BPRG Balkans Policy Research Group

KOSOVO IN THE FACE OF CYBERSECURITY THREATS:

Critical Actions to consolidate resilience

Kosovo is a target of malicious cyber-attacks, just like many countries and especially those underdeveloped in digitalisation. In 2022, Kosovo institutions were the target of several continuous cyber-attacks aimed at disrupting the services and citizens' access to them. One of them was eKosova, which went down on 5 September.[1] A cyber-attack is a malicious attempt that aims to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic, making it unreachable to the legitimate audience. To address it, technical and legislative measures should be in place, as well as capable and professional human resources.

The fuss continued as Kosovo experts operating abroad criticised the government for not disclosing details on what seemed to be a distributed denial-of-service attack (DDoS).[2] In September, 2022, the government confirmed that the Kosovo Information Society Agency's (KISA) cybersecurity team was closely working with external cybersecurity specialists to mitigate the impact. According to KISA, the cyberattack, in fact, failed to penetrate the internal network infrastructure as it was detected and prevented by a basic security measure that filtered incoming traffic as malicious behaviour.

Yet, Kosovo continues to face several challenges in cybersecurity. One of the key issues is the lack of trained personnel and expertise to detect and respond to cyber threats. The government has dedicated a limited budget for cyber defence, which is insufficient to support the necessary investments in technology and infrastructure for the protection against cyber-attacks. Likewise, the legislative framework (specific legislation and regulations) for cybersecurity is undeveloped. This has a domino effect on law enforcement and other government agencies, which cannot effectively investigate and prosecute cybercrime. Furthermore, it can create confusion among private sector organisations regarding their legal responsibilities and obligations related to cybersecurity.

Despite these challenges, the government has undertaken some actions to address cybersecurity, including the establishment of the National Cyber Security Unit (KOS-CERT), Agency for Information Society of Kosovo (ASHIK), Kosovo Security Council (KSC), Kosovo Police Cybercrime Unit, Cyber Security Centre of Excellence (CSOC), has increased funding for cybersecurity, and has developed a national cybersecurity strategy to guide its efforts in the area. In February 2023, the President of Kosovo signed the updated Legislation for Cybersecurity to enhance cybersecurity and support the development of a secure and resilient digital ecosystem in the country.[3] However, further efforts are still needed to fully address the cybersecurity challenges that the country is facing, including strengthening cooperation with international partners and private sector organisations, as well as implementing tools that will support expert reporting and more robust legislation and regulations specific to cybersecurity. Moreover, investing in training and education programs to help build a skilled workforce is also crucial.

1 E Kosova is the official platform where public services located in the offices and physical counters of institutions are provided electronically. The service digitisation project within eKosova represents the following process towards the digitalisation of all services in the state administration of Kosovo.

2 DDoS is an attack which attempts to block access to and use of a resource. It is a violation of availability and can include flooding attacks, connection exhaustion, and resource demand. The purpose of a DDoS attack is to significantly amplify the level of the attack beyond that which can be generated by a single attack system to overload larger and more protected victims.

3 The Official Gazette of the Republic of Kosovo, Law No. 08/L-173 on Cyber Security, 27 February 2023, at https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933.

RECOMMENDATIONS

The key to mitigating any attack vector, not just a DDoS attack, is the proper working triangle between people, processes, and tools. A well-working chain of layered approaches should be coherently in place to prevent and mitigate such disruption attempts. These include having proper:

- Cybersecurity Mitigation Strategy and Resiliency Plan;
- Allocated budget for cyber defence resources:
    a. Human capacity:
        - Trained staff to recognize and react toward suspicious patterns (i.e., DoS[4]-DDoS);
    b. Technology:
        - Network and Resource Segmentation based on resource criticality.
        - OWASP Top 10 Protection Guidelines and solutions, such as Network Monitoring tools, Advanced Firewall and WAF, DNS configurations, IDPS, and Rate Limiting;[5]
- Implementation of a state-wide incident reporting portal where worldwide experts can report.

If the government of Kosovo had this chain of layered approaches in place, the attack toward eKosova would have looked as simulated in Figure 1.

