaces, including social media platforms, are increasingly being used for cyberbullying, particularly targeting vulnerable individuals such as women, youth, ethnic-minorities or members of the LGBTIQ+ community, to name a few.⁹ Lastly, the proliferation of fake news and disinformation has become even more prevalent, particularly in the aftermath of significant events such as the COVID-19 pandemic and the Russian invasion of Ukraine. Information from unreliable and suspicious sources during the pandemic often led to fear, panic, and social uncertainty among citizens,¹⁰ while Russian media narratives that seek to undermine Kosovo's statehood have intensified since the offset of the war in Ukraine.¹¹

METHODOLOGY

There is a notable scarcity of data concerning topics related to digital security in Kosovo, including information on what the most prevalent cyber threats faced by individuals and organizations are, how the latter respond to these threats and the mechanisms employed, if any, to mitigate against cyber incidents.

The aim of this report is to provide a analysis of perceptions of key digital threats and digital capacity-building needs of the non-governmental sector in Kosovo. It seeks to fill the existing data gap by conducting an initial assessment of the key challenges faced by NGOs in terms of digital security and identifying their specific needs for enhancing their digital capacity.

The report employs a quantitative survey approach to assess prevalent cyberthreats, response mechanisms, and digital capacity-building needs. An online survey comprising 43 questions was distributed to over 200 NGOs operating in Kosovo. The list of NGOs to whom the survey was distributed was sourced from the CIVIKOS database, a platform that brings together over 200 NGOs in Kosovo with the objective of promoting collaboration and engagement.¹²

The survey questions were developed in collaboration with an external IT expert and are based on a set of universal indicators of cybersecurity metrics for NGOs, including areas such as governance, technical implementation of procedures, monitoring of security and information systems, testing and auditing of security and information systems, as well as staff training and awareness. A more detailed description of these indicators is provided in the subsequent section of the report.

The survey took approximately 5 minutes to complete and featured a range of question types, such as yes/no, Likert scale, and a few open-ended questions. Microsoft Forms was utilized as the online survey platform, and participants received the survey via email. To ensure a higher response rate, two reminder emails were sent to participants during the survey period. A total of 48 NGOs responded to the survey. The majority of them (92 percent) were NGOs that identified as associations, while the remainder identified as foundations. These NGOs operate across various municipalities in Kosovo, whose scope of works covers a diverse range of fields, including women's rights, child protection, inter-ethnic reconciliation, youth empowerment, human rights and rule of law, environmental protection, advocacy, health, and psychosocial and health services, to name but a few.

The chosen quantitative method for the following analysis serves as an important first step to establishing the groundwork for understanding the level of cyber preparedness and resilience demonstrated by NGOs in Kosovo. However, it should be noted that this method has its limitations in the context of this study, namely that it may fail to provide a detailed and comprehensive picture of cybersecurity needs of this sector. Hence, additional research is necessary to explore more in depth the specific challenges and themes emerging from this report.

CYBERSECURITY INDICATORS FOR NGOs






The following section provides an overview of cybersecurity indicators for NGOs. These indicators are categorized into five thematic areas, namely governance, technical implementation of procedures, monitoring of security and information systems, testing and auditing, and staff training and awareness.

Governance in the context of cybersecurity refers to the establishment of policies, procedures, and frameworks that guide and govern an organization's approach to managing and mitigating cyber risks.¹³ This includes a range of documents and measures such as policies regulating the use of electronic devices and accounts, procedures for data backups, protection of sensitive information, incident response plans, and procedures for software and application updates, among others. The technical implementation of IT-related procedures is another important aspect of ensuring cyber resilience. It refers to the practical application of an organization's governance mechanisms – such as policies, procedures and frameworks – which enable organizations to establish robust defenses and response mechanisms against cyber threats. These procedures may include the implementation of access controls, encryption mechanisms, antivirus software and secure network devices.

Monitoring security and information systems that an organization possesses is an additional crucial indicator through which organizations can detect and respond to a cyber incident in a timely and effective manner. Monitoring can be done either by employing electronic systems or designating staff members within the organization to oversee these systems. To ensure that an organization has strong and robust security and information systems, it is important that these systems are frequently tested and audited. This helps in identifying potential vulnerabilities within these systems, which, if left unaddressed, could lead to security breaches, unauthorized access, data breaches, service disruptions, financial losses, reputational damage, and other detrimental consequences.

