Cyber Attacks and Critical Infrastructure in Kosovo

By Mejreme Asllani

DCAF *Young Faces* 2022 Participant

Abstract

This policy paper discusses the vulnerability of cyberspace and the rise in cyberattacks in Kosovo. The advancement of technology and the widespread usage of the Internet have also come with threats towards critical infrastructure and data privacy for public and private institutions. One of the major issues that Kosovo and the Western Balkans face is the lack of an effective legislative framework, as well as limited public awareness and harmonization of cyber security law with the critical infrastructure strategy and other national security initiatives. It is critical that the government further develops a relevant legislative framework that is easily applicable to the context. This policy brief provides suggestions for governments and key stakeholders about cyberspace and critical infrastructure protection.

Keywords: cyberattacks, cybersecurity, critical infrastructure, law, strategy, data privacy

Introduction and Context

The rapid advancement of technology has enabled cybersecurity to become one of the most pressing issues confronting governments today. Despite its valuable contribution to the growth and development of societies and nations, it is not without drawbacks. The World Economic Forum claims that cyberattacks and cyberwarfare are the most serious threats concerning cyberspace. The digital revolution and its use by governments, people, private and public enterprises, criminal groups and non-state actors, have expanded substantially in recent years. As a result, the potential threat of major state assets such as critical infrastructure disruption, with serious consequences for national security, is widely visible in all countries. Such cyberattacks impact not just underdeveloped countries but even the most developed ones. Many cyberattack cases have been reported in Western Balkan countries. In the last two years, Kosovo has faced an increased number of cyber violations and cybercrimes e.g., phishing, malware, data theft and ransomware DDoS[1], in online media[2], banking, private businesses, and government websites[3]. According to the Kosovo Agency of Statistics[4], 95.3% of the population ages 16-74 used information technology and communication in 2021. Because Kosovo is a new country with fragile institutions and a high percentage of people use the internet, the risk of exposure to cyberattacks and cyber intrusions is costly.

According to BIRN[5], the most prevalent violations in cyberspace have been fake news during the Covid-19 pandemic, information security breaches, propaganda, threats and hate speech. Citizens, political parties, public personalities, state entities, financial institutions, and journalists have all been targeted by cybercriminals.[6] In April 2020, a significant cyberattack hit the Economic Bank, which resulted in the publication of private customer data with information on financial transactions.[7] Online media such as Gazeta Express, infokus.com (where 300 articles were deleted) and Kosovo's Independent Media Commission were subjected to a severe cyber-attack in January 2022. The cyberattack resulted in a loss of data, access to official email addresses and internal systems for almost two months.[8] Cyberattacks have also targeted commercial companies such as HIB Petrol and other government institutions. These cyberattacks demonstrate Kosovo's cyberspace vulnerability and the potential risk to human rights, data privacy violations, destruction of business activities and profits, and critical infrastructure endangerment. The most contentious instance was the transfer of two million euros from the Ministry of Economy, respectively, from the Treasury of Kosovo.[9] The transfer was conducted by an insider -- an employer who used fake accounts to gain access to the system and execute the transfer. The investigation regarding the official duty abuse is ongoing, and the Ministry of Economy has not been able to return the stolen money yet.

In 2018, an additional cyberattack on Kosovo occurred after the imposition of a 100% tax on Serbian goods. Consequently, government websites and the emails of Kosovo diplomats have been subjected to cyber-attacks. According to data investigations conducted, interventions came from some countries in the region[10]. During the parliamentary election in February 2021, the Kosovo Central Election Commission website was hacked, exposing weakness on official government websites. Recently, Kosovo has been facing multiple cyber-attacks on the Kosovo Police and government website.[11] Additionally, Kosovo has been subjected to a politically motivated cyberwar waged by Russia and Serbia through disinformation and fake news.[12] As a result, crimes committed in online settings exceed national boundaries, making it difficult to investigate and prosecute the cyber-offenders. Therefore, it is critical for the Kosovo government to be aware of such violations to invest in the capacity building and expertise to defend the people as well as national stability and security.

