PhD Tal Pavel
The Institute for Cyber Policy Studies, Israel
Communication Science, Alma Mater Europaea – European Center, Maribor, Slovenia
ORCID: 0000-0002-4046-0867
e-mail: Tal@cybureau.org

THE RIPPLE EFFECT: BILATERAL, REGIONAL, AND INTERNATIONAL IMPLICATIONS OF IRANIAN CYBER ATTACKS ON ALBANIA

“Cyber threats to one party in the Western Balkans are threats to all of us in the region. Tangible regional collaboration is essential to the collective safety and security of our communities in cyberspace"[1].

Igli Tafa, Director General of the National Cyber Security Authority of Albania

Abstract

The paper analyses the Albanian bilateral, regional and international implications of the Iranian cyber-attacks in Albania during 2021-2024.This analysis explores the far-reaching consequences of Iran's cyber operations against Albania. It investigates how these attacks impact Albania's bilateral relationship with Iran, regional stability, and the broader international cybersecurity landscape. This study prioritised selecting diverse and reliable sources to ensure a comprehensive analysis. Sources were chosen based on their relevance to the research topic, reliability, and diversity, incorporating academic articles, analyses from cyber research companies, journalistic reports, and official publications. The findings reveal that Iran's cyber operations had significant multi-level impacts. Locally, the attacks disrupted Albania's critical infrastructure, exposing vulnerabilities in its cybersecurity readiness and cutting its diplomatic relations with Iran. Regionally, the incident heightened tensions in the Western Balkans, amplifying concerns over foreign cyber influence and regional stability. Internationally, the attacks underscored the growing risks of state-sponsored cyber aggression, prompting calls for stronger global cooperation and frameworks to counter such threats. The study highlights the need for improved cyber resilience, enhanced regional collaboration, and coordinated international responses to address evolving cyber challenges.

Keywords: Albania, Cyber Security, Strategy, Balkans, Iran, NATO, EU.

[1] ORF America, ‘Global Cyber Policy Dialogues: Western Balkans’ (20 November 2024) <https://orfamerica.org/recent-events/western-balkans-cyber-experts-meeting> [accessed: 1.12.2024]

INTRODUCTION

Cyber-attacks – Between the years 2021-2024, Albania was under several waves of cyber-attacks allegedly performed by Iranian state-sponsored actors: (1) initial access to the network of the Albanian Government as early as May 2021[2], followed by email exfiltration from the compromised network between October 2021 and January 2022. (2) email harvesting between November 2021 and May 2022. (3) Destructive campaign in mid-July 2022[3] (4) and in September 2022[4] against the Albanian government computer system that destroyed data and disrupted government services. (5) Cyber-attack on the Albanian Parliament in December 2023, disrupting the Parliament services[5]. (6) Destroyed and leaked data of allegedly over 100 terabytes of Albania's geographic information system and population data at the end of January 2024[6].

Attribution – In his message from 7 September 2022, Albania's Prime Minister Edi Rama mentioned "the engagement of four groups that enacted the aggression – one of them being a notorious international cyber-terrorist group, which has been a perpetrator or co-perpetrator of earlier cyber-attacks targeting Israel, Saudi Arabia, UAE, Jordan, Kuwait and Cyprus"[7]. Mandiant researchers stressed "with moderate confidence that one or multiple threat actors who have operated in support of Iranian goals are involved", mentioning "a cross-team collaboration or other scenarios that we lack insight into at this time"[8]. Microsoft researchers assessed "with high confidence that multiple Iranian actors participated in this attack—with different actors responsible for distinct phases"[9].

[2] Microsoft Threat Intelligence, Microsoft Investigates Iranian Attacks against the Albanian Government (Microsoft Security Blog, 8 September 2022) <https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/> accessed 7 September 2024.

[3] Elona Elezi and Niloofar Gholami, Albania Blames Iran for Cyberattacks (Deutsche Welle, 16 September 2022) <https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285> accessed 13 October 2024.