Finally, awareness raising and capacity building activities relating to security, in general, and cybersecurity, in particular, are crucial for fostering a strong security culture within an organization. These refer to organizational initiatives that are aimed at educating staff on topics relating to security within the organization. For instance, regular employee training on cybersecurity-related issues helps ensure that they develop the skills required to identify a potential attack and respond to it accordingly. Beyond that, it also teaches them about why it is important to care about cybersecurity in an organizational context and what is at stake should they fail to do so.

TABLE 1 CATEGORIZED CYBERSECURITY INDICATORS AND THEIR DESCRIPTIONS BY THEMATIC AREA

THEMATIC AREA	INDICATORS	DESCRIPTION
 GOVERNANCE	<ul style="list-style-type: none"> » Organization has a written cybersecurity strategy, policy and/or procedure » Organization has a written plan/procedure for mitigating cyber risks » Organization has set procedures and dedicated staff for handling cybersecurity incidents 	<p>The establishment of policies, procedures, and frameworks that guide and govern an organization's approach to managing and mitigating cyber risks</p>
 TECHNICAL IMPLEMENTATION	<ul style="list-style-type: none"> » Organization is equipped with network protection devices such as firewalls and IPS » Organization utilizes computer protection applications including antivirus and IPS » Organization implements access control systems » Organization employs protocols for data encryption 	<p>The practical application of an organization's governance mechanisms such as policies, procedures, and frameworks which enable it to establish robust defenses and response mechanisms against cyberthreats</p>
 MONITORING SECURITY AND INFORMATION SYSTEMS	<ul style="list-style-type: none"> » Presence of electronic systems for security monitoring within the organization » Organization has dedicated staff for cybersecurity monitoring 	<p>Monitoring an organization's security and information systems to detect and respond to a cyber incident in a timely and effective manner.</p>
 TESTING AND AUDITING	<ul style="list-style-type: none"> » Organization conducts regular testing to assess the security of its electronic systems » Organization performs regular audits of its electronic systems 	<p>Regular testing and auditing of an organization's security and information systems to identify potential vulnerabilities within these systems</p>
 STAFF TRAINING AND AWARENESS	<ul style="list-style-type: none"> » Organization offers regular training/presentations for its staff in the field of cybersecurity 	<p>Organizational initiatives that are aimed at educating staff about best practices, potential risks and appropriate behaviours related to cybersecurity</p>

BACKGROUND

The development of the cybersecurity framework in the country began during the early years of its independence in 2008. The initial legislative act approved by the Assembly of Kosovo in 2010 was the Law on the Prevention and Combating of Cybercrime, which serves as a cornerstone for effectively preventing, detecting, and penalizing cybercrime offenses within the online network.¹⁴ In the following years, two additional laws of significant relevance to the sector were ratified, namely the Law on Information Society Services, which entered into force in 2012 and which regulates electronic services such as e-commerce, e-banking and e-governance, as well as the Law on the Interception of Electronic Communications.¹⁵ The latter constituted an important development in the realm of cybersecurity, since it regulates the procedures and conditions for the interception of electronic communications related to the criminal procedure, national security and the security of Kosovo citizens.¹⁶ The Law on Protection of Personal Data, which came into force in 2019, constitutes an additional significant element of the cybersecurity framework. This law defines the rights, responsibilities, principles, and punitive measures pertaining to the protection of personal data and the privacy of individuals, further enhancing the overall cybersecurity ecosystem.¹⁷ The independent authority responsible for overseeing the enforcement of the Law on Protection of Personal Data as well as the Law on Access to Public Documents is the Information and Privacy Agency. At the forefront of the Agency's leadership is Commissioner Krenare Sogojeva-Dermaku, who was elected by Parliament in June 2023.¹⁸

The most comprehensive legal document for cybersecurity in Kosovo to date is the Law on Cybersecurity, which was ratified by the President of Kosovo in February 2023.¹⁹ The law establishes the principles of cybersecurity, the institutions responsible for developing, implementing, and promoting cybersecurity policies, the roles and responsibilities of authorities in the field of cybersecurity, and the duties of cybersecurity entities. It also emphasizes inter-institutional cooperation, addresses the prevention and combating of cybercrime in the Republic of Kosovo, and foresees the establishment of the Cybersecurity Agency, which is to act as the main institutional mechanism responsible for proposing and implementing cybersecurity measures and ensuring the overall guarantee of cybersecurity in the country.²⁰

On a policy-level, an additional key instrument guiding cybersecurity efforts in Kosovo is the now-outdated Cybersecurity Strategy and Action Plan 2016–2019. The strategy was set out to “ensure a safe environment of cyber space by minimizing and preventing cyber threats in cooperation with national and international partners”.²¹ The four strategic objectives through which cybersecurity is tackled in this strategy are the protection of critical information infrastructure, institutional development and capacity building, fostering public and private partnerships, incident response, and international cooperation. Additionally, through this strategy the National Coordinator for Cybersecurity and the State Council for Cybersecurity were created, with the aim to strengthen multi-stakeholder involvement and coordination in relation to security in the cyber sphere.

