From threat to response: The evolution of cybersecurity in Albania

Klorenta Pashaj
National Cyber Security Authority of Albania
klorenta.pashaj@gmail.com

Vilma Tomço
State Authority for Geospatial Information
vimatster@gmail.com

Eralda Gjika
Department of Applied Mathematics, Faculty of Natural Science, University of Tirana
eralda.dhamo@fshn.edu.al

Abstract:
As Albania's digital landscape expands, its vulnerability to sophisticated cyber threats increases correspondingly. This study explores the evolution of Albania's cybersecurity strategies, tracing the shift from reactive measures to a proactive defence approach. It critically examines significant cyber incidents that have shaped the national cybersecurity landscape, assessing how these have influenced the development of Albania's current cyber defence strategies. The focus is on how Albania has tailored its strategic responses to enhance digital resilience and national security.
In the second part, the paper provides an in-depth review of the threat models prevalent in the Western Balkans and Albania, highlighting key areas where Albania's cyber management requires further development. One key recommendation is the forecasting of cyber-attacks, which could benefit from the application of time-series and machine learning techniques to enhance predictive capabilities. This approach emphasizes the importance of adapting to emerging threats and fostering international cooperation to bolster Albania's cybersecurity infrastructure.
Keywords: Albania, cybersecurity, threat models, proactive defence, digital resilience, international cooperation, Western Balkans.

1.Introduction

The cybersecurity landscape in the Republic of Albania has been influenced by a series of factors closely related to the country's positioning in the international arena. In recent years, recurring political tensions have extended into the realm of cybersecurity, blurring the lines between politics and cyber operations. The heightened political tensions have led to cyber threats from state-sponsored actors and hacker groups.
The war in Ukraine has been accompanied by sophisticated cyber-attacks from Russian groups. These groups continuously attempt to compromise key sectors, including communications, transport, energy, defence, administrative services, and diplomacy. Such cyber activities reflect broader tactical efforts to destabilize vital infrastructures and extend the conflict's impact beyond physical borders. These cyber operations have targeted multiple international stakeholders, highlighting the interconnected nature of cyber threats in modern conflicts [1].
In the last 2 years, the Republic of Albania has been targeted by various international actors. In 2013, following an agreement with the USA, Albania agreed to host Iranian Mujahideen [2] for humanitarian purposes [3]. This decision faced criticism from the Iranian state, and in 2022, Iranian state-sponsored actors orchestrated several cyber-attacks [4] in response to the Albanian government's support for the Iranian opposition, specifically the MEK community, a threat that remains current.
The risk remains high as Albania is among the leaders in the region regarding digitization and innovation. Currently, the e-Albania portal offers 1,231 electronic services, which account for 95% of all national public services. The utilization of artificial intelligence in proactive public services is one of the objectives of the Albanian government [5], thereby increasing the necessity to remain vigilant against all potential threats that the country faces.
In contrast, the conflict in Gaza has led to an increased presence of cyber-attacks on Israeli digital platforms by hacker groups associated with the Middle East, Islamic countries, and Russia. However, there hasn't been any significant impact on Israeli infrastructure, and the attacks have mainly targeted the regional level [6]. The threat from these attacks remains present, given that in February 2023, the Republic of Albania signed a cooperation agreement with the National Cyber Security Authority in Israel [7].

Attacks against businesses also constitute a high-risk factor. Such incidents include the attacks against Credins Bank in Albania [8] or Intesa San Paolo Bank in Italy [9], both of which operate within our country as critical information infrastructure operators.

The National Cyber Security Authority (NCSA), as the authority responsible for overseeing the implementation of legislation in the field of cyber security, comprises the National Cyber Security Operations Center (SOC), which continuously monitors the networks of critical and important information infrastructures at the national level on a 24/7 basis [10]. However, analysing risk factors is imperative for delineating objectives in formulating policies and awareness-raising initiatives.

2.Cyber security incidents in the Western Balkans region

Cyber threats in the Western Balkans in 2023 were mainly characterized by attacks from Advanced Persistent Threat (APT) groups associated with Iran and Russia. These groups primarily employed tactics such as ransomware, malware, social engineering, and wipers—software designed to irreversibly delete system data. State-sponsored trends included exploiting known vulnerabilities, targeting individuals and legitimate apps and devices, and disrupting public services and critical information infrastructures.

