University for Business and Technology in Kosovo
UBT Knowledge Center

UBT International Conference | 2023 UBT International Conference

Oct 28th, 8:00 AM - Oct 29th, 6:00 PM

CYBER THREATS RISK ANALYSIS IN STATE POLICIES IN GUARANTEEING NATIONAL SECURITY

Bahri Gashi
bahrigashi@hotmail.com

Bashkim Smakaj

Ngadhnjim Brovina

Arian Kadriu

Follow this and additional works at: https://knowledgecenter.ubt-uni.net/conference

Recommended Citation

Gashi, Bahri; Smakaj, Bashkim; Brovina, Ngadhnjim; and Kadriu, Arian, "CYBER THREATS RISK ANALYSIS IN STATE POLICIES IN GUARANTEEING NATIONAL SECURITY" (2023). *UBT International Conference*. 13.
https://knowledgecenter.ubt-uni.net/conference/IC/ps/13

This Event is brought to you for free and open access by the Publication and Journals at UBT Knowledge Center. It has been accepted for inclusion in UBT International Conference by an authorized administrator of UBT Knowledge Center. For more information, please contact knowledge.center@ubt-uni.net.

CYBER THREATS RISK ANALYSIS IN STATE POLICIES IN GUARANTEEING NATIONAL SECURITY

Bahri Gashi[1], Bashkim Smakaj[2], Ngadhnjim Brovina[3], Arian Kadriu[4]

Abstract

Cyber threats, generally including hybrid warfare, are among the greatest challenges that states and organizations are facing in modern times. This is due to the significant evolution of technology in recent years, which has made a vast amount of information available to individuals and organizations. Such threats can cause serious damage to critical infrastructure, such as transportation, energy, and water resources, as well as communication and financial systems. They can also impact a country's national security and political stability.

To address this threat, states have implemented various policies and measures to ensure national security against the backdrop of cyber security measures. These measures often involve establishing the foundation for national strategies, legal regulations, and specialized agencies responsible for protection against cyber threats.

These agencies collaborate with both public and private organizations to detect, prevent, and respond to cyber-attacks. States have also taken steps to increase public and business awareness regarding cyber threats and to assist in the prevention of cyber threats and the protection of national assets.

This study will provide insights into the policies and measures that states needed to take in order to ensure national security. Overall, states require proactive policies and detailed strategies aimed at preventing cyber threats and safeguarding critical infrastructure from potential attacks.

Keywords: analysis, risk, cyber threats, state policies, national security

[1] Professor at Faculty of Security Studies, University for Business and Technology (UBT), Prishtina, Kosovo, bahri.gashi@ubt-uni.net

[2] Professor at Faculty of Security Studies, University for Business and Technology (UBT), Prishtina, Kosovo, bashkim.smakaj@ubt-uni.net

[3] Professor at Faculty of Political Science, University for Business and Technology (UBT), Prishtina, Kosovo, ngadhnjim.brovina@ubt-uni.net

[4] Professor at Faculty of Security Studies, University for Business and Technology (UBT), Prishtina, Kosovo, arian.kadriu@ubt-uni.net

1. Introduction

Cyber threats are becoming increasingly complex, continuously targeting state systems through hacking and cyberattacks, seriously endangering critical infrastructure through external cybercrime assaults.

On the other hand, it is the undeniable duty and necessity of the State to provide a secure cyberspace, ensuring that all measures are in place to protect vital state and private assets in: National security systems; Personal data systems; Public services systems; Educational system; Border control system; Emergency system; Banking services system; Personal accounts system; Hotel system; Tourism system; Road traffic services system; Air traffic system; Healthcare operating system; Energy and supply system; Construction industry system; Automotive industry system; Transportation systems, etc.

Currently, National Security, primarily state institutions and sectoral policies within the framework of state security infrastructure must intricately encompass the technological and human resource aspects for a comprehensive response against threats and chaotic cyberattacks. Cyber Defense will always be at the forefront as, in the era we are living in, cyber (in)security is a new trend of hybrid warfare with various unconventional characteristics.

2. Cyber threats and the role of governments in their prevention

For more than two decades, the internet has played a significant role in global communication and has become increasingly integrated into people's lives worldwide. Innovations and low costs in this field have significantly increased the availability, usage, and performance of the internet, so that today it has around 3 billion users worldwide (Li & Liu, 2021).