Significant challenges persist, however, when it comes to the implementation of the legal framework on cybersecurity. While the passing of the Law on Cybersecurity is a positive first step towards creating a comprehensive cybersecurity framework, limited progress towards the implementation of key provisions of this law, such as the functionalization of the Agency

for Cybersecurity within the Ministry of Interior Affairs, which is intended to serve as the central authority for coordinating and overseeing cybersecurity efforts, hinders its effectiveness.²² Additionally, the current Cybersecurity Strategy and Action Plan 2016-2019 is outdated. The new Draft Strategy for Cybersecurity 2023-2027 has undergone the public consultation process and is now awaiting Government approval.²³ Minimal considerations for cybersecurity issues in the recently ratified Kosovo Security Strategy for 2022-2027 is worrisome, as it raises concerns about the level of priority given to this crucial aspect of security in the country.²⁴

In the absence of a state-based support system to rely on in case of incidents in the digital sphere, individuals, organizations and businesses often have to rely on their own resources to respond to cybersecurity-related issues. Furthermore, due to a general lack of public awareness on the subject, individuals and organizations often fail to proactively invest in preventative measures, instead only responding to incidents once they have already occurred.

MAIN FINDINGS

The following section provides an overview of the key findings stemming from the online survey responses collected in the scope of this study. It highlights some of the trends, patterns, and overall tendencies within the sample of NGOs that participated in the study.

In terms of organizational size, the majority of NGOs (71 percent) indicated that they have between 1-10 employees, while 25 percent indicated having 11-30 employees, and the remaining 14 percent indicated having 31 or more employees. Of the total 48 NGOs that responded to the survey, only eight reported not having a functional official website. However, six of NGOs mentioned that they utilize social media platforms, including Facebook and Instagram, as a means of establishing an online presence and engaging with their target audience. The complete set of survey questions can be found under Annex 1.

According to the survey responses, the majority of NGOs expressed concern about the cybersecurity risks faced by the non-governmental sector in Kosovo as a whole. Out of all respondents, 44 percent indicated that NGOs are endangered or very endangered by cyberattacks, while 33 percent stated that they are only somewhat endangered. Yet, when asked about the perceived importance of cybersecurity among NGOs in general, the majority (58 percent) responded that cybersecurity is considered to be of little to no importance. Strikingly, none of the respondents indicated that NGOs view cybersecurity as a highly important organizational concern. Additionally, the majority of NGOs (83 percent) reported to have never been targeted by a cyberattack in the past. Those that had been a target of such attacks in the past (17 percent) outlined various damages incurred, including financial theft through online banking, data loss, website interruptions, social media account hacking, and loss of contacts and important documents. The implications of these findings appear to point towards a scenario where NGOs recognize the reality of cyber threats, yet the limited number of them that have experienced cyberattacks in the past might contribute to the underestimation of the significance of cybersecurity within these organizations. In essence, it suggests that NGOs might grasp the importance of investing in cybersecurity resilience only after they have faced actual challenges, rather than proactively as a preventive measure.

TABLE 2 CYBERSECURITY RISKS AND PERCEIVED IMPORTANCE OF THE ISSUE AMONG SAMPLED NGOS

How endangered are NGOs in Kosovo from cyberattacks?

- Not at all endangered 4%
- Somewhat endangered 33%
- A little endangered 19%
- Very endangered 8%
- Endangered 36%



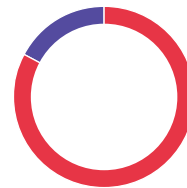
How much importance do NGOs in Kosovo attach to the cybersecurity of the systems they own and data they handle?

- No importance at all 23%
- Some importance 38%
- High importance 4%
- A little importance 35%



Has your organization ever been the target of a cyberattack in the past?