[4] Cybersecurity & Infrastructure Security Agency (CISA), Iranian State Actors Conduct Cyber Operations Against the Government of Albania (23 September 2022) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a> accessed 19 October 2024.

[5] Llazar Semini, A Cyberattack Targets Albanian Parliament's Data System, Halting Its Work (27 December 2023) <https://apnews.com/article/albania-cyberattack-parliament-iran-cc1a03b58bd753bbe935ad74f1abc0f7> accessed 19 October 2024.

[6] Daryna Antoniuk, Iran-Linked Hackers Claim Attack on Albania's Institute of Statistics (Recorded Future News, 2 February 2024) <https://therecord.media/iran-linked-hackers-claim-attack-on-albania-census-org> accessed 19 October 2024.

[7] Albanian Government, Videomessage of Prime Minister Edi Rama (7 September 2022) <https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/> accessed 13 October 2024.

[8] Luke Jenkins and others, ROADSWEEP Ransomware Targets the Albanian Government (*Google Cloud Blog*, 4 August 2022) <https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/> accessed 2 September 2024.

[9] Microsoft Threat Intelligence (n 19).

Damages – The Iran cyber-attacks were catastrophic for Albanian public services, hampering the Government's ability to govern and affecting every citizen. (1) The vast majority of government services had been digitised and brought online to circumvent the slow and corrupt bureaucratic public process. (2) The hackers managed to gather, delete and leak private and even classified information of the general public and civil servants, including customer financial records, the data of everyone who entered and exited Albania for more than 17 years, and the identities of hundreds of undercover Albanian intelligence officers[10]. Indeed, Prime Minister Edi Rama emphasised, "Based on the investigation, the scale of the attack was such that the aim behind it was to completely destroy our infrastructure back to the full paper age, and at the same time, wipe out all our data"[11].

BILATERAL

Iran – Due to the 15 July 2022 cyber-attacks on its digital infrastructure, Albania cut diplomatic ties with Iran on 7 September 2022, the first known case of a country cutting diplomatic relations over a cyber-attack[12]. It issued an ultimatum to the diplomatic staff at the Iranian embassy to leave the country within 24 hours. Prime Minister Edi Rama said in a video statement, "The in-depth investigation provided us with indisputable evidence that the cyberattack against our country was orchestrated and sponsored by the Islamic Republic of Iran"[13].

Soon, the conflict between the two countries moved to the international diplomatic arena.

On the same day, the Permanent Representative of Albania to the United Nations addressed a letter to the Secretary-General and the President of the Security Council, stating that "A thorough, in-depth investigation conducted in cooperation with specialised partner agencies on cyberterrorism has now confirmed, beyond any doubt, that the cyberattack was a state-sponsored aggression carried out by four groups, orchestrated and sponsored by the Islamic Republic of Iran"[14].

The next day, Albanian special forces forced entry into the Iranian embassy, surrounding the compound after the last staff members departed in

[10] Ayman Oghanna, How Albania Became a Target for Cyberattacks (25 March 2023) <https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/#selection-1123.0-1123.44> accessed 19 October 2024.

[11] Tim Starks, 'How Albania Reckoned with Alleged Iranian Hackers' (*The Washington Post*, 26 September 2022) <https://www.washingtonpost.com/politics/2022/09/26/how-albania-reckoned-with-alleged-iranian-hackers/> accessed 20 October 2024.

[12] Tim Starks, Albania Is the First Known Country to Sever Diplomatic Ties over a Cyberattack (*The Washington Post,* 8 September 2022) <https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/> accessed 13 December 2024.

[13] Albanian Government (n 7).

[14] Ferit Hoxha, Letter Dated 7 September 2022 from the Permanent Representative of Albania to the United Nations Addressed to the Secretary-General and the President of the Security Council (2022) <https://documents.un.org/doc/undoc/gen/n22/586/41/pdf/n2258641.pdf> accessed 21 October 2024.

compliance with the Government's expulsion order[15]. The Iranian Ministry of Foreign Affairs "strongly condemn the Albanian government's anti-Iran measure"[16].