The analysis of the risk of cyber threats in the context of national security encompasses several key elements of a comprehensive national cybersecurity strategy. The five elements of successful national cybersecurity strategies are as follows (Fadia, Nayfeh & Noble, 2020):

1. A dedicated national agency for cybersecurity (NCA)
2. A National Program for the Protection of Critical Infrastructure
3. A national incident response and recovery plan
4. Well-defined laws addressing all cybercrimes
5. A thriving cybersecurity ecosystem.

Countries around the world have become heavily reliant on cyberspace for communication and control of the physical world, to the extent that it is undoubtedly inseparable. Therefore, the responsibilities and functions of the national security of each country are increasingly influenced by cyberspace (Li & Liu, 2021).

In contemporary concepts, cybersecurity is an integral part of research and development across all government agencies. As threats evolve, making it crucial to stay ahead of potential risks, innovations are continually being developed, thereby creating challenges to stay ahead of the curve (Scopus, 2023).

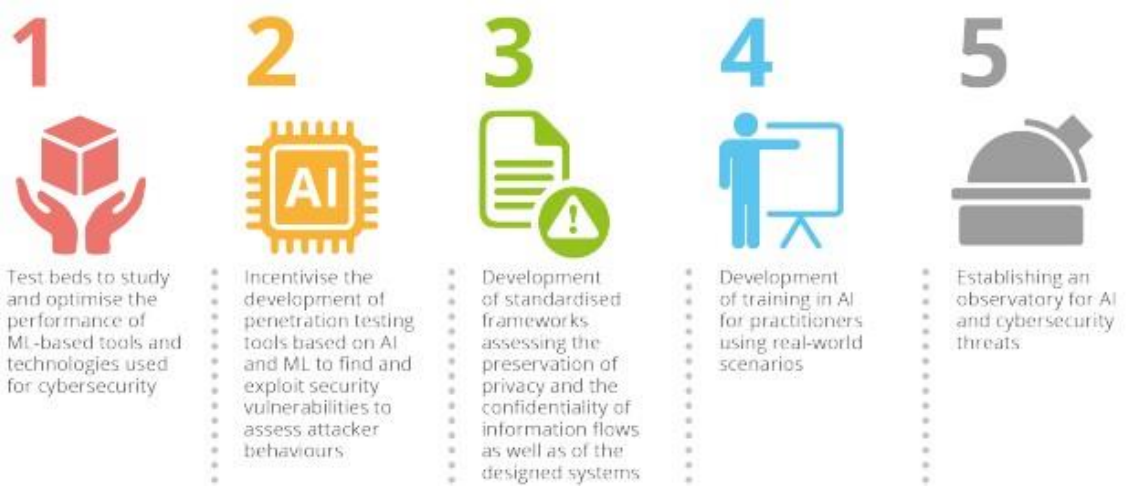
Governments are now striving to enhance their preparations to combat these cyber-attacks. Governments must establish dynamic means to counter these threats due to the pace and nature of technology (Mishra et.al., 2022).

State leaders are in the best position to understand critical infrastructure risks within their own state and to develop programs to aid in mitigating and effectively responding to the wide array of cyber threats they may face. However, for success, states will need to cultivate the abilities, culture, and mindset for public-private collaboration in critical infrastructure defense programs that effectively cover cybersecurity (Deloitte, 2017).

Throughout the research, we find several crucial elements on our topic, observing how the analysis of critical infrastructure and AI is conceptualized, even from the perspective of the European Union Agency for Cybersecurity, characterizing the 5 priorities that governments and EU member states should have in mind, and naturally, other countries on their path to membership, including Kosovo in this case.

The following table provides accurate guidelines regarding the way forward that states should implement.

Table 1 – Top 5 research needs for AI and cybersecurity



Source: (European Union Agency for Cybersecurity [ENISA], 2023)

3. Analysis of the cyberattack threat risks and the role of states in this context

Analysis of the Threat of Cyber Attack Threats is now evident, systematic, and relentless against states, primarily targeting critical infrastructure. For these reasons, defensive policies need to be carefully conceived at two main levels: 1. the policy development of strategies compatible with the current needs, and 2. the technical and technological aspect of professional readiness preparation.

Most importantly, a threat is distinct from a risk. Risk is the probability and consequences or impact of a specific threat, if and when it materializes. National security strategy should be formulated around a clear understanding of risks, not threats. Understanding and assessing risks should be done dynamically, adapting to real-world events (Center for Strategic and International Studies [CSIS], 2021).