Until 2021, Albania was not a significant target for major and known cyberattacks. However, in 2022, one of the most sophisticated cyberattacks against the Albanian government systems occurred, originating from the Islamic State of Iran. The attackers aimed to erase all governmental systems and their data. Following the identification of the ransomware attack, immediate actions were taken to prevent its spread, and thanks to well-implemented backup and disaster recovery policies, governmental services were restored within the first week.

The cybersecurity situation in the Republic of Albania is influenced by a range of factors closely linked to the country's positioning in the international arena. As Albania aligns itself globally, the intersection between politics and cybersecurity becomes increasingly blurred, with political tensions evolving into sophisticated cyber threats from state-sponsored actors, terrorist organizations, and hacker groups.

January 2023: Cyberattacks and Geopolitical Tensions

On January 30, 2023, the cybercrime group LockBit, operating from Russian territory and composed of Russian-speaking members, targeted Air Albania with a significant cyber-attack [11]. This event underscored the ongoing risk to Albanian infrastructure, closely tied to international geopolitical tensions.

June 2023: MEK Community and Relations with Iran

In June 2023, Albanian authorities conducted raids in ASHRAF 3 camp in Manzë, home to the Mujahedin-e Khalq (MEK), suspecting planned cyber-attacks among other offenses. This reflects Albania's complex relationship with Iran, particularly following the 2013 agreement to host MEK, which led to several cyber-attacks by the Iranian threat actors in 2022 in response to Albania's support for the Iranian opposition [12].

August and September 2023: International Cybersecurity Dynamics

In August 2023, a DDoS attack targeted five banks in Italy, including Intesa San Paolo, with the perpetrating hacker group declaring through Telegram their perception of the Italian authorities as Russophobic [13]. This event highlights the broader context of international cyber threats where Albania, due to its alliances, could become a collateral victim.

In September 2023, Albania's stance on the war in Ukraine was reaffirmed during its presidency of the UN Security Council. Prime Minister Edi Rama’s statements supported Ukraine's sovereignty and opposed any territorial annexations [14]. This position likely influences the cyber threat landscape, given Russia's historical use of cyber warfare in geopolitical conflicts.

October 2023: Stance on the Conflict in Gaza

On October 24, 2023, during a high-level UN Security Council meeting, Albanian Foreign Minister Igli Hasani reiterated Albania's support for Israel's right to self-defense in accordance with international law, amidst the ongoing conflict with Hamas [15]. This stance, while aiming to maintain balance, also potentially exposes Albania to cyber threats from groups aligned with Palestinian interests or opposing nations.

November 2023: OSCE Ministerial Council and Russia's Regional Influence

Foreign Minister Igli Hasani, during the OSCE Ministerial Council in North Macedonia, condemned Russian aggression in Ukraine, highlighting the impact of the conflict on regional security [15]. He emphasized the need for coordinated efforts among allies to counter threats, including those in cyberspace, advocating for the recognition of Kosovo's independence as a stabilizing factor in the Balkans.

Albania's cybersecurity landscape is profoundly influenced by its geopolitical relationships and regional dynamics. The country's alignment with Western institutions and its strategic stance on various international issues make it a target for cyber-attacks emanating from both state and non-state actors. As Albania navigates these complex geopolitical waters, the necessity for a robust, proactive cybersecurity strategy becomes increasingly apparent, necessitating continual adaptation and international cooperation to mitigate emerging threats.

3.Cybersecurity Challenges in Albania

In 2022, a significant cyber incident profoundly impacted Albania, primarily attributed to state-sponsored actors from Iran. This attack was a part of ongoing geopolitical tensions, largely because of Albania's sheltering of Iranian opposition groups, which led to severe disruptions across Albania's governmental digital services. This incident highlighted not only the vulnerabilities within Albania's cybersecurity infrastructure but also brought international attention, resulting in widespread condemnation and support from Albania's allies, including the United States and NATO members [16].