- No 83%
- Yes 17%



Out of the 48 NGOs that responded to the survey, 50 percent stated that they do not have any policy, procedure, or regulation in place that guides or governs their approach to managing and mitigating cyber risks. Among the NGOs that indicated having policies, procedures, or regulations in place, 58 percent reported having between 1-3 such measures, while the remaining respondents reported to have 4 or more. The three most frequently mentioned policies included procedures for creating backup copies of data, policies for the physical security of sensitive information (including the use of locked file cabinets, etc.), and policies for the destruction or disposal of sensitive data. When it comes to incident response, the majority of respondents (62 percent) indicated that they do not have a designated procedure for handling cyber incidents, nor do they have dedicated staff members responsible for this task. Among the remaining respondents, 19 percent stated that they have designated staff members responsible for incident response despite not having a formal procedure in place. Conversely, 10 percent stated that they have a procedure for incident response, but no dedicated staff members assigned to this role. Only 2 percent of the NGOs that participated in this study reported having both a designated procedure and dedicated staff members for incident response. What these findings demonstrate is that if most of the surveyed NGOs were to fall victim to a cyberattack in the near future, they would be largely unprepared to handle the situation promptly and effectively, which could lead to potentially devastating consequences and substantial losses for the organization.

An overwhelming majority of survey respondents, specifically 92 percent, stated that they have never conducted a risk assessment for cybersecurity. In other words, these organizations have never identified potential threats and weaknesses in their systems and information assets that could potentially expose them to cyberattacks or data breaches. Only 38 percent of the survey respondents indicated that they have conducted an inventory of assets, including electronic systems, and have identified and assessed the vulnerabilities of the electronic devices owned by their organization. Additionally, only 19 percent of the survey respondents stated that they use electronic systems to access sensitive information, while a mere 17 percent of them reported having implemented access control measures. Most respondents use one-factor authentication (only password) to access electronic systems within their organizations

(71 percent), instead of a two- or multi-factor authentication. This finding highlights that the security of the electronic systems of the surveyed NGOs is relatively weak and vulnerable, making them more susceptible to unauthorized access through password breaches or other related attacks. Only 11 percent of the NGOs surveyed reported using protocols to encrypt data that is carried over the wireless network and stored on electronic devices within their organization. A positive trend that points to a more proactive approach to enhancing the cybersecurity of electronic systems and assets is that a significant portion of the surveyed NGOs (60 percent) reported using malware protection applications on their electronic systems, including computers, laptops, tablets, and other devices. Furthermore, 40 out of the 48 NGOs surveyed indicated that they use an antivirus program to protect themselves while surfing the internet.

TABLE 3 CYBERSECURITY PREPAREDNESS AMONG SAMPLED NGOs

Do you have any procedures of handling incidents within your organization, and do you have a dedicated team to manage these incidents?

We have procedures and dedicated staff for incident response 2%

We have procedures but not dedicated staff for incident response 10%

We do not have procedures nor dedicated staff for incident response 63%

We do not procedures, but we have dedicated staff for incident response 19%

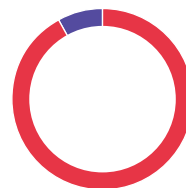
Other 6%



Have you ever conducted a risk assessment for cyberattacks in your organization?

No 92%

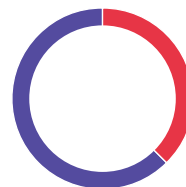
Yes 8%



Have you ever conducted an inventory of assets (electronic systems) in your organization?

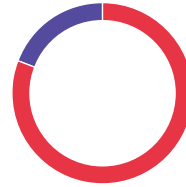
No 38%

Yes 62%



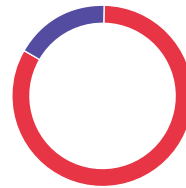
Do you use electronic systems in your organization to control access to sensitive information?

No ■ 81%
Yes ■ 19%



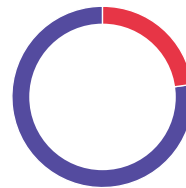
Do you have electronic systems within your organization for determining access control to computer systems, information, etc.?

No ■ 83%
Yes ■ 17%



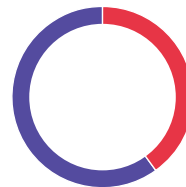
What method do you use to access electronic systems within your organization?

Through multi-factor authentication
(in addition to passwords, you also use
smart cards, SMS codes, two-factor
authentication, etc.) ■ 29%
Through a single factor (password only) ■ 71%



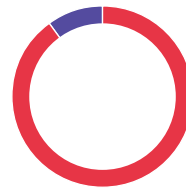
Do you use applications for protection against malware (viruses, worms, etc.) on the electronic systems (computers, laptops, tablets, etc.) of your organization?

No ■ 40%
Yes ■ 60%



Do you use protocols for encrypting the data transmitted over the wireless network?