How can the government improve its approach to better identify threats and prioritize national security risks? Here's a highly useful example that states should implement, regardless of the specifics they face: The process can begin with a "data call" for the top threats from the Intelligence Community potentially linked to a classified version of the Worldwide Threat Assessment by the DNI. Data can also be solicited from U.S. allies and close partners through their existing sophisticated threat assessment and risk management processes, such as the United Kingdom, Germany, Australia, Japan, New Zealand, and Singapore (Center for Strategic and International Studies [CSIS], 2021).

From this perspective, it's rightfully acknowledged that risk analysis is highly complex and demands ever-increasing attention. Besides the United States and developed states, even the Balkans and Kosovo must follow the path of strategies compatible with Western nations, as security challenges are shared.

While the world is in this spotlight, President Biden has made it clear that all Americans deserve the benefits and full potential of our digital future. The recently published National Cybersecurity Strategy by the Biden-Harris Administration calls for two fundamental shifts in how the United States approaches roles, responsibilities, and resources in the cyber realm: Ensuring that the largest, most capable, and positioned entities – both in the public and private sectors – take a greater share of the burden for cyber risk mitigation, and Increasing incentives to encourage long-term investments in cybersecurity (The White House, 2023).

From this perspective, as a result of the critical need, more than 100 governments have developed national cybersecurity defense strategies to combat the cybersecurity threats faced by their citizens, businesses, and critical infrastructure (Fadia, Nayfeh & Noble, 2020):

One of the important regulatory aspects also involves online communication platforms. To meet government requirements, private companies, especially social media giants like Facebook, Google, and Twitter, have developed terms of service and codes of conduct to regulate expected content on these social media platforms, effectively creating norms on the internet. However, these terms of service and codes of conduct differ across different platforms, creating legal ambiguity and uncertainty about what content is prohibited on which platform (DCAF, 2019).

4. State-sponsored attacks

Beyond hackers seeking profit through the theft of individual and corporate data, entire nations are now utilizing their cyber capabilities to infiltrate other governments and conduct attacks on critical infrastructure. Cybercrime today is a significant threat not only to the private sector and individuals, but also to the government and the nation as a whole (Moore, n.d.).

The rise of state-sponsored cyberattacks poses an escalating and substantial threat to private businesses. These attacks are increasingly targeting sectors within the business landscape that offer viable opportunities for addressing geopolitical disputes (Moore, n.d.).

In democracies with consolidated institutions, specialized entities such as the Department of Homeland Security and its components play a leading role in enhancing cyber security resilience nationwide, investigating malicious cyber activity, and advancing cyber security while upholding democratic values and principles (U.S. Department of Homeland Security, 2023).

Similarly, there is the utilization of threat intelligence for threat prevention. Threat intelligence is organized, pre-analyzed information about potential attacks that may jeopardize an organization. Threat intelligence helps organizations understand possible or ongoing cyber threats. The more the information security staff knows about threat actors, their capabilities, infrastructure, and motivations, the better they can safeguard their organization (Cassetto, 2023).

Usually, in the topic analysis the meaning of "What is a cyber threat?" in the text titled: "Hostile Nation States," stating that state-sponsored cyber warfare programs present evolving

cyber threats ranging from propaganda, internet page defacement, espionage, and disruption of critical infrastructure to loss of life. Government-sponsored programs are becoming increasingly sophisticated and pose advanced threats compared to other threat actors. Their evolving capabilities can lead to widespread and long-term damage to the national security of many countries, including the United States (Tunggal, 2022).

While hostile nation-states can conduct cyberattacks against local companies and institutions, aiming to interfere with communications, cause disruptions, and inflict damage, there are also Terrorist Organizations that can carry out cyberattacks with the intention of destroying or abusing critical infrastructure, threatening national security, and disrupting economies. Additionally, Criminal Groups and organized hacker groups strive to infiltrate computer systems for economic gains. These groups employ phishing, spam, spyware, and malware for theft, private information breaches, and online scams (Imperva, n.d.).

The context of cybersecurity, with all the complexity of Cyber Security Threats, in the case of Kosovo, overshadows the issues that the country has faced on its way forward and at the same time present a serious challenge to the governmental institutions in Kosovo.

5. Critical infrastructure – Cybersecurity and the case of Kosovo

According to the Security Strategy of Kosovo, point 2.1 states: The primary security threat to the Republic of Kosovo is Serbia's territorial claim, the undermining of sovereignty by illegal structures supported by the Serbian state, and the active and ongoing efforts of the Serbian state to hinder Kosovo's progress and integration into Euro-Atlantic structures and other international organizations and mechanisms (Government of Kosovo, 2022, p. 7).