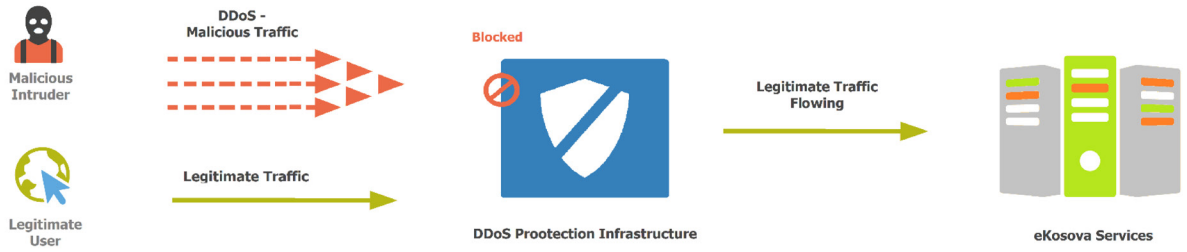


Figure 1. Simulation of the DDoS prevention toward eKosova

Two sources are simultaneously seeking services from eKosova: The malicious traffic coming from the intruder and the legitimate one coming from the legitimate citizens in need of using the eKosova services. The layered approach is black-boxed in the figure as 'DDoS Protection Infrastructure'. This 'black box' acts as a shield for detecting and blocking malicious traffic and simultaneously allowing citizens' access to the source.

Kosovo's National Cyber Security Unit (KOS-CERT), which operates under the Regulatory Authority for Electronic and Postal Communications (AKREP) is the responsible body for incident response and awareness.[6] As of February 2023 (with the newly approved legislation), the Cyber Security Agency (CSA) is officially established by the government and is serving as a centralised body for establishing, managing, auditing, and defending against malicious attempts. [7]According to this legislation, the national CERT will be functionalized under CSA. Additionally, a National Cyber Security Council (NCSC) will be appointed to act as an independent advisory body to the Agency.[8] NCSC will be composed of high-level representatives from government institutions, the business community, public and private NGOs, and the scientific community.

The updated legislation was reviewed by the NIS European Directives in an attempt to remove redundancies and make it as relevant as possible.[9] The NIS Directive is an EU initiative that provides solid legal measures to enhance the EU cybersecurity maturity level by ensuring member states' preparedness. Besides, the legislation was further complemented with inputs from external experts.

4 DoS is a variation of the DDoS attack but the resource demand is generated by only a single attack system.

5 OWASP Top 10 or The Open Web Application Security Project is an open-source application security community with the goal to improve the security of software; A firewall is a security tool, hardware, or software, that is used to filter network traffic. Advanced firewalls can make allow/deny decisions based on user authentication, protocol, header values and even payload contents WAF is short for Web Application Firewall which is an Advanced Firewall specifically for protecting web applications from common exploits and vulnerabilities; DNS, or the Domain Name System, translates human-readable domain names (i.e.: www.amazon.com) to machine-readable IP addresses (i.e.: 192.0. 2.44); IDPS, or Intrusion Detection and Prevention System is a system that monitors a network and scans it for possible threats to alert the administrator and prevent potential attacks; Rate limiting is generally put in place as a defensive measure for services. Shared services need to protect themselves from excessive use—whether intended or unintended—to maintain service availability.

6 In simple terms, it's a plan that helps an organisation respond to unexpected security incidents, such as cyber-attacks or physical breaches. The goal of incident response is to limit the damage caused by an incident and get back to normal operations as quickly as possible. This refers to the education and training of employees and other stakeholders on how to identify and respond to potential security threats. It is important because a significant number of security incidents are caused by human error, such as clicking on a malicious link in an email or sharing sensitive information with unauthorised individuals.

7 The Official Gazette of the Republic of Kosovo, Law No. 08/L-173 on Cyber Security, February 2023.

8 The Official Gazette of the Republic of Kosovo, National Cyber Security Council, as defined in Kosovo's Law on Cyber Security, Chapter IV: Institutions Responsible for Cyber Security, Article 21: National Cybersecurity Council, 2022.

9 NIS European Directive, Directive on security of network and information systems, Shaping Europe's digital future, European Commission, 2022, at https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

Kosovo's Overall Cybersecurity Maturity

The new law sets the minimum norms and criteria for the conservation of network systems and the necessary information for the functioning of society, network systems, and the information of state authorities, liabilities and oversight, and the base for the handling, forestalment and combating cybercrime in Kosovo against any attack.