Albania's response to the cyberattacks was firm, with the government taking decisive actions such as severing diplomatic ties with Iran. This move was unprecedented but deemed necessary given the severity of the cyberattacks, which included attempts to wipe sensitive government data. Furthermore, the situation prompted discussions within Albania about the potential invocation of NATO's Article 5, which treats an attack on one member as an attack on all, requiring collective defense. However, Albania ultimately chose not to escalate the situation to this level, highlighting the complex decisions nations must navigate when dealing with cyber aggression from state actors.

The cyberattacks from Iran have underscored the critical need for Albania to strengthen its cyber defenses. This includes enhancing the resilience of critical infrastructure, improving incident response capabilities, and increasing international cooperation to manage cyber threats effectively. Investments in cybersecurity capacity building, such as advanced detection and response systems, are essential to safeguard against such sophisticated threats [17].

The year 2022 marked a pivotal moment in the cyber threat landscape of Albania, characterized by a marked increase in both the frequency and complexity of cyber incidents [18]. These developments were largely driven by geopolitical tensions and strategic national decisions. One significant event was the accommodation of the Mujahedin-e Khalq (MEK), which precipitated a series of targeted cyber assaults by Iranian state-backed entities. These operations, which aimed at disrupting governmental and key infrastructural systems, were manifest demonstrations of political dissent and strategic pressure. According to Microsoft (2022), these operations utilized advanced tactics centred on espionage and service disruption, underscoring the critical need for Albania to enhance its cybersecurity counteractions.

During this period, Albania also encountered severe cyber-attacks against essential national frameworks. The Total Information Management System (TIMS), pivotal for border and immigration control, suffered disruptions that adversely affected national security and operational continuity [19].

The financial sector remained a preferred target as well, with major banking institutions like Credins Bank encountering security breaches that prompted a national revaluation of cybersecurity measures within financial entities (A2News, 2022). These episodes accentuated the susceptibility of critical infrastructures to cyber threats and underscored the imperative for a comprehensive cybersecurity framework capable of countering sophisticated state-backed operations and cybercriminal endeavours.

On December 25th, 2023, the National Cyber Security Authority of Albania (NCSA) reported cyber-attacks targeting the ONE telecommunications company and the Parliament of Albania ([20]. National Cyber Security Authority quickly mobilized expert teams to support the affected institutions in managing the cyber-attacks and initiating recovery processes. These actions included a detailed analysis of the attack methods and coordination with international partners to assess the damage and prevent further incidents, highlighting a proactive and collaborative approach to strengthening national cybersecurity resilience.

The incident at the Parliament of Albania also involved a cyber-attack orchestrated by Iranian threat actors, which targeted critical infrastructure in Albania. The attack exploited vulnerabilities in the infrastructure's systems, allowing the perpetrators to gain unauthorized access and disrupt operations. The attack files deployed by Iranian threat actors caused significant damage, impacting various sectors and services vital for the functioning of the

country. The incident prompted an urgent response from authorities to contain the attack and mitigate its effects, while also initiating an extensive analysis to understand the attack vectors and enhance cyber resilience measures to prevent similar incidents in the future [21].
Concurrently, the Albanian Institute of Statistics (INSTAT) was compromised, threatening crucial demographic and economic data, thereby posing substantial risks to data integrity and national planning initiatives ([22].
The extensive cyber threats encountered in 2022 were not isolated events but part of a broader trend of escalated cyber aggression towards nations embroiled in geopolitical disputes or hosting contentious groups. The repercussions of these threats are far-reaching, affecting national security, economic stability, and public confidence in digital platforms. With Albania's continued expansion of its digital infrastructure, such as the e-Albania portal which delivers a wide range of public services online, the associated cyber risks have also escalated, necessitating significant enhancements in national cybersecurity measures.
Throughout 2023, NCSA tracked the frequency and categories of reported cyber incidents across different sectors National Cyber Security Authority [23]. The banking sector experienced the highest incidence, accounting for 36% of all reported cyber incidents, making it the most affected sector. It was followed by the digital infrastructure sector with 31%, the energy sector with 12%, the transportation and financial sectors each with 7%, the healthcare sector with 5%, and the telecommunications sector with 2%. This data highlights sector-specific vulnerabilities and the critical need for tailored cybersecurity enhancements in each area.

