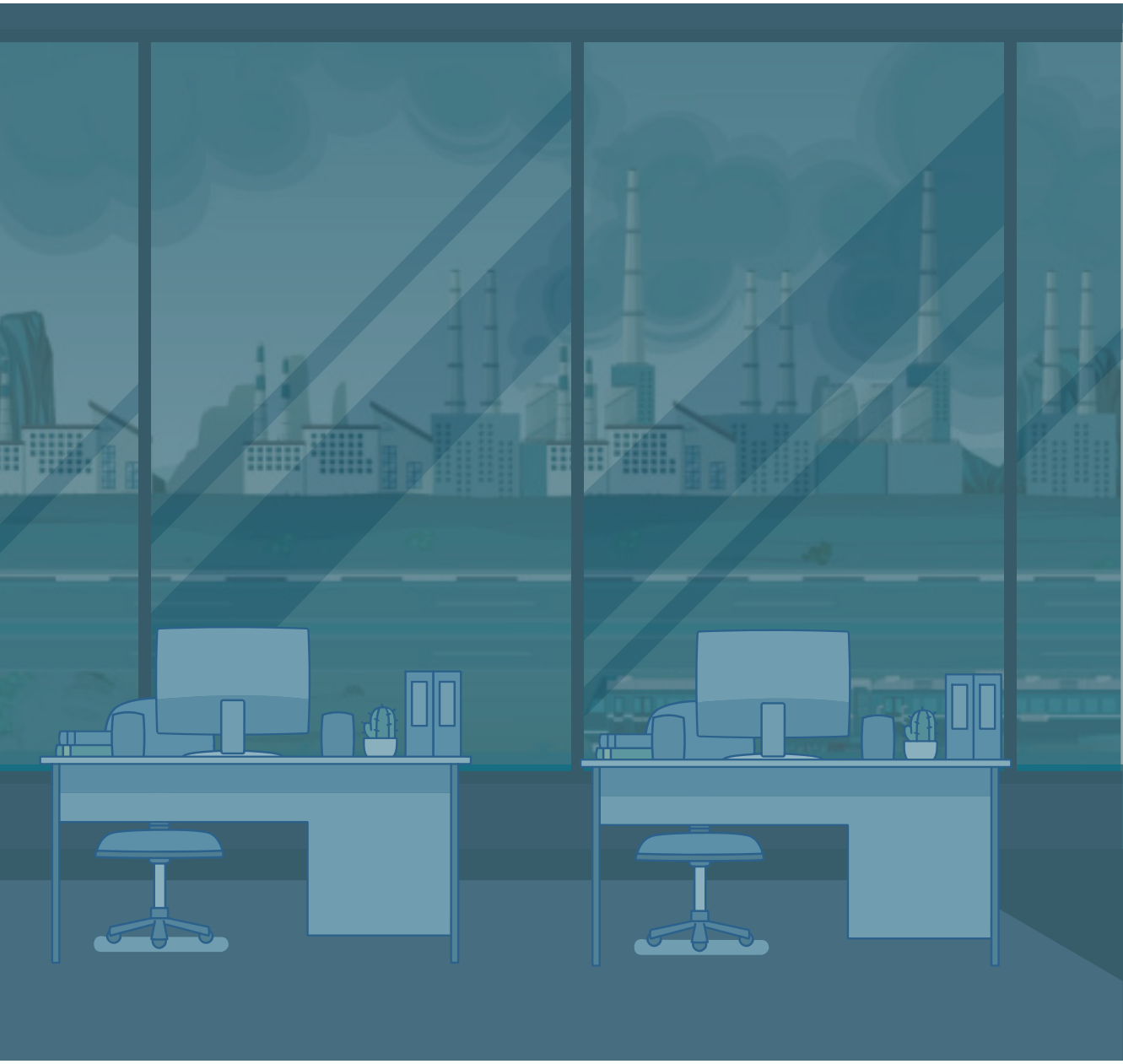
KCSS
Kosovar Centre for Security Studies

EMERGING THREATS PROGRAMME

ROAD TO RESILIENCE:
Governance and Capacity Building in Kosovo's Cyber Defense and Critical Infrastructure



March 2024

EMERGING THREATS PROGRAMME

Author: *Chris J. Dolan*

About the Emerging Threats 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, critical infrastructure protection, disinformation and hybrid threats, 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.*

For more information, contact us at: **EmergingThreats@qkss.org**

KCSS
Kosovar Centre for Security Studies

ROAD TO RESILIENCE:
Governance and Capacity Building in Kosovo's Cyber Defense and Critical Infrastructure

March 2024

Table of Contents

Executive Summary

The government of Kosovo (GOK) has made cybersecurity and critical infrastructure protection national priorities. GOK enacted the Law on Cyber Security (LCS) and Law on Critical Infrastructure LCI) and adopted the Kosovo Security Strategy (KSS) and Cyber Security Strategy. It also established a Cyber Security Agency (CSA) designed to function as a central hub for coordinating GOK cyber agencies and protecting cyber assets across various sectors. In addition, GOK prioritized governance and capacity-building in cyber defense and identification of key sectors in critical infrastructure.