It provides a general roadmap of how the overall cyber security infrastructure will look in Kosovo, starting from:

- Establishing the principles of cybersecurity;
- The institutions that develop and apply cyber security policies;
- The liabilities of the authorities in the field of cyber security;
- The duties of appointed cyber security professionals, and
- Inter-institutional cooperation.[10]

However, according to external experts of the Kosovar cybersecurity community, there are, in fact, some issues with the current draft-law, among them being:

- The exclusion of a legal basis for responsible disclosure and reporting of vulnerabilities;
- Critical Asset Infrastructure Regulation;
- Compliance Rewards along with Punitive Measures;
- Minimal Cyber Risk Criteria Creation;
- Tackle Expert Shortage; and
- Support and Promotion of Cybersecurity.

Some of these issues are included in the 2020 Cyber Security Capacity Assessment of Kosovo of the Global Cyber Security Capacity Centre. The report highlights many cybersecurity areas that need improvement. Yet, the 'Cybersecurity Policy and Strategy' stands as the most undeveloped/immature dimension. The report aimed to measure the level of maturity that Kosovo has reached within the last five years. This Cybersecurity Maturity Model (CMM) assessment conducts factor analysis and developments on five core cybersecurity dimensions:

D1: Cybersecurity Policy and Strategy

Assesses Kosovo's ability to develop and implement cybersecurity policies and strategies, as well as improve incident response and infrastructure protection. It also considers early warning, deterrence, defence, and recovery. Effective policies can advance national cyber defence and resilience while promoting access to cyberspace.

D2: Cyber Culture and Society

Emphasises the need to develop a responsible cybersecurity culture and society by educating all Internet users about cyber risks and personal data protection. It also highlights the importance of accountability mechanisms and the role of media in shaping cybersecurity values and behaviour.

D3: Cybersecurity Education, Training and Skills

Assesses the existence and effectiveness of cybersecurity awareness programs for executives and the public. It also examines the quality and accessibility of training and education programs for different stakeholders, including government and private sector groups.