Sector	No. of incidents
Banking	15
Digital Infrastructure	13
Energy	5
Transport	3
Financial	3
Health	2
Telecommunication	1

Table 1
Source: Reported cyber security incidents, NCSA, 2023

Throughout the year, the Albanian government and its cybersecurity divisions were tasked with addressing immediate threats and pre-empting potential future vulnerabilities. This demanded a dynamic and adaptable cybersecurity strategy, capable of keeping pace with the rapidly evolving threat landscape. The response strategies devised during this period played a crucial role in shaping the future trajectory of Albania's cybersecurity policies and initiatives, paving the way for an extensive revision of the nation's cybersecurity frameworks in the following years.

4.Advancements in National Cybersecurity: 2022-2024
Over the span from 2022 to 2024, Albania has demonstrated significant advances in cybersecurity, marked by strategic, legislative, and technical improvements that align with European Union standards. The commitment to enhancing cybersecurity is evident in the comprehensive updates to the National Cybersecurity Strategy Action Plan. This document now effectively addresses contemporary challenges and delineates clear priorities, establishing a roadmap that is both adaptive and proactive.
The legislative landscape has seen transformative changes, particularly with the enactment of a new law No.25/2024 “On Cyber Security”, that aligns with the EU's NIS 2 Directive. This pivotal legislation underpins Albania's cybersecurity framework, providing a robust legal foundation that supports comprehensive cybersecurity measures across various sectors. The law's implementation is supported by detailed subordinate acts, which guide its application and ensure a cohesive national cybersecurity strategy. Considering that EU member states have a deadline until October 2024 to transpose and implement this directive into their national legislations, Albania has made strides in integrating the provisions of the NIS2 directive into its national legal framework through the adoption of this law. This step is a significant advance towards enhancing the country's

cybersecurity infrastructure and aligning with European standards, underscoring Albania's commitment to bolstering its cyber resilience and regulatory compliance.

The 2020-2025 “National Cybersecurity Strategy of Albania” highlights the necessity of revising the Action Plan every two years, reflecting the dynamic development of the cybersecurity sector. NCSA has diligently revised the 2020-2025 Action Plan and formulated the 2024-2025 Action Plan, identifying priorities and needs while coordinating with relevant institutions for its implementation.

The revised Action Plan for 2024-2025 establishes specific measures to address the needs, accelerate progress in cybersecurity, and achieve several objectives set forth by the 2020-2025 National Cybersecurity Strategy [23]. These objectives include improving the legal and policy framework by integrating EU cybersecurity policies and standards, strengthening cybersecurity structures and infrastructures through enhanced technical and professional capacities, and improving procedures for handling and managing cybersecurity incidents.

Additional goals of the plan are to increase awareness and education about cybersecurity threats, cybercrime, and illegal online content, as well as to enhance protective measures for children online and to address violent extremism and radicalization in cyberspace. The plan also aims to boost professional capacities in cybersecurity through training and certifications in collaboration with national and international partners.

The 2024-2025 Action Plan further contributes to Albania's European integration process by aligning legal frameworks and policies with EU standards and best practices, and by fostering international cooperation with strategic partners. This comprehensive approach not only aims to fortify Albania's cybersecurity defences but also integrates the country more deeply into the broader European and global cybersecurity frameworks.

Albania's collaboration with international organizations like NATO and the OSCE has significantly enhanced its cybersecurity capabilities. As a member of these organizations, Albania participates in various programs that improve information sharing, experience exchange, and capacity building in cybersecurity both regionally and globally. This international cooperation has been instrumental in enhancing Albania's cybersecurity framework and preparedness.

The National Cyber Security Authority (NACS) has signed Memorandums of Understanding for cybersecurity information exchange with several countries, including the United Arab Emirates, Israel, and Romania, among others. These agreements are pivotal for fostering a collaborative approach to handling cyber threats and enhancing the security protocols within Albania.