In this perspective, this document indicates that the Republic of Kosovo is exposed to hybrid threats, which include unconventional, asymmetric elements, influence projection operations, and cyberattacks aimed at weakening the country's sovereignty, undermining its integrity, and damaging its international image (Government of Kosovo, 2022, p. 8).

In this context, the State of Kosovo has also taken concrete steps towards creating the Draft Strategy for Cybersecurity of Kosovo 2023-2027. This strategy aims to address the complexity of national cybersecurity challenges in the Republic of Kosovo through a plan of directions and

approaches approved by the Government of Kosovo, with the goal of enhancing the security and resilience of national infrastructure and services (Government of Kosovo, 2023).

As a result of the implementation, Law No. 08/L-173 FOR CYBERSECURITY has been approved. Article 3 Definitions, 1.26. CSRA - stands for the Cybersecurity Agency, which operates under the Ministry responsible for Internal Affairs. This establishment will regulate this challenging field in our era (Assembly of the Republic of Kosovo, 2023).

In this aspect, it should be emphasized that the first policy related to cybersecurity in Kosovo – the Policy of the Electronics and Communication Sector – the Digital Agenda for Kosovo 2013-2020 – was formulated in March 2013 by the former Ministry of Economy (Ministry of Economy and Environment, Ministry of Economic Development, Republic of Kosovo, 2013).

Over time, in the face of these challenges regarding Cybersecurity Threats, significant steps were taken toward the creation of the State Strategy for Cybersecurity and the Action Plan (2016-2019), as well as the Cybersecurity Strategy in MFA/MoD (2017-2020). These have expired three and two years ago, respectively, and for this reason, they are no longer applicable. However, the new Cybersecurity Strategy (2022-2026) has been drafted, although it has not yet been approved by the Government of Kosovo. Furthermore, the Draft Strategy of Kosovo (2021-2030) (Government of Kosovo, 2020).

Furthermore, the Law on Critical Infrastructure, approved by the Assembly of Kosovo on March 30, 2018, provides legal provisions for regulating critical infrastructure in Kosovo. It identifies the relevant sectors, offers guidelines on how they are managed and defines penalties for non-compliance (Peci & Ukshini, 2022).

Based on the review of state documentation regarding the Risk Analysis in ensuring National Security against cyber threats, as well as other asymmetries of hybrid warfare, significant legal measures and implementation aspects have been undertaken, positioning Kosovo as a serious and consolidated state in terms of fulfilling legal infrastructure. However, it is still not adequately prepared in other essential resources, such as human resources, technological equipment aspects, and other important determinants in this process.

6. Conclusions

In the era of technology, strengthening cyber security capacities and protection against cyber threats will remain an essential step to ensure that all critical systems and infrastructure operate securely, guaranteeing all levels of national security.

Reassessment is not merely a guide for further improvements; it should be a proactive way to better understand strengths and weaknesses comparatively and correlate them with the challenges of the times.

It can be concluded that Kosovo has taken critical steps in cyber security, fulfilling Cyber Security capacities and overall moving toward completion of the National Security architecture, as a necessity for Euro-Atlantic processes.

Preparing for technological transformation, facing challenges in cyberspace, reassessing legal and technological aspects, human resources, and continuous education as an implementation phase should remain the main focus of managing these national security challenges.

All regional states, including Kosovo, have implemented policies to address this critical threat to ensure national security. These measures should include comprehensive capacities by establishing specialized and responsible agencies to reassess risk analysis and protection against cyber threats.

For the state of Kosovo, critical security aspects remain at a high risk, as long as proper security architecture is not adequately implemented, including budget allocations, human resource capacity building, interactive technological devices, military technological capacity enhancement, alignment of strategic documents with the security environment, laws, and their revisions in line with critical security situation assessment.

The Republic of Kosovo, specifically its security encryption institutions, must also be supplemented with four new laws, resulting in the establishment of four vital institutions for National Security in the fight against Crime and Corruption; Verification and Classification; Counter-Intelligence; Cyber Space Defense (Hybrid Warfare), respectively, creating legal aspects for law enforcement and defense against cyber warfare, cyberattacks, cybercrime, cyber espionage, cyber extortion, cyber terrorism, as precursors to conflicts in hybrid warfare arising from Cyber Threats.