But challenges remain and more work should be completed if Kosovo is going to build resilience to cyberattacks and secure its infrastructure sectors, especially in energy, e-governance, and telecommunications. More people in Kosovo, as well as across the Western Balkans, use information and communication technologies (ICT) today than ever before, which means more cyber incidents and attacks will take place. 95% of Kosovo's population between the ages of 16-74 access the Internet on a regular basis and broadband coverage and 5G telecommunications increasing on an annual basis. Kosovo has witnessed an increase in cyber violations and crimes, targeting telecommunications, financial institutions, and e-government services. From 2020 to 2023, Kosovo experienced a significant increase in malware, social engineering, and ransomware attacks with many going unreported to authorities. Moreover, Kosovo's public institutions are targeted on a regular basis. High profile attacks targeted Kosovo's Central Election Commission, Kosovo Telecom, and e-Kosova. The Cybercrime Investigations office in the Kosovo Police maintain records of arrests and apprehensions of suspected cybercriminals.

As cyber threats and attacks against Kosovo's critical infrastructure sectors and public institutions become increasingly more sophisticated, the GOK must be relentless and vigilant in its pursuit of resilience concepts through capacity-building efforts and connecting capacity with governance frameworks GOK has passed key legislation, drafted strategic guidance documents, and established agencies to address cyber threats. While governance has improved and cyber agencies are in place, capacity-building remains a challenge. The GOK must work with its international partners, build, maintain, and expand partnerships with Kosovo's dynamic private sector, and promote cybersecurity education and awareness.

In 2023 and 2024, KCSS published analyses of critical infrastructure and cybersecurity. These include guidance on digital threats and capacity-building in NGOs, best practices and guidance in Kosovo's critical infrastructure sectors, modeling critical infrastructure protection approaches developed by the Baltic States, Kosovo's critical infrastructure protection in a comparative regional perspective, alignment of the Law on Critical Infrastructure with European Union NIS2 Directive, and a cybersecurity handbook on incident response, data protection, and Internet safety.

This report relies on open-source assessments of publicly available information and structured interviews with Kosovo's stakeholders in public institutions and the private sector to assess progress in governance and capacity. It analyzes legislation and governing frameworks on

cybersecurity and critical infrastructure, strategic guidance, and agency operations and capacities. The report concludes that whole-of-government and whole-of-society efforts are needed to keep Kosovo on the road to resilience.

Findings

Kosovo's cyber defense posture and critical infrastructure protection capacities rest on building a resilient society and prosperous economy, protecting data and privacy rights, and securing digital assets. But Kosovo is building capacities from the ground up. Based on these observations, this report issues the following findings:

1. **Laws and strategic guidance:** the Law on Cyber Security (LCS) and Law on Critical Infrastructure LCI) and the Kosovo Security Strategy (KSS) and Cyber Security Strategy are significant legislative achievements that collectively view cyber threats, risks, and vulnerabilities as national security priorities. Creation of the Cyber Security Agency is a significant step toward boosting Kosovo's cyber defense posture and resilience.

2. **Cyber Security Agency (CSA):** While legislative achievements, reforms, and strategic guidance reflect GOK emphasis on strengthening governance in cyber defense and building critical infrastructure protection, CSA must receive necessary support as it becomes operational in overseeing cyber policy implementation and incident response. Centralized agency coordination is needed to ensure that legislation, strategic guidance, and capacities are aligned and that the voices of key stakeholders are heard.

3. **Capacity Building Needs:** Continuous improvements are needed to attract and retain an expert cyber workforce in public institutions, international partners and public-private partnerships are key pillars in cybersecurity and critical infrastructure protection, accessing advanced technologies and applications will boost threat intelligence, vulnerability scanning, and risk mitigation, and cybersecurity education and awareness are essential pillars in whole-of-government and whole-of-society resilience.

Introduction

With the Law on Cyber Security (LCS) and Law on Critical Infrastructure LCI) and the Kosovo Security Strategy (KSS) and Cyber Security Strategy, GOK now views cyber defense and critical infrastructure protection as national security priorities. Laws and strategic guidance serve as governance frameworks for agencies responsible for securing energy, telecommunications, e-government services, transportation, and financial institutions.

However, leaders must do more to work with international partners and the private sector to build and expand capacity as Kosovo transitions from digitalization of operations to cybersecurity. Resilience measures are needed to enable critical infrastructure sectors and institutions to recover, withstand, and adapt to disruptions from cyberattacks, physical damage, and climate change. International partners provide guidance on resilience concepts. The European Commission defines critical infrastructure resilience as ensuring stability and regular functioning of everyday social and economic life. This is applied to Kosovo through alignments

with European Union directives and governing entities.

USAID embraces task-oriented initiatives via Critical Infrastructure Resilience Activities (CIRA). USAID Kosovo adapts CIRA principles to developing robust activities and tasks in Kosovo's eleven critical infrastructure sectors. CIRA is a significant investment in Kosovo's economic development, national development, and public. Specific tasks include strengthening Kosovo's governance frameworks and capacity building through, for example, cyber workforce development, training personnel on cyber threats, smart technologies, and CERT. Other activities include threat intelligence, vulnerability assessments, and risk mitigation. Information sharing is another critical component as it promotes interagency communication and collaboration with the private sector on incident response and best practices.