Albania's participation in global forums like the International Telecommunication Union, Forum of Incident Response Security Teams, TF-CSIRT, Trusted Introducer, and Counter Ransomware Initiative further demonstrates its commitment to international cybersecurity cooperation. These engagements allow Albania to align with global cybersecurity standards and practices, which is crucial for managing the challenges in this rapidly evolving field.

The importance of cybersecurity diplomacy is also emphasized through Albania's active role in the United Nations, where it contributes to discussions on securing information and communication technologies. The focus of these international engagements is on building trust, increasing capacity, and establishing responsible state behaviour in cyberspace.

Overall, Albania’s strategic partnerships and active participation in international cybersecurity initiatives highlight its proactive approach to enhancing national and regional cyber defences. These efforts are critical in addressing the heightened challenges of cybersecurity and ensuring a secure digital environment for its citizens and allies.

A detailed sector-specific analysis has underscored the critical need for prioritizing cybersecurity, with a special focus on building human and technical capacities. This is crucial for mitigating the risks posed by increasingly sophisticated cyber threats. The banking sector, often a prime target for cyberattacks, has exemplified significant progress by implementing stringent cybersecurity measures, achieving a 94% rate in the adoption of technical security protocols. This sector's proactive stance is a testament to the effectiveness of Albania's strategic cybersecurity initiatives.

Further investments in digital infrastructure have bolstered the country's defensive capabilities. The digital infrastructure sector, essential for national connectivity and security, has also made substantial strides, reflecting a 72% implementation rate of advanced cybersecurity measures. The financial sector follows closely, showcasing an adherence to cybersecurity protocols with a 71% implementation rate, while the energy sector has recorded a 63% compliance rate [23].

The government's approach extends beyond reactive measures to include proactive strategies, such as the identification and protection of 'Crown Jewels'—critical assets that are most vulnerable to cyber-attacks. This strategy is aimed at strengthening defences around crucial components of Albania's infrastructure, thereby enhancing the overall security posture.

International cooperation has significantly enriched Albania's cybersecurity strategy. Engagements with global cybersecurity bodies have facilitated a rich exchange of knowledge and expertise, which has been instrumental in enhancing capacity building and refining incident response strategies. These international partnerships are vital as they enable Albania to combat the sophisticated and evolving cyber threats that transcend national borders.

5.Conclusions

Despite these advancements, challenges remain, highlighting the ongoing need for vigilance and continuous improvement. The proactive and collaborative efforts made thus far provide a strong foundation for future enhancements in cybersecurity. Albania's strategic approach to cybersecurity governance, coupled with its commitment to international cooperation and sector-specific advancements, sets a robust example for comprehensive digital defence mechanisms.

Albania’s journey through 2022 to 2024 highlights a significant evolution in cybersecurity readiness, characterized by an integrated approach that blends strategic policy enhancements, robust legal frameworks, and sector-specific advancements. The nation has not only adapted to the challenges presented by the digital age but has also positioned itself as a proactive player in the international cybersecurity arena. This ongoing commitment to cybersecurity is crucial as Albania continues to navigate the complexities of the digital era, ensuring the security and resilience of its national infrastructure against potential cyber threats. The strategic, legislative, and cooperative measures undertaken reflect a mature approach to cybersecurity, setting the stage for continued progress and positioning Albania as a model of effective cybersecurity governance in the region.

While Albania has laid a robust groundwork for safeguarding its critical information infrastructures, there remains significant work ahead. The upcoming years are pivotal in shaping how effectively Albania will integrate into the evolving international cybersecurity arena. By strategically enhancing technological resources, developing human capital, and strengthening global partnerships, Albania aims to surpass existing standards and secure a resilient digital future. The expansion of comprehensive and varied data resources will also facilitate dynamic analyses and modelling, enabling institutions and agencies to better assess their cybersecurity stance and implement more targeted risk mitigation strategies.

Looking ahead, enhancing Albania's capacity to predict cyber-attacks is a key strategic initiative. By integrating time-series analysis and machine learning into their cybersecurity framework, Albania aims to refine its ability to foresee and mitigate potential threats. This approach not only bolsters defences by identifying risks early but also exemplifies a forward-thinking stance in cybersecurity management. Adopting these advanced analytical techniques allows for a dynamic response to the evolving landscape of cyber threats, ensuring that preventive measures are both timely and effective.