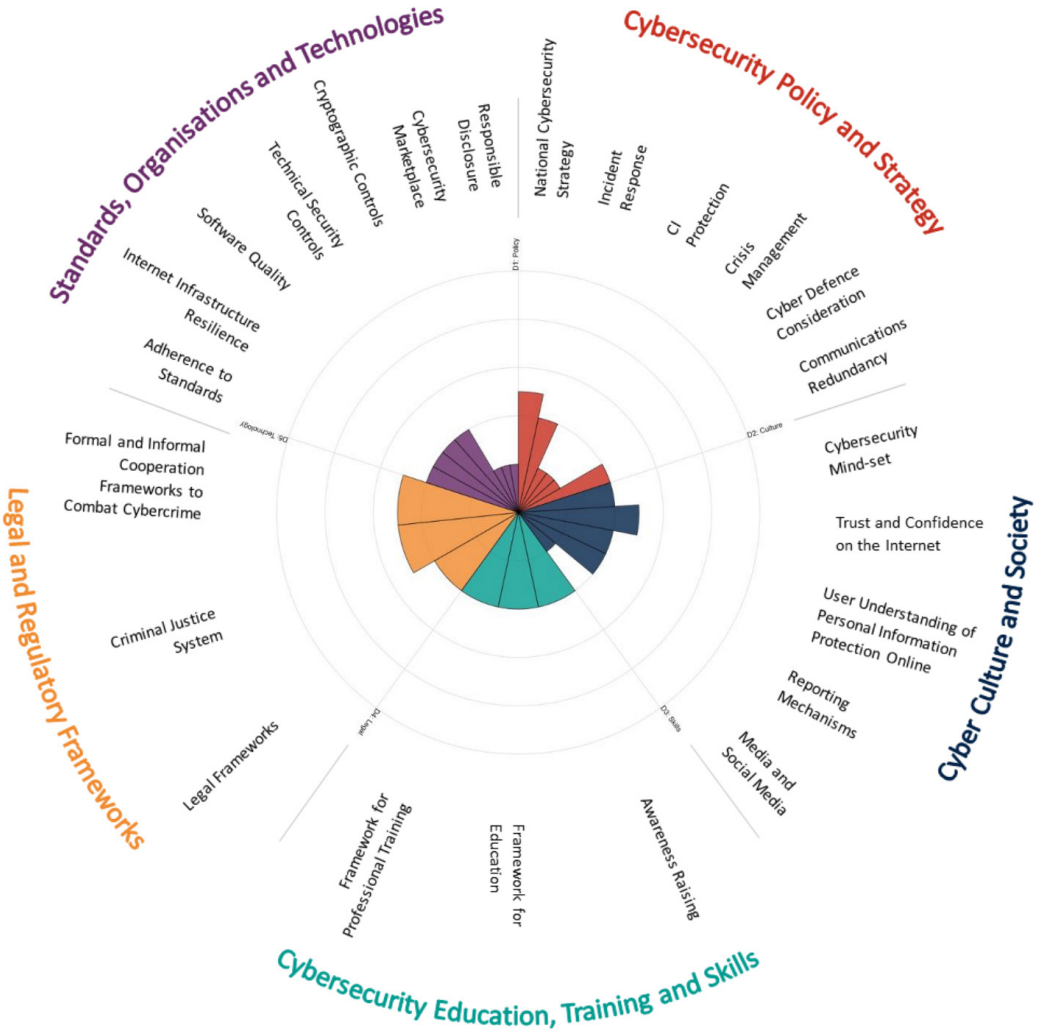
D4: Legal and Regulatory Frameworks

Evaluates the government's ability to create and enforce cybersecurity-related legislation, particularly in areas, such as ICT security, privacy, and data protection. It also assesses the capacity of law enforcement, prosecution, and courts to enforce these laws, as well as formal and informal cooperation frameworks to combat cybercrime.

D5: Standards, Organisations and Technologies

The dimension focuses on the use of cybersecurity technology to safeguard individuals, organisations, and national infrastructure, including the implementation of standards and good practices, control deployment, and technology development to minimise cybersecurity threats.

10 The Official Gazette of the Republic of Kosovo, Law No. 08/L-173 on Cyber Security, February 2023.



Graph 1: Cybersecurity Capacity Review Republic of Kosovo 2020[11]

This graph illustrates the maturity level of responsible disclosure, which falls under the D5, and incident response and crisis management, falling under the D1. All these issues belong to the undeveloped/immature dimensions, and according to experts, they should have been regulated through the updated version of the law.

In the current law on cyber security, some issues are not included, while others are only generally referred to. Among the missing issues are:

- Responsible Disclosures; and

- Punitive Measures and Compliance Rewards.

Responsible Disclosure: is one of the most evident missing issues - also of a high priority - in the new law. Coordinated vulnerability disclosure (CVD) is a vulnerability exposure model in which a vulnerability or an issue is exposed to the public only after the responsible parties at stake have been allowed sufficient time to patch or remedy the vulnerability or issue. A similar approach is taken by tech giants, governments and institutions around the world, and the rewarding mechanisms to encourage researchers to report are not always monetary. Some form of reward can be a 'hall of fame' or other virtual rewards of acknowledgement.[12] Google's Project Zero and OWASP-based practices are the best examples of a successful vulnerability disclosure process.[13] The Norwegian Broadcasting Corporation (NRK), the U.S. Department of Energy, and Nokia have adopted such a program and are a good example to follow.[14] Private experts and the whole contributing community need a place where they can confidentially submit their state security findings, therefore, the newly adopted law should have encouraged

11 Each dimension represents one-fifth of the graphic, the more the factor is extending outwards from the centre of the graphic the more developed is that scope maturity and vice versa.

12 A "Hall of Fame" is a recognition program that rewards individuals or groups for finding security vulnerabilities in software, websites, or other computer systems. Its goal is to encourage individuals and groups to report vulnerabilities to organisations, rather than exploiting them or selling them on the black market.

13 Google Project Zero Policy and disclosure, 2020 edition, 2022, at Project Zero: Policy and Disclosure: 2020 Edition and OWASP 2022 Vulnerability disclosure Cheat Sheet Series, at Vulnerability Disclosure - OWASP Cheat Sheet Series.