The effectiveness of CIRA is influenced by planning, development, and implementation plans to upgrade and maintain critical infrastructure and boost resilience to climate-related risks to the public. Climate risks elevate the need to promote early warning systems for droughts, floods, and extreme heat, allowing critical infrastructure operators to make proactive decisions and mitigate disruptions to the public and business in Kosovo.

Governance of Kosovo's Cyber Security

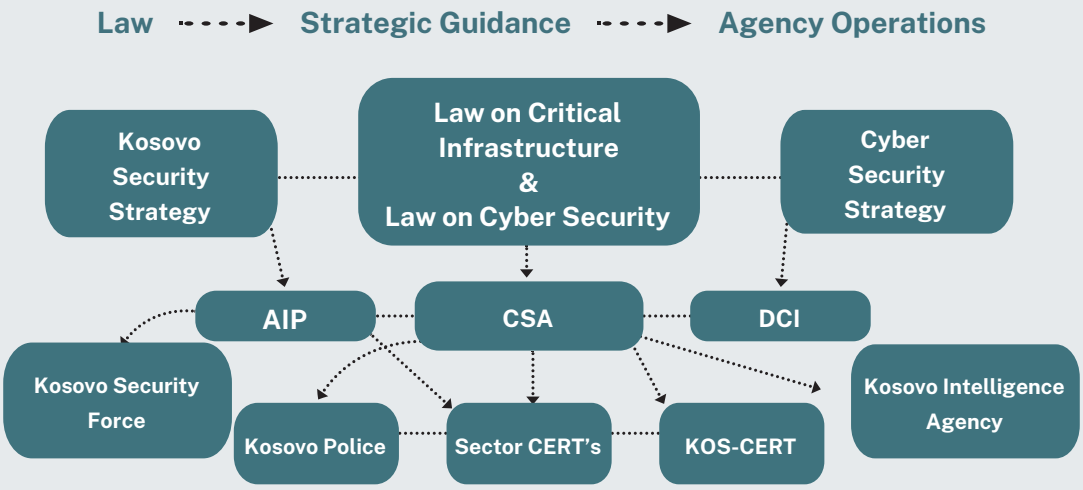
GOK is working to develop a coherent legislative framework to address discrepancies between current legal frameworks and implementation of newly created agencies with responsibility for cybersecurity and critical infrastructure protection. This means GOK must purposefully align legislation with leading documents that set strategic priorities for protecting Kosovo's cyberspace and critical infrastructure sectors. Legislation and strategic priorities are designed to guide agency operations and coordination of existing and emerging public institutions.

Laws and Legal Frameworks

Kosovo adopted the Law on Cyber Security (LCS) and established the Cyber Security Agency (CSA). LCS provides the legal framework for formulating cybersecurity policy and management, regulation of cybersecurity agencies, and combating cybercriminal activities. While KOS-CERT along with other national teams like CERT-KP-RKS, CERT-KSF-RKS, ICT Academy CERT, and UBT-CERT are responsible for incident tracking and response, once fully operational CSA will work with CERT to provide 24-hour/7-day incident response and secure cyberspace.

Like the LCS, the Law on Critical Infrastructure (LCI) oversees Kosovo's 11 security sectors. The sectors include public health, energy, water supply, agriculture, ICT, public health, financial services, government institutions, national values. transportation, and national goods. The law defines critical infrastructure as an array of sector specific "systems and assets, whether physical or virtual" while prioritizing risk mitigation and boosting national security and social wellbeing. But strong and effective governance means aligning the LCS and LCI the Kosovo Security Strategy of 2022-2027, Cyber Security Strategy, and critical infrastructure resilience activities.

A hands-on approach to governance is needed to ensure public institutions cooperate with one another and collaborate with the private sector. It must also ensure that governance, capacities, and agencies operations are aligned. Legislation and strategic guidance must inform GOK agencies, especially the Cyber Security Agency, KOS-CERT and sector specific CERTs, the Agency for Information and Privacy, the Division of Critical Infrastructure, Kosovo Police, Kosovo Security Force (KSF), and the Kosovo Intelligence Agency.



Key Cyber Security Strategies

The Kosovo Security Strategy (KSS) of 2002-2027 provides general guidance in governance of cybersecurity and cyber capacities, innovation and technology, and critical infrastructure protection. KSS sets four strategic focus areas including protecting national sovereignty and territorial integrity, securing the constitutional order and public safety, promoting human security and human development, integration within Euro-Atlantic institutions and norms. The design of KSS is modeled on the U.S. State Department's Integrated Country Strategy.

Cybersecurity and critical infrastructure fall under KSS provisions for protecting national sovereignty and territorial integrity and energy security and digital transformation under human security and social development. Kosovo's leaders must therefore ensure that action items are grounded in KSS guidance. Cyberattacks, data breaches, and disinformation campaigns are risks to Kosovo's national security as much as conventional weapons. The GOK should remain committed to improving cyber defense capabilities, incident response infrastructure, and raising cyber threat awareness. While KSS acknowledges Kosovo's challenges in cyber space, greater capacity is needed in recovering from and responding to cyber and physical threats, risks, and vulnerabilities.