Emphasizing predictive analytics underscores the importance of staying updated with technological advancements and emerging cyber threats. Adopting state-of-the-art technologies and methodologies is essential for maintaining a robust defence mechanism. Machine learning plays a pivotal role by analysing vast data sets to detect patterns and anomalies indicative of potential security breaches. This proactive measure significantly enhances Albania's cybersecurity capabilities, providing a strategic edge in monitoring and neutralizing threats.

Moreover, international cooperation is crucial in reinforcing Albania’s cybersecurity infrastructure. Engaging in partnerships with global entities enables the exchange of critical intelligence and resources, which enhances the collective ability to tackle cybersecurity challenges. Such collaborations are vital for sharing best practices and fostering a unified approach to cybersecurity, ensuring Albania is well-equipped to handle the complexities of modern cyber threats and maintain its resilience against a backdrop of global digital threats.

References

1. A2News. (2022, December 22). *Banka Credins: Kemi rënë pre e një sulmi kibernetik, asetet e klientëve janë të sigurta dhe paprekura*. A2news.com. https://a2news.com/2022/12/23/banka-credins-kemi-rene-pre-e-nje-sulmi-kibernetik-asetet-e-klienteve-jane-te-sigurta-dhe-paprekura/
2. AKSHI. (2023, October 31). *TechAccelerator në Bruksel, Karçanaj: Shqipëria plotësisht digjitale në 2030 përmes Inteligjencës Artificiale – Agjencia Kombëtare e Shoqërisë së Informacionit*. Akshi.gov.al; AKSHI. https://akshi.gov.al/techaccelerator-ne-bruksel-karcanaj-shqiperia-plotesisht-digjitale-ne-2030-permes-inteligjences-artificiale/
3. Albanian Post. (2023, February 2). *Autoritetet shqiptare dhe izraelite nënshkruajnë marrëveshje për sigurinë kibernetike*. Albanian Post. https://albanianpost.com/autoritetet-shqiptare-dhe-izraelite-nenshkruajne-marreveshje-per-sigurine-kibernetike/
4. BIRN. (2023, June 23). *Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity*. BIRN. https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/
5. Bleih, A. (2023, December 8). *Israel-Hamas vs. Ukraine-Russia War*. Cyberint. https://cyberint.com/blog/research/israel-hamas-vs-ukraine-russia-war/#Conclusions
6. Duguin, S., & Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf
7. Euronews Albania. (2023, June 21). *Zbardhet hetimi i SPAK për banorët e MEK, rreth 150 pajisje të sekuestruara*. Euronews Albania. https://euronews.al/zbardhet-hetimi-i-spak-per-banoret-e-mek-rreth-150-pajisje-te-sekuestruara/
8. Lyngaas, S. (2022, September 10). Albania blames Iran for second cyberattack since July | CNN Politics. *CNN*. https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html
9. Microsoft. (2022, September 8). *Microsoft investigates Iranian attacks against the Albanian government*. Microsoft. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/
10. Miller, M. (2022, October 5). *Albania weighed invoking NATO's Article 5 over Iranian cyberattack*. POLITICO. https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347
11. Ministria e Puneve te Jashtme. (2023, November 30). *Ministeriali i OSBE, Ministri Hasani: Evropa e sigurtë vetëm me njohjen e pavarësisë së Kosovës*. Punetejashtme.gov.al. https://punetejashtme.gov.al/ministeriali-i-osbe-ministri-hasani-evropa-e-sigurte-vetem-me-njohjen-e-pavaresise-se-kosoves/
12. Ministria e Puneve te Jashtme. (2024). Situata në Lindjen e Mesme, Ministri Hasani: Çështja e Palestinës nuk duhet të vazhdojë të mbetet një punë e papërfunduar. Punetejashtme.gov.al. https://punetejashtme.gov.al/situata-ne-lindjen-e-mesme-ministri-hasani-ceshtja-e-palestines-nuk-duhet-te-vazhdoje-te-mbetet-nje-pune-e-paperfunduar/