---

[1] Western Balkans: Emerging Cyber threats report, p.40
[2] https://kallxo.com/gjate/mendime/alarmi-kibernetik-per-mediat-ne-kosove/
[3] https://kallxo.com/komuna/analize-komuna/siguria-e-brishte-kibernetike-e-faqeve-qeveritare/
[4] KAS, 2021
[5] Online intimidation: Controlling the Narrative in Western Balkans, BIRN, 2021
[6] ibid.
[7] Western Balkans: Emerging Cyber threats report, p.29
[8] Kosovo's Independent Media Commission (IMC): https://balkaninsight.com/2022/03/10/kosovo-media-regulator
[9] GLPS: Kosovo in 2020-Cybersecurity: https://www.legalpoliticalstudies.org/kosovo-in-2020-cybersecurity/
[10] Cybersecurity if official websites: https://kallxo.com/komuna/analize-komuna/siguria-e-brishte-kibernetike
[11] The Risk from Russia's cyberattacks: https://kallxo.com/lajm/rreziku-nga-sulmet-kibernetike-te-rusise-ne-kosove/
[12] Fake News: https://kallxo.com/lajm/lajmet-e-rreme-ne-kosove-te-sponsorizuara-nga-rusia

Legal framework

Kosovo's legal framework is one of the most advanced in the region, making visible progress in harmonizing the cybersecurity legislation and strategy with the European Union framework[13]. However, significant limitations persist when it comes to implementation and cyberattack prevention mechanisms. The first 'Cyber Security Strategy and Action Plan 2016-2019' was approved in 2016, making Kosovo the second country in the Western Balkans, after Montenegro, to have such a strategy. The main strategic components of this strategy are critical information infrastructure protection, institutional development and capacity building, public and private partnership building, incident response, and international cooperation.[14] Additionally, the legal framework includes Law on Prevention and Fight against Cybercrime approved in 2010[15]. The new Draft Law on Cyber Security was initiated in 2020, but it has not been completed. There is also a Law on Interception of Electronic Communication (2012)[16], Law on the Information Society Services (2013[17]) and Law on Information Society Government Bodies (2013)[18], and National CERT/CSIRT/CIRT hosted by the Regulatory Authority of Electronic and Postal Communication[19]. The law on Cyber Security is expected to be approved by 2022[20] based on EU Directives which will, "*establish[es] the principles of cyber security, the institutions that develop and implement cyber security policy, the responsibilities of the authorities in the field of cyber security, the duties of cyber security entities, inter-institutional cooperation, the prevention and combating of cybercrime in the Republic of Kosovo against any threat or attack, and establishes the National Authority for Cyber Security (...))*[21]. Consequently, the current legislative framework is not harmonized, and cyberspace is secured by several legislative policies rather than by a single legislation or plan[22].

The existing cybersecurity framework handles a limited set of cybercrimes, and reformation is required to adapt sophisticated technology to potential criminal cyber offenses.[23] Hence, to be more successful in law enforcement, there should be a law that regulates this field and provides clear guidelines for coordination and leadership in this regard, which is expected to be regulated by the new law on cybersecurity.

Critical Infrastructure

Critical infrastructure is one of the most vulnerable sectors that might be targeted by cyberattacks. Critical infrastructure is regarded as a vital pillar for a functional state, and its disruption would jeopardize national security and have a substantial impact on the state's assets. In Kosovo, critical infrastructure is regulated by the Law on Critical Infrastructure, which went into effect in 2019 and was drafted in compliance with EU regulations, the Croatian model and the American Patriot Act.[24] It contains 11 essential sectors; public health, energy, agriculture and food, water supply, public services, information and communication technology, financial services, government institutions, national values, national goods, and transport-- which are described as *"virtual or physical assets that are crucial to the state's operation, and disruption of such assets would have a significant impact on Kosovo's national security, public health, economy, and people's well-being.*"[25]Additionally, most of the critical assets are private owned, making the public-private partnership crucial in securing the functionality and protection of these vital sectors.

Despite having a legislative framework for critical infrastructure, the Ministry of Internal Affairs failed to build an institutional apparatus with enforcing provisions that would implement it. Critical Infrastructure is related to other sectors of strategic interest, such as national security strategy and defense strategy. Consequently, Kosovo institutions should prioritize the Critical Infrastructure and give

[13] European Commission. Kosovo 2018 Report
[14] National Cyber Security Strategy: https://kryeministri.rks-gov.net/repository/docs/
[15] Law No. 03/L-166: http://old.kuvendikosoves.org/?cid=2,191,490
[16] Law No. 04/L-109: https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851
[17] Law No.04-L-094: https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2811
[18] Law No. 04/L-145:https://gzk.rks-gov.net/ActDetail.aspx?ActID=8669
[19] DCAF -National Cybersecurity Strategies in WB, 2021
[20] Ecosystem article
[21] Draft Law on Cybersecurity: https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=40905
[22] See also: DCAF -National Cybersecurity Strategies in WB, pp.12-13
[23] Cybersecurity Capacity Review: https://me.rks-gov.net/repository/docs/
[24] KCSS, Critical Infrastructure in Kosovo, 2022, p.15
[25] Law on Critical Infrastructure: https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313

the right space under the strategies and papers now being created, such as the draft Cyber Security Law, draft National Security Strategy, and draft Counter-Terrorism Strategy.[26] It is critical for the Kosovo government to not only develop a solid legislative and regulatory framework, but also to accommodate current and real capacities, as well as to provide viable possibilities for future field improvement. Disparities between present legislation and implementation would become addressed, and effective measures to safeguard such assets from cyberattacks and other threats would be implemented.