On 10 September 2022, the Permanent Representative of the Islamic Republic of Iran addressed a letter to the United Nations Secretary-General and the Security Council President, rejected allegations of a cyberattack against Albania and called the claims false and politically motivated. The letter highlights Iran's victimisation from cyberattacks and accuses the Mujahedin-e Khalq Organization (MKO), hosted in Albania, of orchestrating such incidents with foreign backing. The letter condemns Albania's breach of diplomatic protocols by forcibly entering Iran's diplomatic premises, deeming it a violation of international law. It also emphasises Iran's readiness to cooperate in addressing accusations while reserving the right to defend its interests under international law[17].

On 14 September 2022, Iran's National Center for Cyberspace (NCC) announced a statement denying the allegation of committing the cyber attacks ("The Islamic Republic of Iran, while underlining that it pursues peaceful goals and purposes in cyberspace and information and communication technology by all countries, rejects baseless accusations against it with respect to alleged cyberattacks against Albania") and assisted support in investigating the cyber attacks ("expresses readiness to coordinate the dispatching of a technical delegation to investigate the issue and exchange information among computer emergency response teams (CERTs)")[18].

Speaking at the 77th UN General Assembly session on 24 September 2022, Prime Minister Edi Rama condemned Iran for its cyberattacks on Albania, describing them as a severe threat to national security and international stability. He highlighted the damaging impact on Albania's infrastructure and sovereignty, calling for global solidarity to combat cyber warfare and ensure accountability for such actions. Rama stressed that such attacks undermine trust and peace, urging the international community to strengthen defences against state-sponsored cyber aggression[19]. Two days later, the Delegation of the Islamic Republic of Iran to the United Nations stated that "Iran

[15] The Arab Weekly, Weeks after a Major Cyberattack, Albanian Police Force Open Iranian Embassy (9 September 2022) <https://thearabweekly.com/weeks-after-major-cyberattack-albanian-police-force-open-iranian-embassy> accessed 13 December 2024.

[16] Ministry of Foreign Affairs of the Islamic Republic of Iran, The Iranian Ministry of Foreign Affairs Strongly Condemns Albania's Anti-Iran Measure (8 September 2022) <https://en.mfa.gov.ir/portal/newsview/692576> accessed 13 December 2024.

[17] Amir Saeid Iravani, Letter Dated 10 September 2022 from the Permanent Representative of the Islamic Republic of Iran to the United Nations Addressed to the Secretary-General and the President of the Security Council (12 September 2022) 1 <https://documents.un.org/doc/undoc/gen/n22/587/06/pdf/n2258706.pdf> accessed 16 December 2024.

[18] Tehran Times, Iran Ready to Participate in Investigation into Albania's Cyberattack: Statement (14 September 2022) <https://www.tehrantimes.com/news/476755/Iran-ready-to-participate-in-investigation-into-Albania-s-cyberattack> accessed 13 December 2024.

[19] UN Audiovisual Library, Albania - Prime Minister Addresses General Debate, 77th Session (24 September 2022) <https://media.un.org/avlibrary/en/asset/d293/d2938921> accessed 16 December 2024.

categorically rejects such fictitious accusations, which are unfounded and based solely on false and erroneous assumptions"[20].

In response to a letter dated 6 June 2023 from the Permanent Representative of Albania to the United Nations addressed to the President of the Security Council[21], the Permanent Mission of The Islamic Republic of Iran - New York issued a letter to the President of the UN Secretary-General dated 16 June 2023 asserting again that "The Islamic Republic of Iran strongly and unequivocally rejected and denounced any kind of attribution to itself for the alleged cyber-attack on Albania's infrastructure in a letter dated 10 September 2022 (S/2022/685). Therefore, the allegations leveled against Iran during the abovementioned meeting are completely unfounded and are categorically rejected"[22].

Again, on 20 June 2024, the First Counselor and Representative of the Islamic Republic of Iran to the United Nations addressed the President of the council regarding the "Right of Reply to Anti-Iran Allegations During UNSC Session on Cybersecurity", arguing that "the representatives of Albania and the Israeli regime have misused this Chamber to level unsubstantiated claims against Iran, falsely accusing my country of supporting cyberattacks". He mentioned that Iran "in good faith, extended an offer to the government of Albania to cooperate and engage constructively to clarify the unfounded accusation leveled against Iran, but unfortunately, our request went unanswered"[23].