No ■ 90%
Yes ■ 10%



The survey responses regarding the licensing status of applications used by NGOs were nearly evenly split. Approximately 48 percent of the respondents indicated that the applications they use are licensed, while the remaining 52 percent stated that the applications are not licensed. The use of licensed software within organizations is highly important, as it helps NGOs maintain their credibility, protect sensitive data and avoid legal issues that could potentially disrupt their operations. Most NGOs (77 percent) stated that they do not use technology, such as VPN, to protect records stored in their organization’s electronic systems during remote access from outside via the internet. A striking 98 percent declared that they do not have electronic systems or applications specifically designed for managing and monitoring cybersecurity within their NGO. None of the NGOs surveyed have conducted an internal audit of its cyber defense procedures and systems, and only one out of the 48 NGOs has undergone an external audit of its electronic systems in the past. Most NGOs (65 percent) lack dedicated staff responsible for managing and monitoring cybersecurity within their organizations, nor do they rely on external resources for this task. The absence of systems and staff responsible for cybersecurity management and monitoring is concerning, as it leaves these NGOs completely exposed to a range of cyber risks and vulnerabilities. Cyber threats are always evolving, therefore having dedicated systems and staff to oversee and monitor security measures is crucial to stay ahead of possible breaches and attacks.

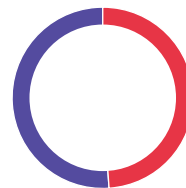
Interestingly, among the NGOs that declared having dedicated staff, a notable finding is that they stated their organizations do not provide professional training to these staff members in the field of cybersecurity. None of the NGOs surveyed have ever provided training to all of their staff members in the field of cybersecurity. Moreover, only 2 NGOs organized awareness raising campaigns or presentations among their staff members about the risks of cyberattacks. This points to a lack of security culture within these organizations, whereby an attack can have multiplying effects not only on the NGO itself, but also for its staff, including on their physical and emotional wellbeing.

TABLE 4 CYBERSECURITY PREPAREDNESS AMONG SAMPLED NGOS
(CONTINUED)

Are the application you utilize within your organization licensed?

No 48%

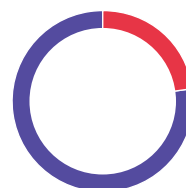
Yes 52%



If there is a need for remote access to the records stored in your organization’s electronic systems (via the internet-remote), do you utilize technology to protect these records during transportation (VPN)?

No 23%

Yes 77%



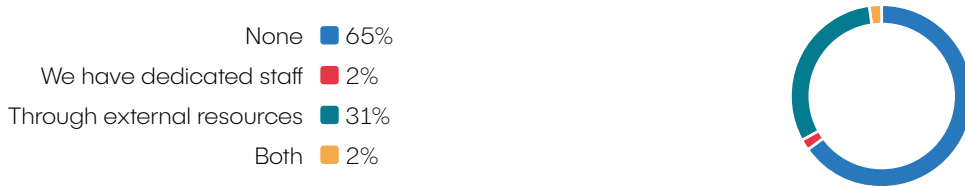
Do you have electronic systems/applications in your organization for managing and monitoring cybersecurity?



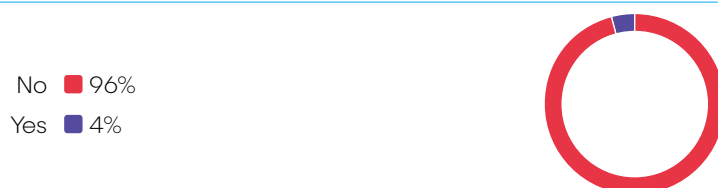
Have you ever conducted an external audit of the cyberattack defense systems to identify weaknesses in the system?



Do you have dedicated staff/employees in your organization responsible for managing and monitoring cybersecurity, or do you rely on external resources for this?



Have you organized campaigns/presentations for your staff to raise awareness about the risk of cyberattacks?