14 Norway, N.R.K., publicly owned Norwegian public broadcaster responsible disclosure policy, at https://info.nrk.no/responsible-disclosure-policy/?%2Fkx02fi2v19x; Department of Energy Responsible Disclosure powered by Synack, Department of Energy Responsible Disclosure, U.S. Department of Energy, 2022, at Vulnerability Disclosure Program; Nokia Responsible disclosure, Nokia Networks position on responsible vulnerability disclosure, at Responsible disclosure | Nokia.

responsible disclosure. Implementing a responsible disclosure portal may be costly, but the benefits of improved security and reduced risk of cyber-attacks will outweigh the expenses. The actual cost will depend on the size and complexity of the portal and the resources available to the organisation. The cost of implementing a responsible disclosure portal depends on various factors, such as the size of the organisation, the complexity of its systems, and the level of security required. Some of the costs associated with implementing a responsible disclosure portal may include:

1. **Development costs**: Creating a portal requires skills and resources in software development. Depending on the complexity of the portal, it may require a team of developers, designers, and testers.

2. **Hosting costs**: A responsible disclosure portal needs to be hosted on a web server. The hosting costs will depend on the size and traffic of the portal.

3. **Maintenance and support costs**: Once the portal is launched, it will require ongoing maintenance and support. This includes software updates, bug fixes, and responding to reports submitted through the portal.

Despite these costs, implementing a responsible disclosure portal can provide significant benefits for a state or government agency. It can help identify security vulnerabilities before they are exploited by malicious actors, reduce the costs associated with responding to security incidents, and improve the overall security posture of the organisation

Punitive Measures and Compliance Rewards: Another overlooked issue is the current punitive measures toward institutions. According to some experts these measures can easily be bypassed.[15] For instance, 'X' stakeholders from the private sector, could freely bypass the current detention payment rule if the latter earns double or triple monthly. Say, company 'X' operator of a digital service that earns 60,000 quarterly just recently failed to comply with Article 5 on timely reporting of a cybersecurity incident with the intent of maintaining their reputation. This caused significant harm to the provider of an essential service. Based on the law, company 'X' now must pay 15,000-30,000 EUR as a punitive measure. Company 'X' can afford and will pay the fine as that merely impacts their profit. [16]What is worse, is that this company might act the same when another similar case comes along. To avoid the above-stated scenario, options and suggestions on making this part of legislation bullet-proof would include an adapted version of the following:[17]

• Rewards for compliance: the government could offer incentives for compliance, such as tax breaks or other financial rewards.[18] This would motivate operators to prioritise cybersecurity and would help to create a culture of security within essential state services.

• Mandatory cybersecurity training: Making the (regular) cybersecurity training mandatory to all essential state services operators can help to raise awareness of the importance of cybersecurity and can help operators to better understand the risks and best practices for managing those risks.[19]

• Cybersecurity audits: Regular audits can help to identify vulnerabilities and areas of non-compliance and provide operators with specific recommendations for improving their cybersecurity posture. By making audits mandatory, operators will be motivated to ensure that they are following regulations.[20]

• Certification programs: The state could develop certification programs for essential state services operators that demonstrate compliance with cybersecurity regulations. This could help to create a competitive advantage for operators who prioritise security and would help to reassure customers and stakeholders that security is being taken seriously.[21]

• Public reporting of cybersecurity incidents: Requiring essential state services operators to publicly report cybersecurity incidents can help to create a culture of transparency and accountability.[22] This can also help to raise awareness of the importance of cybersecurity and can help to create a sense of urgency around improving cybersecurity posture.

15 Reference i.e. Balkans Group workshop with cybersecurity experts, Emerald Hotel , October, 2022.
16 The Official Gazette of the Republic of Kosovo, Law No. 08/L-173 on Cyber Security, February 2023.
17 Highly effective and resistant to failure or setbacks
18 In 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) launched the "Cybersecurity Incentives Initiative," which aims to "identify and promote cybersecurity practices and policies that can measurably improve the cybersecurity posture of organisations and the collective security of the national cyber ecosystem." As part of this initiative, CISA is exploring various types of incentives, including "insurance discounts, access to grants or loans, preferred contract status, public recognition, and streamlined regulatory requirements." For more, see https://www.cisa.gov/cybersecurity-incentives-initiative.
19 Cybersecurity Awareness Training for State Employees, National Conference of State Legislatures, 2021, at https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-awareness-training-for-state-employees.aspx.
20 Cybersecurity audits, The National Institute of Standards and Technology (NIST) provides guidance on conducting cybersecurity audits in its Framework for Improving Critical Infrastructure Cybersecurity. For more, see https://www.nist.gov/cyberframework.
21 Organisations can obtain certification to ISO 27001 to demonstrate compliance with the standard. For more, see https://www.iso.org/isoiec-27001-information-security.html.
22 For more, see https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Chapter 5 Article 24: Proposed Bylaws

24.1 Punitive Measures

1. Overall profit-based punitive measure based on the providers' overall profit percentage.

2. Prohibit the lawful operation of the company/certain service for a predefined time.

24.2. Compliance Rewards

1. Rewards for compliant service providers;

2. Certification programs to demonstrate compliance.

24.3 Enforcement and Monitoring

1. The Cybersecurity Training Centre will provide mandatory cybersecurity training to the service provider.

2. The Cybersecurity Agency will make sure to conduct regular cybersecurity audits to identify vulnerabilities and areas of non-compliance.