On 27 September 2024, Prime Minister Edi Rama, speaking at the 79th UN General Assembly session, condemned the cyberattacks conducted by Iran against Albania, emphasising their impact on national security and calling for international cooperation to address such threats[24].

Israel – After the September 2022 Iranian cyber-attack on Albania, Israel offered to share knowledge and experience in cyber defence assistance[25]. On

[20] Permanent Mission Of The Islamic Republic Of Iran - New York, 'Reply of the Delegation of the Islamic Republic of Iran to the Statement by Albania. Before the 77th Session of the United Nations General Assembly. On "General Debate" New York, 26 September 2022' (Ministry of Foreign Affairs of I.R.Iran, 26 September 2022) <https://newyork.mfa.ir/portal/product/9700/451/Reply-to-the-statement-by-Albania-UNGA> accessed 16 December 2024.

[21] Ferit Hoxha, Letter Dated 6 June 2023 from the Permanent Representative of Albania to the United Nations Addressed to the President of the Security Council' (7 June 2023) 1 <https://documents.un.org/doc/undoc/gen/n23/162/08/pdf/n2316208.pdf> accessed 17 December 2024

[22] Permanent Mission Of The Islamic Republic Of Iran - New York, Letter Dated 16 June to the President of the UN Secretary General (*Ministry of Foreign Affairs of I.R.Iran*, 16 June 2023) <https://newyork.mfa.ir/portal/product/10810/451/Letter-Dated-16-June-to-the-President-of-the-UN-Secretary-General> accessed 17 December 2024.

[23] Permanent Mission Of The Islamic Republic Of Iran - New York, Right of Reply to Anti-Iran Allegations During UNSC Session on Cybersecurity (*Ministry of Foreign Affairs of I.R.Iran*, 20 June 2024) <https://newyork.mfa.ir/portal/newsview/748245/Right-of-Reply-to-Anti-Iran-Allegations-During-UNSC-Session-on-Cybersecurity> accessed 17 December 2024.

[24] UN Web TV, 'Albania - Prime Minister Addresses General Debate, 79th Session' (27 September 2024) <https://webtv.un.org/en/asset/k1x/k1xhb91bek> accessed 16 December 2024.

[25] The Times of Israel, 'Israel Offers Cyber Aid to Albania, Which Severed Iran Ties over Hacking Claim' (13 September 2022) <https://www.timesofisrael.com/israel-offers-cyber-aid-to-albania-which-severed-iran-ties-over-hacking-claim/> accessed 13 December 2024.

February 2023, during the "Cyber Security Challenges in Albania" conference in Tirana, the Ambassador of the State of Israel, Galit Peleg, stated that "the State of Israel has concretised the cooperation with Albania, through the signing of the Memorandum of Cooperation, with a focus on increasing professional capacities, sharing information and strengthening defense capabilities between the two states"[26].

REGIONAL

NATO's statement on 8 September 2022 was general in attributing the cyber attacks to Iran, indicating that "Allies acknowledge the statements by Albania and other Allies attributing the responsibility for the cyber attack to the Government of Iran" and affirming, "We will continue raising our guard against such malicious cyber activities in the future, and support each other to deter, defend against and counter the full spectrum of cyber threats, including by considering possible collective responses"[27]. The Albanian Government ultimately decided against triggering Article Five of the NATO declaration[28], which treats an attack against one member as an attack against them all, requiring collective defence[29].

In his speech at the Prague Cyber Security Conference 2022 on 3 November 2022, NATO Deputy Secretary General Mircea Geoană condemned the Iranian cyberattacks on Albania's national infrastructure, describing the incident as an attempt to destabilise a NATO member state and harm its citizens. He emphasised NATO's collective response, solidarity with Albania, and the importance of enhanced cooperation to defend against cyber threats[30].