RECOMMENDATIONS

In order to address the challenges identified above, it is crucial that NGOs in Kosovo, regardless of their scope of work, take cybersecurity seriously and implement the following recommendations:

- **Investing in cybersecurity should be a priority for NGOs, but it does not have to be costly. There are various resources available that are cost-efficient or completely free, which they can utilize to develop and enhance their cybersecurity measures.** One such resource is KCSS's Cyber Security Manual for Civil Society Organizations in Kosovo, a comprehensive guide specifically tailored to the needs of NGOs in Kosovo. The manual provides practical advice, step-by-step guidance, and best practices for implementing effective cybersecurity measures. With little time, effort, and resources put into cybersecurity, NGOs can go a long way in strengthening their defenses and protecting their organizations.
- **The donor community should increase their support and collaboration efforts with NGOs to effectively tackle the issue of cybersecurity. This can entail various forms of assistance,** including financial resources dedicated to cybersecurity initiatives, access to specialized expertise in the field, and the provision of training programs tailored to the unique challenges faced by NGOs.
- **NGOs need to be more vocal and proactive in advocating for digital safety.** Because all NGOs are susceptible to falling victim to cyberattacks - irrespective of their field of work- they should prioritize this effort and play an active role in raising awareness about cyber threats, be they security hacks, data breaches, disinformation operations or any other form of online attack. By leveraging the diverse online and offline platforms that NGOs use in their daily work, they can engage with their target groups and wider audiences on issues pertaining to digital safety and digital rights.

ANNEX 1.

LIST OF SURVEY QUESTIONS

QUESTIONNAIRE ON THE LEVEL OF CYBERSECURITY AMONG NGOS IN THE REPUBLIC OF KOSOVO

1. The name of the organization you represent:

2. The city where your organization operates:

3. The year your organization was founded:

4. Type of non-governmental organization (NGO):

- a. Institute
 - b. Foundation
 - c. Association
-

5. Your organization's scope of work:

6. Number of employees in your organization:

- a. 1-10
 - b. 11-30
 - c. 31-60
 - d. 61+
-

7. Your organization's website:

8. Please respond to the question below by selecting one of the provided options:

How endangered are NGOs in Kosovo from Cyberattacks?

- a. Not at all
 - b. A little
 - c. Somewhat
 - d. Endangered
 - e. Very endangered
-

9. Has your NGO ever been a target of a Cyberattack in the past?

- a. Yes
 - b. No
-

10. If yes, what was the damage caused by this attack?

11. Please answer the question below by selecting one of the given options:

How much significance do Kosovo's NGOs attribute to the cybersecurity of the systems they possess and the safeguarding of the records they manage?

- a. Not at all
- b. A little
- c. Somewhat
- d. Significant
- e. Very significant

12. Please answer with a 'yes' or 'no' to the following questions:

Have you ever conducted a risk assessment for Cyberattacks in your NGO?

- a. Yes
- b. No

Have you ever conducted an inventory of assest (electronic systems) in your NGO?

- a. Yes
- b. No

Have you ever identified or assessed weaknesses of the electronic devices owned by your organization?

- a. Yes
- b. No

Do you use electronic systems in your NGO to control access to sensitive information?

- a. Yes
- b. No

Do you have electronic systems in your NGO for determining the level of access control for electronic devices, information, etc.?

- a. Yes
 - b. No
-

13. Which of the following does your NGO possess? (Check all applicable options)

- a. Written Cybersecurity policies, procedures or regulations
- b. Policies, procedures, or regulations for creating passwords, minimum password length, password complexity, and password change frequency
- c. Policies, procedures or regulations for updating software and applications used by your NGO
- d. Policies, procedures, or regulations for the use of mobile devices (tablets, smartphones, etc.)
- e. Procedure for creating back-up copies of your records
- f. Procedure for restoring records in the event of a Cyberattack or accidental/intentional deletion or loss of these records
- g. Policy for the physical security of sensitive information (locked file cabinets, etc.)
- h. Policy for the destruction or disposal of sensitive data after their use is completed
- i. Concrete plan for how to respond in case of incidents, whether they are cyber or physical in nature
- j. Procedure for externally reporting cases where there are suspicions of a cyber incident
- k. Procedure for identifying and registering individuals who physically visit the premises of your NGO
- l. None of the above

14. If your NGO has Cybersecurity policies, procedures, or regulations, are they communicated to all employees of the organization?

- a. Yes
- b. No
- c. NGO does not have any Cybersecurity policies, procedures, or regulations

15. Do you update the policies, procedures, or regulations that you have outlined in the previous question?

- a. Yes
- b. No
- c. NGO does not have any Cybersecurity policies, procedures, or regulations

16. If yes, how often do you update them?

17. Do you have any procedure on how incidents are handled within your NGO, and do you have a dedicated team to handle these incidents?

- a. We have procedures and a dedicated staff for handling incidents
 - b. We have procedures but no dedicated staff for handling incidents
 - c. We don't have procedures, but we have dedicated staff for handling incidents
 - d. We don't have a procedures for handling incidents, nor do we have dedicated staff
 - e. Other
-

18. Do you have any partnerships with other organizations or contractors that involve the processing of sensitive data of your NGO?