KSS leaves the details of cybersecurity governance to the Cyber Security Strategy. This document directs cyberoperations and enhances resilience and cyber defense in Kosovo's 11 critical infrastructure sectors. It establishes frameworks that commit the GOK to strengthening through investments in cyber defense, innovation, technologies and procurement, personnel development and building cybersecurity capacities across public institutions.

The Prime Minister's Office of Good Governance created the Cyber Security Strategy in 2022 with support provided by Cybersecurity Capacity Maturity Model for Nations (CMM) through the Global Cyber Security Capacity Centre (GCSCC). The strategy is to strengthen

cyber defenses and critical infrastructure through public-private collaboration, institutional development, legal frameworks, capacity building, incident response, and cooperation with international partners, institutions, and non-government organizations.

Existing cybersecurity efforts have fallen on law enforcement. Cybercrimes and identity theft are law enforcement issues but cyberattacks are malign operations designed to cripple entire critical infrastructure sectors, thereby threatening Kosovo's national security and economy. Clearer guidelines are needed to improve CSA coordination and leadership of Kosovo's cyber defense and critical infrastructure measures.

Institutions Relevant to Cybersecurity and Critical Infrastructure Protection

The Cyber Security Agency (CSA) was created as the lead agency in response to increased cyberattacks against Kosovo. The agency will have responsibility for protecting Kosovo's cyberspace, implementing cyber defense measures, supporting KOS-CERT and incident response, and securing information systems. However, CSA is currently being established and not fully operational.

Once it becomes functional, CSA will play a crucial role in safeguarding Kosovo's digital infrastructure and cyberspace. With the general acknowledgment of cyber defense in the Kosovo Security Strategy and cybersecurity featured in the Cyber Security Strategy, CSA is expected to serve as a national security organization subject to best practices, ethical guidance, and compliance. CSA should ensure that only trained professionals with knowledge, skills, and experience in cybersecurity and dedicated to the mission will fill positions. CSA decision-making processes must be in consultation with colleagues and stakeholders in other agencies and ministries informed by private industry, academia, and civil society groups.

One area that needs greater definition and refinement is protecting e-government services such as the e-Kosova platform. As of now, e-government is monitored and overseen by the Information Society Agency (ISA), which along with CSA is organized within the Ministry of Internal Affairs. ISA also supervises ICT implementation in public institutions. Another is how CSA will interface with the Regulatory Authority of Electronic and Postal Communications (ARKEP), which oversees electronic communications and postal facilities utilized by e-government services.

Once CSA assumes operations, it should advise and provide security assessments for e-government services and other critical sectors. ISA and ARKEP can still integrate cybersecurity considerations into their regulations and technical standards. Kosovo's Agency for Information and Privacy (AIP) is entrusted with protecting data privacy, and addressing data leaks, and implementing ethical and legal compliance measures within legal and regulatory guidelines. AIP also protects public access to information and ensures accountability in governance. Data Protection Officers (DPOs) enforce these provisions in public institutions.

AIP investigates public complaints against government agencies if personal data and privacy are breached, punishes violators, and ensures compliance. AIP even oversees online portals

offering access to public information and documents and promotes awareness and educates the public and business about privacy and data protection. AIP also promotes public cyber awareness so people and businesses can make better decisions in protecting their own data while also utilizing AIP as a resource. Governance should ensure that AIP's voice is heard in the Cyber Security Agency. For it to remain effective, AIP needs more trained DPOs to support and expand its role in protecting public institutions from data leaks, breaches, and privacy violations. Key to this is ensuring the best and most qualified talent are hired and retained as well as regular and continuous training on data protection best practices.

Agency operations, however, should be streamlined. Ministry of Internal Affairs structures, developing bylaws, and regulatory frameworks must be harmonized to avoid competition and siloing between GOK cyber agencies. Greater definition and specificity is needed in delineating CSA roles and responsibilities in critical infrastructure protection relative to the Division for Critical Infrastructure (DCI). DCI protects Kosovo's 11 infrastructure sectors, conducts risk mitigation, and coordinates security protocols consistent with mandates in the Law for Critical Infrastructure (LCI). Building connections between cyber defense and critical infrastructure through governance frameworks and interagency cooperation is paramount.

In the past, support for DCI operations was lacking. As of 2022, DCI was comprised of just six staff members including the director with responsibility for Kosovo's 11 critical infrastructure sectors. Just six individuals were entrusted with the responsibility for telecommunications, energy, and hospitals among other sectors. DCI is also hampered by capacity challenges and impediments to building operational critical infrastructure sectors. DCI and CSA must cooperate and coordinate with one another and collaborate with the private sector and U.S. and E.U. partners.

Centralized Governance

While not fully operational, CSA is positioned as the nerve center for cybersecurity rules, management, and policy regulations as well as interagency coordination and holds cyber agencies accountable to the Kosovo Security Strategy and the Cyber Security Strategy. CSA is also designed to coordinate and monitor critical infrastructure and cyber agency activities and operations, manage and oversee incident response with KOS-CERT and sector specific CERTs, and intelligence and information sharing. CSA will be responsible for adhering to the strategic vision of cyber security, identifying risks and vulnerabilities, and developing threat intelligence assessments of patterns and trends in the broader landscape. The Kosovo Intelligence Agency and Kosovo Security Force must be part of this process given the assets they bring to strategic guidance and operational capacities.