At the same time, The Council of Europe conducted an "International workshop on conducting criminal investigations of ransomware attacks" in The Hague, Netherlands, on 3-4 November 2022[31]. As part of the workshop, Edmond Koloshi, prosecutor at the General Prosecutor's Office of Albania,

[26] National Cyber Security Authority (NCSA), 'Addressing Cyber Security Challenges, in the Focus of the Discussions of the "Cyber Security Challenges in Albania" Conference' <https://aksk.gov.al/en/addressing-cyber-security-challenges-in-the-focus-of-the-discussions-of-the-cyber-security-challenges-in-albania-conference/> accessed 17 December 2024.

[27] North Atlantic Treaty Organization (NATO), 'Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania, 08-Sep.-2022' (8 September 2022) <https://www.nato.int/cps/en/natohq/official_texts_207156.htm> accessed 19 October 2024.

[28] Michaela Ppruckova, 'Cyber Attacks and Article 5 – a Note on a Blurry but Consistent Position of NATO' (The NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), 2022) <https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/> accessed 19 December 2024.

[29] Maggie Miller, 'Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack' (POLITICO, 5 October 2022) <https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347> accessed 21 October 2024.

[30] NATO, 'Speech by NATO Deputy Secretary General Geoană at the Prague Cyber Security Conference 2022 in Prague, Czechia, 03-Nov.-2022' (3 November 2022) <https://www.nato.int/cps/en/natohq/opinions_208702.htm> accessed 17 December 2024.

[31] Council of Europe, 'Ransomware Attacks Workshop - Cybercrime' (3 November 2022) <https://www.coe.int/en/web/cybercrime/ransomware-attacks-workshop> accessed 16 December 2024.

delivered a presentation titled "Threats, trends and impact of ransomware attacks in Albania"[32].

On 4-5 November 2024, Albania hosted the First Networking and Technical Workshop of Cybersecurity Agencies in the Western Balkans, Georgia, and Moldova with the cooperation of the United Nations Development Programme (UNDP) "In response to the growing prevalence and sophistication of cyber threats, domestic and regional cooperation is becoming increasingly crucial to securing digital infrastructures". The workshop discussed the urgent need to bolster national defences and align cybersecurity frameworks with EU standards. It underscored the role of partnerships, education, and capacity-building to mitigate vulnerabilities and prepare for evolving threats. The event also promoted the creation of a Cybersecurity Cooperation Network (CCN) for real-time threat intelligence and response.

INTERNATIONAL

Diplomatic – Immediately after Albania's Prime Minister's announcement on 7 September 2022, support statements were issued by the U.S. and U.K.

On 7 September 2022, The White House National Security Council stated, "The United States strongly condemns Iran's cyberattack against our NATO Ally, Albania", and held Iran accountable for this "unprecedented cyber incident". The statement emphasised the U.S. commitment "to support Albania's remediation efforts over longer-term"[33]. On 26 October 2022, the Principal Deputy National Security Advisor Jon Finer met with Albanian Foreign Minister Olta Xhacka and "reaffirmed the United States' immediate, significant, and continuing support for Albania's efforts to strengthen its cybersecurity in the face of repeated, disruptive cyber attacks by Iran"[34].

During the "Cyber Security Challenges in Albania" conference[35] On 7 February 2023, the U.S. ambassador in Albania, Yuri Kim, stated that the cyber-attacks in Albania, "the United States' NATO Ally, have been dangerous, reckless, and a threat to the Albanian people and the Albanian nation. The United States will not hesitate to respond forcefully to malicious cyber actors when their actions threaten the United States or our Allies, or friends and partners", indicating the U.S. actions taken to support Albania in terms of diplomacy, policy, cyber forensic investigation, incident response, training, financial, strategic planning and including the strengthening Albania's cyber

[32] Edmond Koloshi, 'Threats, Trends and Impact of Ransomware Attacks in Albania' (2022) <https://rm.coe.int/session-i-edmond-koloshi-albania/1680a8cbe4> accessed 16 December 2024.