Challenges

The most significant challenges that Kosovo faces in the cybersecurity governance area are similar to those other Western Balkan nations face. According to DCAF[27], one pressing issue is a lack of appropriate norms and regulations, as well as an absence of public awareness on the subject, which creates an easy setting for cyberviolence. Another national concern is the preservation of confidential national data by the government and institutions, which might threaten national security. Sensitive official data and information that are at risk to cyberattacks are not protected by adequate information security systems. Data privacy and fake news have been demonstrated to be some additional and relatively recent incidents that have led to confusion in society. Additionally, the low reporting of cyberattack violations is attributed to a variety of factors. Businesses, for example, are scared that if they make public cyber-violations and incidents involving their customers' data, they will suffer a loss. Therefore, they want to keep things hidden. Other elements that limit the efficiency of cyberspace defense are the lack of resources, the lack of a budget, incompetent institutions, and the lack of cyber experts to implement cybersecurity policy.[28]

Conclusions and Policy Recommendations

The fast advancement of digitalization, as well as human reliance on technology, is one of the most serious challenges that society faces and will confront in the future. States that have weak internal security and are in the developing phase, such as Kosovo but also other Western Balkan countries, will be more vulnerable to cybercrimes that can develop severe consequences, especially when it comes to Critical Infrastructure. These cyberattacks manifest in different forms - including data privacy violations, human rights violations and even jeopardizing national security. Even though Kosovo has a solid legal framework, it is required to finish the Draft Law on Cybersecurity and to have other adequate legislative regulations in power. Moreover, it is particularly important that the Government of Kosovo to include and prioritize in drafting of the National Security Strategy, draft Defense Strategy, and other relevant strategies the protection of Critical Infrastructure through e detailed cooperation between different stakeholders and specifically public-private partnerships. Different types of cyberattacks demonstrate that Kosovo needs to take precautions and work in this direction to respond to such cyberattacks threats and protect the people and national security. Therefore, my legal policy propositions that address these concerns are listed below.

- **Effective legal framework**. The complexity of cyberspace requires appropriate expertise and attention from the executive and legislative branches. The Covid-19 pandemic outbreak has postponed many draft laws and policies that have been in process. Hence, the government should begin completing and implementing such changes as soon as possible.
- **The Draft National Cybersecurity Strategy**. Initiated by the Ministry of Internal Affairs and National Security Strategy, this strategy should include current cyber challenges, and provide adequate preventive measures in line with EU Cybersecurity Strategy and relevant EU legislation. Additionally, the government **should prioritize Critical Infrastructure** and include it in the National Cybersecurity Strategy. Moreover, the National Security Strategy and Defense Strategy should be reviewed and include critical infrastructure in their framework without duplicating the strategy on cybersecurity.

[26] KCSS, Critical Infrastructure in Kosovo, 2022
[27] DCAF, National Cybersecurity Strategies in Western Balkan Economies, p.12
[28] Conway, M and Brady, Sh. "A New Virtual Battlefield - How to prevent online radicalization," p.8-9

- **Public awareness campaign.** In cooperation with the private sector and civil society, the government should launch an awareness campaign on the importance of cyberspace and usage. In this way, people would be aware of the risks of using the internet without previous knowledge. It is particularly important to invest in cybersecurity and data protection education, especially among youngsters through non-formal programs.
- **Harmonized policies.** While developing the Cybersecurity Law and other policies, the government and key institutions should prevent overlapping and duplication of legal provisions by clarifying roles amongst institutions.
- **Research and Development.** Kosovo has the youngest population in Europe and the highest rate of internet users (95.3 percent). This should be viewed as a benefit for the government in terms of investing in initiatives that engage youth in IT and cyberspace. As a result, a generation is being prepared to keep up with the cutting-edge advancement of technology.
- **Regional Cooperation**. The government should have a proactive approach to greater cooperation with other countries in the Western Balkans. Cyberattacks are mostly coming from outside of the WB states due to global trends. Therefore, greater collaboration amongst WB should be promoted to participate in the creation of shared platforms to prevent and battle cyberattacks and cybercrimes through collaborative efforts.
- **International Cooperation.** Institutions in Kosovo should intensify their efforts to participate in cybersecurity initiatives and projects, as well as to develop regional, European, and international partnerships. Kosovo cannot protect itself from hybrid cybercrime and cyberattacks on its own, thus broader coordination and cooperation is essential.