3. Public reporting of cybersecurity incidents if PII[23] data is compromised in a cybersecurity incident.

A state-run analysis is necessary to set the threshold, from which no service provider would comfortably bypass. Moreover, it needs to be very specific to avoid gaps from which service providers can take advantage. The state, on the other hand, needs to provide support and guidance to the private sector to achieve the minimum-security criteria.

Other issues that need more attention and which are not properly regulated through the new law are:

- Critical Asset Inventory Validation;

- Minimal Cyber Risk Criteria Creation;

- Expert Shortage; and

- Supporting and Promoting Cybersecurity.

Critical Asset Inventory Validation: When building a cyber security strategy, the first step is to identify and understand what you need to protect. This is why all state institutions must be able to identify, verify, and monitor critical assets that impact confidentiality, integrity, and/or availability and support state security missions and functions. There are technological means which gather and register all public asset inventory that is classified as critical state infrastructure and/or holds state-sensitive information.[24] However, some are sceptical about whether the inventory is accurate. Some of the common questions raised by the experts are the following.

◦ whether all critical assets are included in that centralised inventory;

◦ whether they are updated on a case-to-case basis;

◦ whether they are properly classified based on their criticality; and

◦ whether there is enough qualified staff to audit, monitor, and update them.

Initially, the accurate identification and classification of critical assets is a fundamental step in the development of any effective cybersecurity strategy. Failure to identify all critical assets can leave important systems and data vulnerable to attack and can result in serious consequences for the state. By including this requirement in cybersecurity law, the state can ensure that all institutions are following a standardised process for identifying and verifying critical assets and that these assets are properly classified based on their criticality.

Secondly, regular updating of the critical asset inventory is essential to ensure that institutions are aware of any changes or updates that may impact their cybersecurity posture. This includes changes to the criticality of assets, as well as changes to the threats and risks faced by the institution. By including this requirement in cybersecurity law, the state can ensure that all institutions are regularly updating their critical asset inventory and that they are taking

23 PII stands for Personally Identifiable Information. It refers to any data that can be used to identify a specific individual, either on its own or in combination with other data.

24 Balkans Group Policy Idea Lab, October, 2022, Prishtina.

steps to mitigate any new risks or threats.

Ultimately, having enough qualified staff to audit, monitor, and update the critical asset inventory is critical to ensuring that the process is effective. By including this requirement in cybersecurity law, the state can ensure that institutions are allocating sufficient resources to this task and that they are maintaining the necessary level of expertise to properly manage their cybersecurity risks.

In terms of evidence and references, Annex A.8 of ISO 27001 outlines the requirements for maintaining an accurate and up-to-date inventory of assets. Additionally, the NIST Cybersecurity Framework includes asset management as a core function and highlights the importance of accurately identifying and classifying critical assets. Finally, the Centre for Internet Security (CIS) Controls also includes asset management as one of its top 20 critical security controls and guides how to develop and maintain an effective asset inventory. These frameworks are widely recognized and adopted by organisations around the world and provide a comprehensive approach to managing cyber risks. By including this requirement in cybersecurity law, the state can ensure that its institutions are following established best practices and are properly managing their cybersecurity risks.