- a. Yes
- b. No

19. If yes, do you have a procedure in your NGO for verifying and monitoring these partners/contractors regarding Cybersecurity?

- a. Yes
- b. No

20. During working hours, employees in your NGO have full access to the following:

- a. Personal laptops/computers
- b. Work laptops/computers
- c. Both
- d. Other

21. What methods do you use to access electronic systems (Please select one of the following)

- a. Through one-factor (password only)
- b. Through multiple factors (in addition to password, using methods such as smart cards, SMS codes, two-factor authentication, etc.).

22. Please answer with a 'yes' or 'no' to the following questions:

Do you use applications for protection against malware (viruses, worms, etc.) on the electronic systems (computers, laptops, tablets, etc.) of your NGO?

- a. Yes
- b. No

Do you use protocols for user authentication accessing this network?

- a. Yes
- b. No

Do you use protocols for encrypting the notes transmitted over the network?

- a. Yes
- b. No

Do you use protocols for encrypting the notes stored on electronic devices (servers) in your NGO?

- a. Yes
- b. No

Do you use protocols for encrypting the notes stored on the computers/laptops of your NGO's employees?

- a. Yes
 - b. No
-

23. What applications do you use for official communication in your NGO?

- a. Official email of the NGO (with the NGO's domain)
- b. Microsoft Teams
- c. Zoom
- d. Employees personal emails
- e. Other

24. What technologies do you use for internet security? (check all that apply)

- a. Antivirus program
- b. Firewall program
- c. IPS program
- d. Firewall devices
- e. Other

25. Are the applications you use in your NGO licensed?

- a. Yes
- b. No

26. If there is a need to access the records stored in your NGO's electronic systems remotely (from outside via the internet - remote access), do you use technology to protect these records during transportation (VPN)?

- a. Yes
- b. No

27. Do you have electronic systems/applications in your NGO for the management and monitoring of Cybersecurity?

- a. Yes
- b. No

28. Do you have dedicated staff or personnel responsible for the management and monitoring of Cybersecurity within your NGO, or do you handle this through external resources?

- a. We have dedicated staff
 - b. Through external resources
 - c. Both
 - d. None
-

29. Who is responsible for Cybersecurity and data security in your NGO? How is this responsibility defined (e.g., through documents, policies)? (Check all that apply)

- a. Dedicated staff appointed through a procedure
- b. Management is responsible, as per the procedure
- c. We do not have a procedure defining responsibility
- d. The person responsible for technical matters - IT personnel
- e. All of the above
- f. None of the above
- g. Other

30. If you have dedicated staff for the management and monitoring of Cybersecurity in your NGO, do they receive regular professional training in the field of Cybersecurity?

- a. Yes
- b. No
- c. We don't have dedicated staff

31. Does your NGO provide training for its staff in the field of Cybersecurity?

- a. Yes
- b. No

32. If yes, how many such trainings were offered in the previous year (2022)?

33. Have you organized campaigns/presentations for the staff to raise their awareness about the risks of Cyberattacks?

- a. Yes
- b. No

34. If yes, when was the last time you organized them?

35. Have you ever conducted security testing of your NGO's electronic systems?

- a. Yes
- b. No

36. If yes, when was the last time you have done that?

37. Have you ever conducted an internal audit of procedures and systems for Cyberattack protection to identify weaknesses in these systems?