Bibliography

Abazi, Tanzer. "Alarmi Kibernetik Për Mediat Në Kosovë". KALLXO.Com (2022). Available at: https://kallxo.com/gjate/mendime/alarmi-kibernetik-per-mediat-ne-kosove/.

Bund, Jakob, and Patricia Esteve-Gonzalez. "Cybersecurity Capacity Review–Republic of Kosovo." Available at SSRN 3658214 (2020). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658214.

Conway, Maura, Brady Sheelagh. "A New Virtual Battlefield - How to prevent online radicalization in the cybersecurity realm of the Western Balkans." Regional Cooperation Council (2018).

Cybersecurity Ecosystem Report - Western Balkans: Emerging Cyber threats. pwc & ISAC (2022). Available at: https://www.pwc.rs/en/publications/cybersecurity-ecosystem.

Draft Law on Cyber Security (2020). Available at: https://konsultimet.rks-gov.net/viewConsult.php

Gashi, Kreshnik. "Siguria E Brishtë Kibernetike E Faqeve Qeveritare". KALLXO.Com (2020). Available at: https://kallxo.com/komuna/analize-komuna/siguria-e-brishte-kibernetike-e-faqeve-qeveritare/.

Gashi, Shqipdona. "Kosovo Është "Ndezur Në Alarm" Ndaj Sulmeve Kibernetike". Kosovolive.org (2020). Available at: https://Kosovolive.org/2020/10/29/Kosovo-eshte-ndezur-ne-alarm-ndaj-sulmeve-kibernetike/.

Halili, Mediana. "Lajmet E Rreme Në Kosovë Të Sponsorizuara Nga Rusia Dhe Serbia - Pjesë E Luftës Hibride". KALLXO.Com (2022). https://kallxo.com/lajm/lajmet-e-rreme-ne-kosove-te-sponsorizuara-nga-rusia.

Halili, Mediana. "Rreziku Nga Sulmet Kibernetike Të Rusisë Në Kosovë". KALLXO.Com (2022). https://kallxo.com/lajm/rreziku-nga-sulmet-kibernetike-te-rusise-ne-kosove/.

Isufi, Perparim. "Kosovo Media Regulator Struggling To Recover From Cyber-Attack". Balkan Insight (2022). Available at: https://balkaninsight.com/2022/03/10/kosovo-media-regulator-struggling-to-recover-from-cyber-attack/.

Johnson, Thomas A., ed. Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. CRC Press (2015).

Khan, Umair Pervez, Sabeel Ahmad Naem, and Haider Ali Khan. "Cybersecurity and Human Rights in the age of Cyberveillance". Cyberpolitik Journal 6, no. 12 (2021).

Law No. 06/L –014 On Critical Infrastructure. Official Gazette of the Republic of Kosovo (2018) Available at: https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=16313.

Mullahtahiri, Aurora. "Kosovo In 2020: Cybersecurity - Group For Legal And Political Studies". Group For Legal And Political Studies (2020). Available at: http://www.legalpoliticalstudies.org/kosovo-in-2020-cybersecurity/.

National Cyber Security Strategy and Action Plan 2016-2019 (2015). Available at: https://kryeministri.rks-gov.net/repository/docs/.

National Cybersecurity Strategies in Western Balkan Economies. DCAF - Democratic Control of Armed Forces (2021).

Online Intimidation: Controlling the Narrative in the Balkans. Annual Digital Report 2021. BIRN (2021). Available at: https://balkaninsight.com/wp-content/uploads/2021.

Poposka, Vesna. "The urge for comprehensive cybersecurity strategies in the Western Balkans." Information & Security 34, no. 1 (2016). https://doi.org/10.11610/isij.3402.

Results of the Usage of Information and Communication Technology 2021. Kosovo Agency of Statistics (KAS), (2021). Available at: https://ask.rks-gov.net/en/kosovo-agency-of-statistics/.

Safeguarding Critical Infrastructure in Kosovo. Kosovor Center for Security Studies (2022). Available at: https://qkss.org/en/publikimet/kujdesi-ndaj-infrastrukutres-kritike-ne-kosove/.