Minimal Cyber Risk Criteria Creation: Another important issue is the lack of minimal criteria for managing cyber risks in state institutions to mitigate the potential risks of a breach. The law must define and enforce a minimum security control check systematically on digital systems.' These control checks should be based on the best cybersecurity framework recommendations like NIST CSF and SP, NIS Directive, ISO 27000 Series, CIS Controls, and GDPR.[25]

The creation of minimal cyber risk criteria is essential for several reasons. First, cyber threats are becoming increasingly sophisticated and widespread, and state institutions are attractive targets for cybercriminals seeking to steal sensitive data or disrupt critical infrastructure. By establishing minimum standards for cybersecurity, the state can help ensure that its institutions are adequately protected from these threats. Second, the lack of a standardised approach to cybersecurity can lead to inconsistencies in how different institutions manage their risks, which can create vulnerabilities and gaps in the overall security posture of the state. By adopting a common set of criteria for managing cyber risks, the state can ensure that all institutions are operating at a similar level of security, which can help reduce the overall risk to the state. Third, the use of established cybersecurity frameworks like NIST CSF, NIS Directive, ISO 27000 Series, CIS Controls, and GDPR can provide institutions with a proven set of best practices for managing cyber risks. These frameworks are widely recognized and adopted by organisations around the world and provide a comprehensive approach to managing cyber risks that covers everything from risk assessment to incident response.

By integrating the minimal cyber risk criteria into state law, the state can ensure that all institutions are required to meet a common set of standards for managing cyber risks. This can help improve the overall security posture of the state, reduce the risk of cyber threats, and provide a clear framework for institutions to follow when managing their risks. Additionally, by enforcing these standards through legislation, the state can hold institutions accountable for their cybersecurity practices and ensure that they are taking the necessary steps to protect sensitive information and critical infrastructure.

Expert Shortage: Another aspect worth considering is the number of professionals necessary to conduct security within an institution. There is an enormous shortage of experts in cybersecurity in the country, much less in institutions. Yet, a minimum number of necessary professionals in critical state institutions is needed. The State Agency must monitor the staff on the completion of their responsibilities, as described in their job description. The types of fines that fall upon the individuals that perform under their legal scope of work, harm or use their capabilities and professionalism in a manner that could damage the institution, should also be defined with by-laws that require staff advancement, performance, as well as an integrity check. Here are a few ideas:

◦ Offer training and professional development opportunities: Institutions can invest in training and development programs that help existing staff members acquire new skills and knowledge related to cybersecurity. This could include courses, certifications, or workshops that provide hands-on experience with security tools and best practices. By providing staff members with opportunities to grow their expertise, institutions can build a more capable and knowledgeable workforce.

◦ Establish performance metrics: To ensure that staff members are meeting their responsibilities, institutions can establish clear performance metrics that define expectations for their work. These metrics could include benchmarks for detecting and responding to security incidents, maintaining compliance with relevant regulations, and completing training and development requirements. By tracking and reporting on these metrics, institutions can hold staff members accountable for their performance.

25 NIST - National Institute of Standards and Technology, US Department of Commerce; ISO/IEC 27000 and related standards, information security management ISO, at ISO/IEC 27001 Standard – Information Security Management Systems; The CIS Controls (formerly known as Critical Security Controls) are a recommended set of actions for cyber defence that provide specific and actionable ways to stop today's most pervasive and dangerous attacks; The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

◦ Conduct regular integrity checks: To prevent staff members from misusing their capabilities or harming the institution, institutions can conduct regular integrity checks that assess their conduct and adherence to ethical standards.

Support and Promote Cybersecurity: Establishing a Cybersecurity Agency is the first step toward creating a dedicated cybersecurity agency that is responsible for developing and implementing cybersecurity policies, strategies, and standards. This agency can work with other government agencies, private companies, and academic institutions to promote cybersecurity awareness and education. However, that is only a small part of what should support and promote cyber security:

1. Funding Research and Development: This can include funding for academic institutions and private companies to develop new tools and technologies to address emerging cyber threats.

2. Providing Cybersecurity Training and Education: A state can provide cybersecurity training and education programs for both government employees and private sector workers. This can include training on cybersecurity best practices, risk management, and incident response.

3. Encouraging Collaboration: A state can encourage collaboration between government agencies, private companies, and academic institutions to share information and expertise on cybersecurity threats and best practices.

4. Offering Incentives: A state can offer incentives for companies to adopt cybersecurity best practices. This can include tax breaks, grants, or other financial incentives for companies that invest in cybersecurity measures.

Conclusions

After the series of cyber-attacks, the Government of Kosovo proposed to establish an Agency for Cyber-Security.[26] The State Agency for Cyber Security and the NCSC will act as a regulatory body and creator of all state controls. The government has adopted the Law on Cyber Security to establish the legal basis for the forestalment of cybercrime and to provide more security to its citizens.[27] The aim is to strengthen computer security in Kosovo, including the establishment of the State Authority for Cyber Security, which will also include new cybersecurity measures.