- a. Yes
- b. No

38. If yes, when was the last time you have done that?

39. Have you ever conducted an external audit of Cyberattack protection systems to identify weaknesses in these systems?

- a. Yes
 - b. No
-

40. If yes, when was the last time you have done that?

41. Have you ever conducted staff testing to assess their knowledge of identifying Cyberattacks (phishing)?

- a. Yes
 - b. No
-

42. If yes, when was the last time you have done that?

43. What percentage of the budget/funds does your NGO invest in Cybersecurity?

ENDNOTES

1. Jacobs, Frank. "Europe's stunning digital divide, in one map." Big Think. June 23, 2023. <https://bigthink.com/strange-maps/europe-digital-divide/>
2. World Bank Support." The World Bank. <https://www.worldbank.org/en/news/press-release/2023/03/21/-every-village-in-kosovo-now-connected-to-high-speed-broadband-internet-with-world-bank-support> (accessed June 19, 2023).
3. Communication Technology in 2022. <https://ask.rks-gov.net/media/7157/tik-ne-ek-familjare-2022.pdf> (accessed June 20, 2023).
4. https://link.springer.com/chapter/10.1007/978-3-030-91247-5_5
5. Democratic Institute, 2022. <https://www.ndi.org/sites/default/files/%5BEnglish%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations-compressed.pdf> (accessed June 13, 2023).
6. Society Centre & Cyber Peace Institute (2022) <https://solidarityaction.network/media/cybersecurity-guidance.pdf> (accessed June 12, 2023).
7. <https://www.evropaelire.org/a/telekomi-i-kosoves-sulme-kibernetike-/32032233.html>
8. Attacks."Balkan Insight. Sept. 14, 2022. <https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/>
9. <https://kosovotwopointzero.com/en/squash-online-hate-speech/>
10. Ondozi, Qerim. "Misinformation, Disinformation and Fake News in Online Media in Kosovo". Press Council of Kosovo (2022). http://presscouncil-ks.org/wp-content/uploads/2022/09/Raporti_Keqinformimi_ENG_Final-2.pdf
11. <https://balkaninsight.com/2021/09/07/kosovo-urged-to-start-countering-russian-media-disinformation/> (accessed May 29, 2023).
12. <http://www.civikos.net/en/background>
13. "Guide to Good Governance in Cybersecurity" Geneva Centre for Security Sector Governance. (2019). https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021.pdf

14. <https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2682>
15. Law NO. 04/L-094 On The Information Society Services, https://cps.rks-gov.net/wp-content/uploads/2020/09/LAW_NO_04_L-094_ON_THE_INFORMATION_SOCIETY_SERVICES.pdf
16. Law NO. 05/L-030 On Interception of Electronic Communications, https://cps.rks-gov.net/wp-content/uploads/2020/08/LAW_NO_05_L-030_ON_INTERCEPTION_OF_ELECTRONIC_COMMUNICATIONS.pdf
17. Law NO. 06/L-082 On Protection of Personal Data, <https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=18616>
18. 1818 Information and Privacy Agency, official website: <https://aip.rks-gov.net/en/aip-english/>
19. Law NO. 08/L-173 On Cyber Security, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933>
20. Vllahiu, Emirjeta. "Kosovo to Establish Agency for Cyber Security Amid Recent Attacks." Balkans Insight (Sept. 14, 2022). <https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/>
21. National Cyber Security Strategy and Action Plan 2016 – 2019. <https://afyonluoglu.org/PublicWebFiles/strategies/Europe/Kosovo%202016-2019%20Cyber%20Security%20Strategy-EN.pdf>
22. Law NO. 08/L-173 On Cyber Security, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933>
23. Kosovo Draft Cyber Security Strategy 2023 – 2027, <https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=41780>
24. Kosovo Security Strategy 2022 – 2027, <https://kryeministri.rks-gov.net/wp-content/uploads/2022/10/2-Strategjia-e-Sigurise-e-Kosoves-ENG.pdf>

Katalogimi në botim – **(CIP)**
Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

061.2:007(496.51)(047)

Elshani, Donika

Are non-governmental organizations prepared to deal with cyberthreats?
: an analysis of perceptions of cybersecurity capacities among NGOs in
Kosovo / Donika Elshani. – Prishtinë : QKSS, 2023. – 27 f. : ilustr. ; 28 cm.

ISBN 978-9951-842-03-7

About KCSS

Established in April 2008, the Kosovar Center for Security Studies (KCSS) is a specialized, independent, and non-governmental agency. The primary goal of KCSS is to promote the democratization of the security sector in Kosovo and to improve research and advocacy work related to security, the rule of law, and regional and international cooperation in the field of security.

KCSS aims to enhance the effectiveness of the Security Sector Reform (SSR) by supporting SSR programs through its research, events, training, advocacy, and direct policy advice. Advancing new ideas and social science methods are also core values of the centre. Every year, KCSS publishes numerous reports, policy analysis and policy briefs on security-related issues. It also runs more than 200 public events including conferences, roundtables, and debates, lectures – in Kosovo, also in collaboration with regional and international partners. A wide-range of activities includes research, capacity-building, awareness raising and advocacy.

KCSS's work covers a wide range of topics, including but not limited to security sector reform and development; identifying and analyzing security risks related to extremism, radicalism, and organized crime; foreign policy and regional cooperation; and evaluating the rule of law in Kosovo.

This year, KCSS celebrated its 15th Anniversary. For more details about KCSS, you can check on the following official platforms:



qkss.org
securitybarometer.qkss.org



@KCSSQKSS
#KCSSQKSS

ISBN 978-9951-842-03-7



9 789951 842037