Cyber decision-making processes should take place through the CSA and KOS-CERT to ensure that incident response, risk mitigation, vulnerability analysis, and workforce development, connect with one another. A centralized decision-making system with a resourced CSA leading and coordinating the process will increase resilience and strengthen Kosovo's position in fighting cybercrime, hacks and cyber incidents in critical infrastructure, and data breaches.

Getting to Resilience

Getting to resilience means that Kosovo's governance frameworks should prioritize human capital. Developing competence and expertise in both the public and private sectors on strategic, operational, and technical levels are consequential in resilience. Governance is about ensuring capacity is aligned with rule of law and strategic guidance. But governance in the absence of a dedicated commitment to capacity is not governance.

Kosovo's cybersecurity and critical infrastructure agencies must have resources to fulfill their missions and achieve objectives according to ethical guidelines and best practices. They must have the authority to respond to cyber incidents as well as the power to assess them, collect and analyze intelligence and information, protect privacy rights and data, and collaborate with law enforcement, businesses, and international partners. Only a competent, well-trained, and well-compensated cyber workforce can execute these tasks.

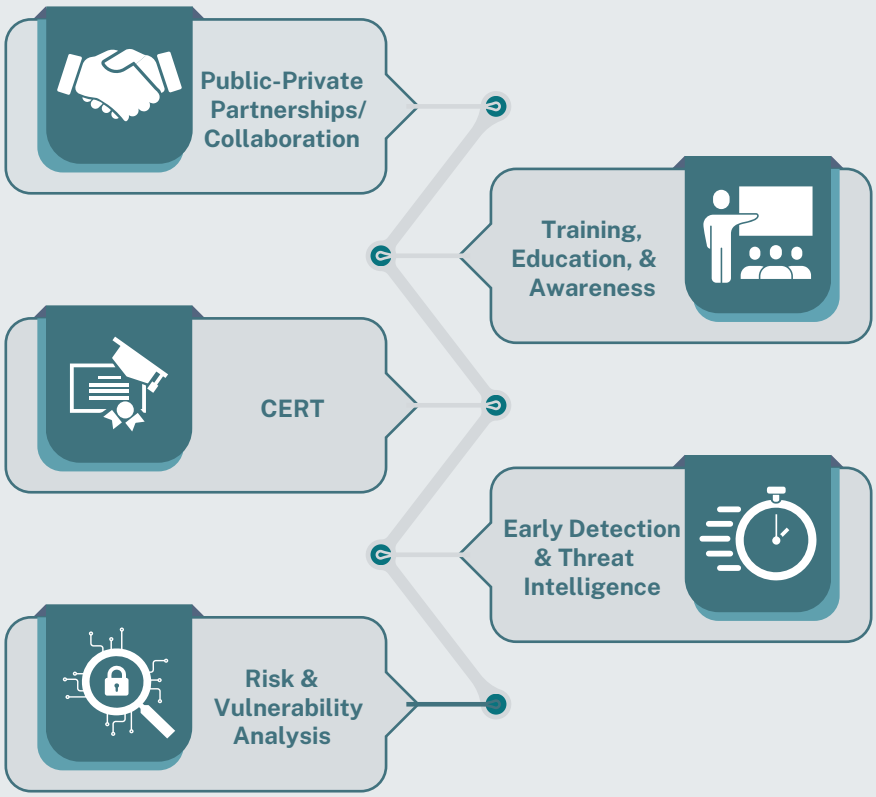
If Kosovo is going to effectively recover from and withstand future attacks from malicious actors and climate change, then it must connect governance with capacity. Kosovo's governance framework should prioritize the building of a cybersecurity workforce and a cybersecurity mindset.

Capacity-Building

Building capacity is essential to Kosovo's cyber defense and critical infrastructure resilience. DCI and AIP, and soon with CSA, will play critical roles in protecting Kosovo's digital spaces, mitigating risks and vulnerabilities, strengthening threat intelligence, and responsibly using technologies. Included in these measures are cybersecurity education and awareness, KOS-CERT, and threat intelligence with CSA and public-private partnerships at the center of all three.

A trained workforce responsibly using technology also plays a key role in building critical infrastructure and climate resilience. While technologies and tools are readily available for use in early detection and threat intelligence, personnel in public institutions must also engage in professional development to keep up with best practices. Humans must remain in the loop.

ZONAT E NGRITJES SË KAPACITETEVE



Higher Education, Training, and Public Awareness

CSA and other agencies are critical in promoting public awareness in cybersecurity and critical infrastructure resilience. Education and outreach campaigns, conferences and workshops, engagement with universities and schools, and collaboration with civil society groups are critically important in building cybersecurity and resilience.

There are educational mechanisms which have been operational in Kosovo for many years that serve as wellsprings of cybersecurity knowledge and research. This includes public and private institutions of higher education and non-governmental and private consulting sectors. While there are some universities and colleges in Kosovo that offer cybersecurity and ICT degrees, more work should be done to ensure that connections and pipelines are created and maintained between GOK cybersecurity and critical infrastructure agencies, institutions of higher education, and training programs.