This law on cybersecurity has tackled many important aspects that will combat cybercrime. However, for it to become highly effective and resistant, the cross-functional cooperation between the public and private institutions should be enhanced, and the following suggestions should be taken into consideration:

- Creating a Vulnerability Disclosure Program for Responsible Disclosure
- Critical Asset Infrastructure Regulation
- Punitive Measures and Compliance Rewards
- Minimal Cyber Risk Criteria Creation
- Tackle Expert Shortage
- Support and Promotion of Cybersecurity

These improvements will impact the future of Kosovo's Cybersecurity landscape. Other legal improvements would also be necessary to establish the foundations for a well-functioning cybersecurity state plan, after which comes a well-constructed cybersecurity strategy that can withstand any unexpected events or risks and allows officials to better understand the state environment and profile.

Recommendations:

1. Set control, audit and constant training for the responsible staff performing their cybersecurity activities within all institutions.

2. Create a legal basis for responsible disclosure and reporting of vulnerabilities.

3. Cyber Warfare as part of the future professional generation contributing to safer cyberspace worldwide.[28]

4. Create a program for career incentives to attract and retain information security and IT professionals in the public sector. For example, offer a compensation package and career path that competes favourably with private-sector opportunities.

26 The Official Gazette of the Republic of Kosovo, CSA, Cyber Security Agency, as defined in Kosovo's Law on Cyber Security, Chapter IV: Institutions Responsible for Cyber Security, Article 13: Establishment and Status of the Cyber Security Agency, 2022.
27 The Official Gazette of the Republic of Kosovo, Law No. 08/L-173 on Cyber Security, February 2023.
28 Cyberwarfare is the use of cyber-attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems.

5. Task the designated body with developing effective metrics to ensure investments in education and upskilling to meet the needs of the cybersecurity environment.

6. Intensify national cybersecurity research resources and laboratories to encourage PhD programs in various universities.

7. Drive the adoption of up-to-date security controls across the economy, including network attack detection, regular data backups, and consistent patch management.

8. Extend training programs to most employees at all levels in the private and public sectors by establishing continuing education on cyber security issues. International best practices and professional training documents should form the basis of these courses.

9. Classify software applications intended for use by government agencies based on their reliability, usability, and performance by international standards and best practices.

The Balkans Policy Research Group is an independent, regional think-tank based in Pristina, Kosovo. We provide timely policy analysis and recommendations on a wide array of state building issues; institutional and democratic consolidation; minority integration and good neighborly relations: European integration and policy change. We have decades of experience in policy reporting and development, strategic thinking and advocacy with governmental, international and non-governmental organizations.

Our rigorous, detailed, impartial reporting, always based on in-depth fieldwork, is the core of our work. We go beyond mainstream positions and seek to make change through creative, feasible, well-measured and forward-looking policy recommendations with the aim of helping develop strong, vibrant democracies, prosperous states and societies based on rule of law in the Western Balkans.

We engage in high-level advocacy, domestically, regionally and internationally, impacting policy discussions and options with regard to the home affairs and European policies toward the Western Balkans.

Balkans Group has developed other tools and platforms to achieve this change:

The Policy Dialogue promotes Kosovo's domestic dialogue, cohesion and reform-making agenda.

The Policy Forum (a Think-Tankers High-level Advocacy Forum) committed to enhancing the dialogue between the civil society and the institutions.

The Kosovo Serbia Policy Advocacy Group (a forum for Cross-Border Civil Society Cooperation) that aims to communicate, promote and enhance dialogue toward full normalisation between Kosovo and Serbia, and their societies.

Women in Politics promotes the empowerment of women and girls; their security and inclusiveness; and is committed to strengthen the Women Caucus' impact and reach throughout Kosovo.

Youth in Politics promotes an active participation from youth from different political parties in the institutions. This component helps in developing a culture of dialogue and cooperation, by providing capacity building trainings on key policy areas and skills and leadership.

The Dialogue Platform promotes the dialogue process between Kosovo and Serbia, by informing the wider public and generating debate about the agreements, benefits and challenges of the Dialogue.

Expert Support component provides policy support to the government and key institutions on key policy areas, peace and state-building agendas.

Norwegian Embassy