[33] The White House, 'Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania' (7 September 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/> accessed 13 October 2024.

[34] The White House, 'Readout of Principal Deputy National Security Advisor Jon Finer's Meeting with Albanian Foreign Minister Olta Xhacka' (27 October 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/27/readout-of-principal-deputy-national-security-advisor-jon-finers-meeting-with-albanian-foreign-minister-olta-xhacka/> accessed 16 December 2024.

[35] National Cyber Security Authority (NCSA) (n 26).

capacity by "implementing one of our largest ever security assistance efforts, amounting to $50 million in support of hardening Albania's cyber defenses. This is only the beginning". The Ambassador determined firmly, "You are not alone. You're not alone in being targeted for cyber-attacks, and you are definitely not alone in the response. The United States is with you"[36].

The U.K. "condemned the Iranian state for a cyber attack against Albania's government that destroyed data and disrupted essential government services, including paying utilities, booking medical appointments and enrolling schoolchildren", mentioning Foreign Secretary James Cleverly firm stand that "Iran's reckless actions showed a blatant disregard for the Albanian people, severely restricting their ability to access essential public services"[37].

Sanctions – Besides the support declaration, the U.S. Department of the Treasury immediately issued a statement "designating Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence for engaging in cyber-enabled activities against the United States and its allies". The statement mentioned the Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson's announcement that "Iran's cyber attack against Albania disregards norms of responsible peacetime State behavior in cyberspace, which includes a norm on refraining from damaging critical infrastructure that provides services to the public"[38].

Cyber – In March 2023, a defensively Cyber National Mission Force (CNMF) team concluded a three-month deployment to Albania as part of "Hunt Forward" operations to "survey the damage and gain insights into the tactics used" as part of their mission to foreign countries to "hunt for threats on their networks at the invitation of host nations", in operations that "require important relationship and trust building with partners in order to place sensors on their networks to observe traffic". The team provided technical findings to the Albanian Government to strengthen its networks, enhancing U.S. cyber defences, partners, and allies by identifying and exposing adversaries' activities, tools, and tactics, enabling partners to take action and collectively improve cybersecurity against shared threats.

Indeed, Mirlinda Karçanaj, general director of the National Agency of Information Society, an Albanian government institution that coordinates information systems, stated, "The cooperation with U.S. Cyber Command was very effective and made us feel safe by assuring that we have followed all the right steps in responding to these sophisticated attacks", expressing the hope that "this cooperation will continue in the future so that we can further exchange experiences and increase our capacities to another level"[39].

[36] U.S. Embassy in Albania, 'Remarks by U.S. Ambassador Yuri Kim at the "Cyber Security Challenges in Albania" Conference' (7 February 2023) <https://al.usembassy.gov/remarks-by-u-s-ambassador-yuri-kim-at-the-cyber-security-challenges-in-albania-conference/> accessed 17 December 2024.

[37] GOV.UK, 'UK Condemns Iran for Reckless Cyber Attack against Albania' (7 September 2022) <https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania> accessed 14 October 2024.

[38] U.S. Department of the Treasury, 'Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities' (9 September 2022) <https://home.treasury.gov/news/press-releases/jy0941> accessed 19 October 2024.

[39] Cyber National Mission Force Public Affairs, '"Committed Partners in Cyberspace": Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania' (23 March

The Big Tech – Another aspect of the international initiative to mitigate the cyber-attacks in Albania was the involvement of the international Big Tech corporates, such as the joint international team of experts from the FBI and Microsoft, who worked with Albanian and other experts to pinpoint and tackle those attacks[40]. The White House National Security Council statement affirmed that the U.S. government "has been on the ground" working alongside private sector partners to mitigate, recover and investigate the 15 July 2022 cyber-attack[41]. Besides, various companies, including Microsoft[42] and Google[43], were involved in discovering, analysing, and researching the cyber-attacks in Albania.