13. Montgomery, R. Adm. (Ret.) M. (2022, September 19). *Iranian-backed attacks on Albania highlights need for Cyber Capacity Building*. The Cipher Brief. https://www.thecipherbrief.com/column_article/iranian-backed-attacks-on-albania-highlights-need-for-cyber-capacity
14. National Cyber Security Authority. (2023a). *Raport Qeverisja Kibernetike 2023*. AKSK. https://cesk.gov.al/raport-qeverisja-kibernetike-2023/
15. National Cyber Security Authority. (2023b, December 26). *Deklaratë Zyrtare ONE* . NCSA. https://cesk.gov.al/deklarate-zyrtare-3/
16. National Cyber Security Authority. (2023c, December 28). *Analysis of Iranian Threat Actors Attack Files That Impacted Infrastructure in AL – Incident Report Parlament*. AKCESK. https://cesk.gov.al/en/analysis-of-homeland-justice-attack-files-that-impacted-infrastructure-in-al-incident-report-parlament/
17. National Cyber Security Authority. (2024a). *Ligji Nr.25/2024 "Për sigurinë kibernetike."* AKCESK. https://cesk.gov.al/wp-content/uploads/2024/04/ligj-2024-03-21-25-5.pdf
18. National Cyber Security Authority. (2024b, February 16). *Raport Incidenti Instati – Analizë MEK-DDMC*. AKSK. https://cesk.gov.al/raport-incidenti-instati-analize-mek-ddmc/
19. Pashaj K., Gjika E., (2024) "The importance of critical information infrastructure protection – Case of Albania", Journal of Natural Sciences, Publication No.35 (2024) https://jns.edu.al/
20. Radio Free Europe. (2023, March 18). *U.S. Calls On MKO Group To Accept Albania Resettlement Offer*. Radio Free Europe. https://www.rferl.org/a/iran-us-mek-albania/24932367.html
21. Reuters. (2023, August 2). Russian hackers crash Italian bank websites, cyber agency says. *Reuters*. https://www.reuters.com/world/europe/russian-hackers-crash-italian-bank-websites-cyber-agency-2023-08-01/
22. Saracini, K. (2023, September 20). *Rama: Shqipëria e ka bërë zgjedhjen e saj, të qëndrojë përkrah dhe me Ukrainën*. Agjencia Telegrafike Shqiptare (ATA). rama: Shqip%C3%ABria e ka b%C3%ABr%C3%AB zgjedhjen e saj, t%C3%AB q%C3%ABndroj%C3%AB p%C3%ABrkrah dhe me Ukrain%C3%ABn

Bibliography

[1] S. &. P. P. Duguin, "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliament.," *https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023),* 2023.

[2] "Zbardhet hetimi i SPAK për banorët e MEK, rreth 150 pajisje të sekuestruara.," *Euronews Albania,* Vols. https://euronews.al/zbardhet-hetimi-i-spak-per-banoret-e-mek-rreth-150-pajisje-te-sekuestruara/, 2023.

[3] "U.S. Calls On MKO Group To Accept Albania Resettlement Offer. Radio Free Europe. https://www.rferl.org/a/iran-us-mek-albania/24932367.html," *Radio Free Europe. https://www.rferl.org/a/iran-us-mek-albania/24932367.html,* 2023.

[4] "Microsoft investigates Iranian attacks against the Albanian government," *Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/,* 2022.

[5] “TechAccelerator në Bruksel, Karçanaj: Shqipëria plotësisht digjitale në 2030 përmes Inteligjencës Artificiale – Agjencia Kombëtare e Shoqërisë së Informacionit.,” *Akshi.gov.al; AKSHI. https://akshi.gov.al/techaccelerator-ne-bru,* 2023.

[6] A. Bleih, “Israel-Hamas vs. Ukraine-Russia War.,” *Cyberint. https://cyberint.com/blog/research/israel-hamas-vs-ukraine-russia-war/#Conclusions,* 2023.