The Rochester Institute of Technology-Kosovo offers a B.S. in computing and information technology and ICT training and professional development courses, and maintains a Cyber Security and Internet of Things project. Also, AAB College offers undergraduate degrees in cybersecurity and programming and a graduate M.S. program in computer science. It also operates a Cyber Security Center Lab that focuses on online data security.

The University of Business and Technology (UBT) offers cybersecurity and ICT programs and centers focusing on Cyber Security and Privacy, Software Development and Innovation, Modeling and Simulation, and Statistics, Data Processing, and Forecasting. UBT also maintains the UBT-CERT Incident Reporting System that receives reports on cyber and data breaches and vulnerabilities. The University of Prishtina maintains cyber education projects in Cyber Hygiene e-Learning course, cooperative projects using Internet of Things technologies, and research and innovation. The University of Gjilan offers an undergraduate program in computer science and a graduate program in control systems and artificial intelligence and another in e-governance.

Academic institutions in Kosovo offer ICT educational programming and have synergies with the business community. But while there is a dynamic private IT sector in Kosovo, there is little emphasis on cybersecurity partnerships with GOK cybersecurity and critical infrastructure agencies. The GOK released a document in 2023 specifying articles for the creation of Kosovo's State Cyber Security Training Center that was supposed to fulfill the goals of building a culture of cybersecurity and developing training programs. The mission and articles place the SCSTC within the Ministry of Defense and the Kosovo Security Force. The document references the creation of a Cyber Range to model and simulate cyberattack patterns and vectors.

Other than the publication of articles, the SCSTC is not functional. Information provided indicates that SCSTC will not assume its duties as a training center until March 2024 at the earliest. The Law on Cyber Security re-actualizes state-supported cyber security training centers. However, few concrete steps have been taken, which could mean that the Cyber Security Agency will play a greater role in state-supported training programs.

Cybersecurity training centers do exist in Kosovo, but in the private sector. Cyber Academy offers a fully developed curriculum on cybersecurity training as well as professional development options for firms seeking to boost the cyber competencies of their employees. Also, CISTCK is a software company and consultancy that specializes in penetration testing, vulnerability analysis, threat intelligence and early detection, and security control audits. Furthermore, Sentry Cybersecurity offers clients training programs in U.S. National Institutes of Standards and Technology (NIST) and the Open Worldwide Application Security Project (OWASP) at enterprise scale to secure applications from cyberattacks. In addition, Cactus Education is an NGO and consulting firm that offers two professional programs of study in system and network administration and web and mobile application development.

In the non-government sector, Innovation Centre Kosovo, which offers cyber training courses and business consultation. Specific programs include the Cyber Unity Academy, Cyber Training, International Cyber Security Exercise, One Step Ahead Cyber Security Education, Cyber Defense Week, and Crypton. However, there other entrants into this are, namely the Albanian Cyber Association, an NGO that works with civil society groups to raise cybersecurity awareness to the public and promotes competitions and professional development.

A better trained and experienced cyber workforce in public institutions will improve incident response and recovery. But the public sector is lacking in this area and is beyond the private sector in offering training programs and raising public awareness about safe internet use. Capacity-building measures should prioritize these efforts by developing partnership programs with higher education institutions and the private sectors.

Cybersecurity and critical infrastructure agencies should develop career incentives to attract and retain talented professionals in public institutions to mitigate brain drain. Embrace experiential learning programs with universities and colleges and NGOs and consultancies to build a pipeline of talent and offer sound compensation and benefits packages that compete with the private sector. Then, offer professional development so the cyber workforce can stay up to date on ethics, best practices, operations, and technologies.

This means GOK cyber security legislation and regulatory frameworks need greater alignment with private sector cyber companies and critical infrastructure operators. Kosovo's Ministry of Economy and Ministry of Education need resources to encourage Kosovar youth to remain in the country and secure positions in the public sector cyber workforce. Consequential to this is developing and sustaining norms valuing public institutions and private sector businesses in cybersecurity and critical infrastructure resilience.

Public-Private Partnerships

To accomplish these tasks and sustain them over time, public institutions and the private sector should be partnering with one another in the spirit of collaboration. Building a culture of public-private partnerships will help cybersecurity and critical infrastructure resilience in Kosovo. Public institutions struggle to establish cyber resilience due to lack of trained cybersecurity personnel and aging ICT infrastructure. Public institutions can learn from

the private sector and should partner with firms and businesses in information sharing, secure technologies, cyber education and awareness, and professional development and training of cyber personnel. Public-private collaboration is a challenge but needs attention if cybersecurity and critical infrastructure resilience will come to fruition in Kosovo.

Kosovo's private sector is concerned with protecting their financial assets, customer data, privacy, and intellectual property. However, smaller companies lack resources to develop cybersecurity measures and use technologies for threat assessment and incident response compared with public institutions entrusted with macro-level critical infrastructure protection, securing public data and privacy, and public safety.

Existing resources can facilitate collaboration between Kosovo's public institutions and private companies. Innovation Centre Kosovo (ICK) assists and supports private sectors firms with consultation, training, and innovative solutions. ICK provides office space, advising, and educational programs, workshops, and public events to startups and firms in different sectors. ICK has a strong record of success in facilitating partnerships and collaborative programming.