Such "Hunt Forward" operations are conducted by the United States Cyber Command (USCYBERCOM), which contracted Sealing Technologies to provide equipment for defensive cyber operations abroad on the networks of partner nations[44]. In addition, the information about the tools, techniques, and procedures of malicious cyber actors was shared with the Albanian Government and "some private companies with critical roles in the digital infrastructure of both countries"[45].

CONCLUSIONS

This study aimed to portray the bilateral, regional and international implications of Iran's cyber-attacks on Albania between 2021 and 2024. The research stresses several conclusions and recommendations:

(1) **Data Breach** – The attacks resulted in the theft, deletion, and leak of private and classified information, including customer financial records and the identities of undercover intelligence officers.

(2) **Local Disruption** – Locally, the attacks severely disrupted Albania's critical infrastructure, exposed vulnerabilities in its cybersecurity readiness, hampered the Albanian Government's governability and affected every citizen.

(3) **Multi-Level Impact** – Iran's cyber operations had significant bilateral, regional, and international impacts.

2023) <https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/> accessed 16 December 2024.

[40] Starks (n 11).

[41] The White House (n 33).

[42] Microsoft Threat Intelligence (n 2).

[43] Google Cloud Blog, 'ROADSWEEP Ransomware Targets the Albanian Government' (4 August 2022) <https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/> accessed 19 December 2024.

[44] SealingTech, 'Sealing Technologies Selected For Nearly $60M Agreement By US Cyber Command's Cyber National Mission Force' (21 April 2022) <https://web.archive.org/web/20220421185855/https://www.sealingtech.com/press/sealing-technologies-selected-for-nearly-60m-agreement-by-us-cyber-commands-cyber-national-mission-force/> accessed 16 December 2024.

[45] Jeff Seldin, 'US, Albania on "Hunt" for Iranian Cyber Actors' (*Voice of America (VOA)*, 23 March 2023) <https://www.voanews.com/a/us-albania-on-hunt-for-iranian-cyber-actors/7018167.html> accessed 16 December 2024.

(4) **Regional and International Instability** – The cyber attacks underscored the growing risks of state-sponsored cyber aggression undermining regional and international stability.
(5) **Attribution** – While there was some initial uncertainty, investigations pointed to the involvement of multiple Iranian threat actors.
(6) **Diplomatic Fallout** – Albania became the first country to cut diplomatic ties with another nation over a cyber-attack, highlighting the severity of the incident.

RECOMMENDATIONS

(1) **Dynamic Cyber Ecosystem** – The cyber attacks demonstrated the need for adaptive cybersecurity frameworks that rapidly respond to sophisticated, multi-stage cyber threats.
(2) **Transnational Cyber Resilience** – Robust cross-border cyber collaboration mechanisms, particularly among NATO and Western Balkan nations, joint cyber defence rapid response teams with clearly defined escalation and intervention protocols, and standardised information sharing platforms that enable immediate threat communication while maintaining data privacy.
(3) **Psychological and Societal Resilience** – There is a need to develop comprehensive public awareness programs about cyber threats and a societal understanding of the geopolitical dimensions of cyber warfare.
(4) **The 'Big Tech'** – The mitigation of the cyber attacks on Albania demonstrated the importance of the 'Big Tech' companies not only by supplying the needed technology to mitigate cyber threats but also by involving those private companies in detecting and analysing the cyber incidents while supporting nation-states.
(5) **Information Sharing** – The research underscores the critical role of cooperation and information sharing between nation-states, private sector players, ICT vendors, and cybersecurity researchers. Effective collaboration relies on sharing accurate, complete information with partners and allies at all levels—local, regional, and international—while ensuring privacy, data security, and system integrity.
(6) **Technology** – The relevant technology must be implemented, and security patches must be updated continuously to avoid security vulnerabilities while minimising the systems' risk and functionalities.
(7) **Regulations** – International and local regulations must be formulated and implemented to address new threats posed by various actors using cutting-edge technologies on multiple platforms.
(8) **Awareness** – Implementing ongoing training programs at national, sectorial, and organisational levels to raise awareness is crucial to enhancing the identifying behaviour of detecting and avoiding security incidents.
(9) **Active Cyber Defence Operations** – Implement defensive "Hunt Forward" operations to proactively identify and mitigate network

threats, building trust with partners to improve collective cybersecurity against shared threats.