References

1. Assembly of the Republic of Kosovo. (2023, February 02). Ligji Nr. 08/L-173, Për Sigurinë Kibernetike [Law No. 08/L-173, On Cybersecurity]. https://www.kuvendikosoves.org/Uploads/Data/Documents/Ligjinr.08-L-173_Lt5nfFXujr.pdf
2. Cassetto, O. (2023, February 01). Cybersecurity Threats: Everything you Need to Know. https://www.exabeam.com/information-security/cyber-security-threat/?fbclid=IwAR0pXPCwOGpEIAqOl-f2wCyAdZSndxjvOAQbs1tAurtDqC_DFGI0pzEk3fk
3. Center for Strategic and International Studies (CSIS). (2021, January 28). A Better Way to Identify and Address Threats to National Security. https://www.csis.org/analysis/better-way-identify-and-address-threats-national-security
4. DCAF. (2019). Udhëzues për qeverisjen e mirë me sigurinë kibernetike [Guidelines for Good Cybersecurity Governance]. Geneva. https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_AL_Jan2021_0.pdf
5. Deloitte. (2017). Cybersecurity for critical infrastructure protection: A growing, highly visible threat calls for state leadership. https://www2.deloitte.com/us/en/pages/public-sector/articles/cybersecurity-for-critical-infrastructure-protection-states.html
6. European Union Agency for Cybersecurity (ENISA). (2023). Artificial Intelligence and Cybersecurity research. ENISA Research and Innovation Brief. https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research
7. Fadia, A., Nayfeh, M., & Noble, J. (2020, September 16). Follow the leaders: How governments can combat intensifying cybersecurity risks. Mc Kinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks
8. Government of Kosovo. (2020). Security strategy of the Republic of Kosovo 2021-2030. https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=40992
9. Government of Kosovo. (2022). Strategjia e Sigurisë e Kosovës 2022 - 2027 [Security Strategy of Kosovo 2022 - 2027]. https://kryeministri.rks-gov.net/wp-content/uploads/2022/10/1-Strategjia-e-Sigurise-e-Kosoves-ALB.pdf
10. Government of Kosovo. (2023). Kosovo Draft Cyber Security Strategy 2023-2027. https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=41780
11. Imperva. (n.d.). Cyber Security Threats. https://www.imperva.com/learn/application-security/cyber-security-threats/?fbclid=IwAR3C1-phtgRlqOi1Xo_BWeU2M1Fc1OFeUUd4VJSHjJF62xr6297r7RnLUDA

12. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments (Vol. 7, November, pp. 8176-8186). Elsevier. https://doi.org/10.1016/j.egyr.2021.08.126
13. Ministry of Economy and Environment, Ministry of Economic Development, Republic of Kosovo. (2013, March). Electronic communication sector policy – Digital Agenda for Kosova 2013 ÷ 2020. https://smartkosova.rks-gov.net/wp-content/uploads/2021/06/Electronic_Communication_Sector_Policy_2013-2020.pdf
14. Moore, M. (n.d.). Top Cybersecurity Threats in 2023. University of San Diego. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/?fbclid=IwAR00OhSNcUJqGOE19Z1_M497lNgDBueeUCP0wukUWk97Yu8r6P4J2iNzC6o
15. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820
16. Peci, L., & Ukshini, V. (2022, September). Qeverisja e Mirë në Sigurinë Kibernetike në Kosovë: Forcimi i themeleve dhe i institucioneve të reja [Good Governance in Cybersecurity in Kosovo: Strengthening Foundations and New Institutions]. KIPRED. https://kipred.org/repository/docs/02_-_Forcimi_i_Inistitucioneve_-_ALB04-web_528063.pdf
17. Scopus. (2023). Cybersecurity: Scopus shows you the latest research trends. Elsevier. https://www.elsevier.com/solutions/scopus/government-and-funding-agencies/cybersecurity
18. Tunggal, A. T. (2022, August 17). What is a Cyber Threat? UpGuard. https://www.upguard.com/blog/cyber-threat?fbclid=IwAR1XOpgAO9KfvlgMf1O6lB78Ma7LVPOVPyOKhrPNn1kaWsLngOf9DQHo16w
19. The White House. (2023, July 13). FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/
20. U.S. Department of Homeland Security. (2023). Cybersecurity. https://www.dhs.gov/topics/cybersecurity?fbclid=IwAR0DPMv9L3OjKysWb5BTdM2Fk9dbbIYHMifBb8IqjxZb_Pfz-TK-m0nxDCM