Also, Cyber Zero, which is supported by U.S. Embassy Pristina, provides resources for stakeholders in agencies and cyber firms to engage one another on best practices, ethics and compliance, and cyber threats. It also serves as forum for knowledge-sharing and innovation that should be utilized by stakeholders in public institutions to learn from the private sector.

Developing Capacities in Critical Infrastructure Sectors

Critical infrastructure operators in energy, e-government services, and telecommunications are increasingly dependent on digital technologies vulnerable to cyberattacks. In Kosovo's energy sector, threats consist of DoS attacks on power grids, cyberattacks on control systems, and manipulation of energy data. Energy sector vulnerabilities include limited resources and budget constraints that prevent state of the art solutions to sophisticated and targeted attacks and lack of cybersecurity experience.

Procedures and processes should implement security protocols for Supervisory Control and Data Acquisition (SCADA) systems, thereby limiting the need for on-site personnel. This is important for managing the power grid, water treatment facilities, energy, transportation, and telecommunications. For power grid management, SCADA systems monitor voltage and power flow, enabling critical infrastructure operators to ensure regular operations, detect threats, mitigate risks, and contain faults. SCADA systems enable remote control of substations and other equipment and boost efficiencies. They also help with understanding and monitoring energy demand and distribution. In water systems, SCADA systems enable operators to oversee continuous and automated water treatment for clean and safe for public consumption and to identify faulty pumps and valves. Effective SCADA monitors for alterations in water flow and oversee reservoirs and distribution.
Other areas demand sound implementation of SCADA systems. This is especially the case for tracking and ensuring safe and efficient distribution and transportation of oil and natural

gas in Kosovo. SCADA systems should also monitor data on traffic flow, congestion, and auto incidents and communicate with law enforcement. This will allow for automation of tasks and operations, mitigate disruptions and incidents, and promote reliable infrastructure management.

In telecommunications, threats include data breaches, infiltration in digital networks and cyberespionage, eavesdropping in communication networks, and SIM swapping. These threats can exploit inadequate data security, poor authentication protocols, antiquated software, and internet of things (IOT). Cyber procedures focus on data encryption, multi-factor authentication (MFA), regular software updating, and continuous improvements in network monitoring. However, the Ministry of Internal Affairs institutional mechanisms should ensure these procedures are fully realized.

E-government services ensure effective public administration of digitalization of electronic services. Kosovo's government has prioritized the development of e-government services through an e-government strategy (2023-2027) that came into effect in 2023. The strategy is designed to make digital interactions with government services user-friendly experiences while also minimizing citizens' frustration, mitigate public costs, and enhance national economic growth. The e-government strategy determines the overall vision for advanced digitization of public policy implementation and public administration and transparency. Positive user experience with e-government services enhances public faith and trust in Kosovo's government and positive interactions with administrative services improve effectiveness and accountability.
Kosovo's citizens can access and use the e-Kosova platform, which serves as a one-stop shop for electronic public services. e-Kosova services include taxes, public health, social services, vehicle registration, citizenship status, property regulations, municipal services, judicial proceedings, ombudsman, pensions, grants and subsidies, education, consular affairs, legal audits, labor and employment, and document verification. After users create accounts through verified means of registration in required areas, they can access services and programs. e-Kosova has been successful in digitizing public services that were once exclusively in-person.

However, risks and vulnerabilities remain. On September 5, 2022, e-Kosova and other government services were targeted in a distributed denial-of-service attack that disrupted services, overloading regular e-government functions. While the risk was mitigated additional resources for trained CERT is needed to understand cyberattack patterns and trends and collaborate with the private sector and international partners.

Early Detection and Threat Intelligence

Intrusion detection systems, firewalls, and monitoring tools will help track cyber threats and secure critical infrastructure operations. Access controls and encryption reduce the dangerous effects of cyber incidents and enhance recovery from disruptions and attacks. Enhancement of cyber workforce training, professional development, and public outreach

complement these measures. Secured communications and information sharing systems will promote cooperation and partnerships when critical infrastructure sectors are under attack or experience outages. Analytic tools and software can help security personnel make effective data-driven decisions, develop risk analyses, and make more optimal investments and resource allocations.

Credible and strong threat intelligence serves as a vital instrument in Kosovo's cyber security and critical infrastructure as it can help incident response through identification and assessment of cyber threats and malicious actors. Threat intelligence is essential in cyber defense and critical infrastructure because it helps with early detection through identification and monitoring of emerging threats before malicious actors inflict damage. Threat intelligence assists with understanding threat actors' tactics, techniques, and procedures (TTPs) and the extent to which threats conform to patterns and trends over time. This will better inform agency budgets by helping direct resources to priority areas.

Threat intelligence also helps protect critical infrastructure, especially the energy, transportation, and telecommunications sectors. In energy, threat intelligence can reduce risk to pipelines, electric grids, and power stations/substations by viewing trends in the threat landscape. In transportation, it can minimize risks to airports and air traffic controls and roadways. In telecommunications, threat intelligence can identify patterns in malicious activity in internet service providers and mobile networks before they attack.