[7] F. 2. A. s. d. i. n. m. p. s. k. A. P. h.-s.-d.-i.-n.-m.-p.-s.-k. 1. Albanian Post. (2023, “Autoritetet shqiptare dhe izraelite nënshkruajnë marrëveshje për sigurinë kibernetik,” *Albanian Post, https://albanianpost.com/autoritetet-shqiptare-dhe-izraelite-nenshkruajne-marreveshje-per-sigurine-kibernetike/,* 2023.

[8] “Banka Credins: Kemi rënë pre e një sulmi kibernetik, asetet e klientëve janë të sigurta dhe paprekura.,” *A2news.com. https://a2news.com/2022/12/23/banka-credins-kemi-rene-pre-e-nje-sulmi-kibernetik-asetet-e-klienteve-jane-te-,* 2022.

[9] “Russian hackers crash Italian bank websites, cyber agency says.,” *Reuters. https://www.reuters.com/world/europe/russian-hackers-crash-italian-bank-websites-cyber-agency-2023-08-01/,* 2023.

[10] “National Cyber Security Authority.,” *AKCESK, https://cesk.gov.al/wp-content/uploads/2024/04/ligj-2024-03-21-25-5.pdf,* 2024.

[11] “Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity.,” *BIRN. https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/,* 2023.

[12] “Zbardhet hetimi i SPAK për banorët e MEK, rreth 150 pajisje të sekuestruara.,” *Euronews Albania. https://euronews.al/zbardhet-hetimi-i-spak-per-banoret-e-mek-rreth-150-pajisje-te-sekuestruara/,* 2023.

[13] “Russian hackers crash Italian bank websites, cyber agency says.,” *Reuters. https://www.reuters.com/world/europe/russian-hackers-crash-italian-bank-websites-cyber-agency-2023-08-01/,* 2023.

[14] K. Saracini, *Agjencia Telegrafike Shqiptare (ATA).*

[15] “Ministeriali i OSBE, Ministri Hasani: Evropa e sigurtë vetëm me njohjen e pavarësisë së Kosovës.,” *Punetejashtme.gov.al. https://punetejashtme.gov.al/ministeriali-i-osbe-ministri-hasani-evropa-e-sigurt,* 2023.

[16] M. Miller, “Albania weighed invoking NATO’s Article 5 over Iranian cyberattack.,” *POLITICO. https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347,* 2022.

[17] R. A. (. M. Montgomery, “Iranian-backed attacks on Albania highlights need for Cyber Capacity Building.,” *The Cipher Brief. https://www.thecipherbrief.com/column_article/iranian-backed-attacks-on-albania-highlights-need-for-cyb,* 2022.

[18] G. E. Pashaj K., “"The importance of critical information infrastructure protection – Case of Albania",” *Journal of Natural Sciences, https://jns.edu.al/,* no. 35, 2024.

[19] S. Lyngaas, “Albania blames Iran for second cyberattack since July,” *CNN Politics. CNN. https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html,* 2022.

[20] “National Cyber Security Authority. Deklaratë Zyrtare ONE . NCSA. https://cesk.gov.al/deklarate-zyrtare-3/,” *NCSA. https://cesk.gov.al/deklarate-zyrtare-3/*, 2023b.

[21] D. 2. A. o. I. T. A. A. F. T. I. I. i. A. –. I. R. P. A. h.-o.-h.-j.-a.-f.-t.-i. 1. National Cyber Security Authority. (2023c, “National Cyber Security Authority. Analysis of Iranian Threat Actors Attack Files That Impacted Infrastructure in AL – Incident Report Parlament.,” *AKCESK.* *https://cesk.gov.al/en/analysis-of-homeland-justice-attack-files-that-impact*, 2023c.

[22] “National Cyber Security Authority.Raport Incidenti Instati – Analizë MEK-DDMC.,” *AKSK.* *https://cesk.gov.al/raport-incidenti-instati-analize-mek-ddmc/*, 2024b.

[23] “National Cyber Security Authority. Raport Qeverisja Kibernetike 2023.,” *AKSK.* *https://cesk.gov.al/raport-qeverisja-kibernetike-2023/*, 2023a.