Kosovo's Cyber Security Strategy prioritizes the development of credible and accessible threat intelligence with open-source intelligence collections and analysis of publicly available information. A culture of threat intelligence and information sharing with public institutions, namely the Agency for Information and Privacy, Division for Critical Infrastructure, the Kosovo Intelligence Agency, and Kosovo Security Force and external actors like the U.S. Cyber and Infrastructure Security Agency (CISA), the E.U. Agency for Cybersecurity as well as cleared personnel in private threat intelligence firms.

Software and other applications are available for subscription and should be purchased. For example, Alien Vault provides real-time reporting on emerging threats, attacks, and vulnerabilities using various public sources. This allows threat analysts to gain insight and assess the threat landscape as it evolves and unfolds. Alien Vault's Open Threat Exchange is an open environment with experts sharing intelligence on emerging threats. Professional and responsible analysis of threats before they attack is essential to cybersecurity and data protection.

Risk Mitigation and Vulnerability Assessment

Cybersecurity and protecting critical infrastructure mean conducting regular risk mitigation and vulnerability scanning. Kosovo's digital infrastructure is especially vulnerable to cyber incidents and attacks from governments, proxy groups, and cyber criminals. Malicious state and non-state actors exploit weaknesses, disrupt essential services, commit cyberespionage, empty bank accounts, and steal proprietary information. They also combine malware and

ransomware attacks with physical acts of terrorism, sabotage, and other violence.

CSA and DCI should follow the World Bank's diagnostic risk assessment report to mitigate threats and vulnerabilities in critical systems. Hiring, training, promoting, and supporting personnel through professional development programs and initiatives support risk assessment, threat mitigation, and incident response. Vulnerability assessment and scanning and risk analyses are for resilience purposes and implementing protective measures. Enhancing access to technology will play a vital role in establishing critical infrastructure resilience in Kosovo as the country confronts cyber threats, cyberattacks, and climate change. Conducting regular and continuous vulnerability scanning using software applications helps with vulnerability detection in key sectors.

Public institutions need access to tools and software applications to assist their vulnerable scanning and risk mitigation efforts. For example, the Nessus vulnerability scanner is used in network security to assess computer ports, network operations, and probes for internal weaknesses that may be exploited by actors seeking to disrupt or disable critical systems. Qualys vulnerability management identifies and patches weaknesses across IT, operational technology, and Internet of Things.

Zeek is an open-source tool that monitors network traffic and develops transaction logs and file content for network analysis and review. Infrastructure and automation tools like Splunk and LogRhythm aggregate and analyze logs from public sources to detect incidents in real-time. Perhaps most impactful will be instilling multi-factor authentication (MFA) practices throughout Kosovo. MFA will prevent data leaks and unauthorized access to classified or proprietary information. CyberArk and Okta are platforms that can help with monitoring of permissions in critical systems. Moreover, data encryption tools can protect against unauthorized access and cloud services like Microsoft Azure and AWS Security protect data in a secure cloud architecture.

Responsible and ethical use of these tools is paramount as analysts should be cleared personnel who follow norms, laws, and regulations. Users must obtain authorization before using vulnerability scanners, network analysis, and threat intelligence collections and analysis. Regular training and professional development of personnel in responsible use of technologies and cybersecurity best practices are essential. Using technology in the absence of best practices, proper training, and compliance standards is not ethical.

RECOMMENDATIONS

1. Centralize and coordinate cyber and critical infrastructure operations. AIP and DCI need better integration within Kosovo's security decision-making processes and a strong working relationship with the Cyber Security Agency. The CSA should be at the center of this process.

2. Align and empower CSA, DCI, and AIP operations within Kosovo's Security Strategy and the Cyber Security Strategy with authority from legislation and legal frameworks. Connect governance with capacity by ensuring the Kosovo Security Strategy and National Cyber Security Strategy result in actionable items.

3. Develop whole-of-government training and professional development programs on cybersecurity principles and incident response. Build a trained, competent, and knowledgeable cybersecurity in Kosovo with state-supported training programs coordinated by CSA and partner with private sector firms and NGOs to maximize capacity.

4. Develop social/human capacity through a whole-of-society effort to promote public awareness about the risks of cyber threats and the need to report suspicious activity.

5. Map critical infrastructure sectors through a needs-based assessment across energy, transportation, water treatment, telecommunication, and e-government.

6. Support and practice regular vulnerability analysis and risk assessment by investing in secure software applications and tools and training on ethical and responsible use.

7. Collaborate with international partners and seek technical assistance from the private sector to share cybersecurity knowledge, threat intelligence, and best practices.

Katalogimi në botim – (CIP)

Biblioteka Kombëtare e Kosovës “Pjetër Bogdani”

355.02(496.51)(047)

Dolan, Chris J.

Road to Resilience : governance and Capacity Building in Kosovo’s Cyber Defense and Critical Infrastructure / Chris J. Dolan. - Prishtinë : QKSS, 2024. -14 f. : ilustr. ; 26 cm.

ISBN 978-9951-842-20-4

KCSS
Kosovar Centre for Security Studies

About KCSS

Established in April 2008, the Kosovar Center for Security Studies (KCSS) is a specialized, independent, and non-governmental organization. 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:

www.qkss.org
www.securitybarometer.qkss.org

@KCSSQKSS

ISBN 978-9951-842-20-4
9 789951 842204