(10) **Diplomatic and International Cooperation** – Maintain robust diplomatic channels to address state-sponsored cyber aggression and promote international cooperation to deter and respond to cyber threats.

Those recommendations align with John McCumber's information security model from 1991, emphasising the need for a holistic approach that integrates technology, policy and practice, education, training, and awareness at all levels[46].

FUTURE RESEARCH

The following research will focus on Albania and the Iranian cyber-attacks: analyse the national cyber defence transformation, cyber measures post-attack, cyber capacity-building initiatives, the legal and regulatory framework development, technological adaptation and recovery, psychological and organisational resilience, and economic impact assessment.

Literature

Albanian Government, 'Videomessage of Prime Minister Edi Rama' (7 September 2022) <https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/> accessed 13 October 2024

Antoniuk D, 'Iran-Linked Hackers Claim Attack on Albania's Institute of Statistics' (Recorded Future News, 2 February 2024) <https://therecord.media/iran-linked-hackers-claim-attack-on-albania-census-org> accessed 19 October 2024

Council of Europe, 'Ransomware Attacks Workshop - Cybercrime' (3 November 2022) <https://www.coe.int/en/web/cybercrime/ransomware-attacks-workshop> accessed 16 December 2024

Cyber National Mission Force Public Affairs, '"Committed Partners in Cyberspace": Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania' (23 March 2023) <https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/> accessed 16 December 2024

Cybersecurity & Infrastructure Security Agency (CISA), 'Iranian State Actors Conduct Cyber Operations Against the Government of Albania' (23 September 2022) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a> accessed 19 October 2024

Elezi E and Gholami N, 'Albania Blames Iran for Cyberattacks' (Deutsche Welle, 16 September 2022) <https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285> accessed 13 October 2024

[46] John R McCumber, 'Information Systems Security: A Comprehensive Model' [1991] 14th National Computer Security Conference 328 <https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1991/10/01/proceedings-14th-national-computer-security-conference-1991/documents/1991-14th-NCSC-proceedings-vol-1.pdf> accessed 3 October 2020.

Google Cloud Blog, 'ROADSWEEP Ransomware Targets the Albanian Government' (4 August 2022) <https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/> accessed 19 December 2024

GOV.UK, 'UK Condemns Iran for Reckless Cyber Attack against Albania' (7 September 2022) <https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania> accessed 14 October 2024

Hoxha F, 'Letter Dated 7 September 2022 from the Permanent Representative of Albania to the United Nations Addressed to the Secretary-General and the President of the Security Council' (2022) <https://documents.un.org/doc/undoc/gen/n22/586/41/pdf/n2258641.pdf> accessed 21 October 2024

——, 'Letter Dated 6 June 2023 from the Permanent Representative of Albania to the United Nations Addressed to the President of the Security Council' (7 June 2023) 1 <https://documents.un.org/doc/undoc/gen/n23/162/08/pdf/n2316208.pdf> accessed 17 December 2024

Iravani AS, 'Letter Dated 10 September 2022 from the Permanent Representative of the Islamic Republic of Iran to the United Nations Addressed to the Secretary-General and the President of the Security Council ' (12 September 2022) 1 <https://documents.un.org/doc/undoc/gen/n22/587/06/pdf/n2258706.pdf> accessed 16 December 2024

Jenkins L and others, 'ROADSWEEP Ransomware Targets the Albanian Government' (Google Cloud Blog, 4 August 2022) <https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/> accessed 2 September 2024

Koloshi E, 'Threats, Trends and Impact of Ransomware Attacks in Albania' (2022) <https://rm.coe.int/session-i-edmond-koloshi-albania/1680a8cbe4> accessed 16 December 2024

McCumber JR, 'Information Systems Security: A Comprehensive Model' [1991] 14th National Computer Security Conference 328 <https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1991/10/01/proceedings-14th-national-computer-security-conference-1991/documents/1991-14th-NCSC-proceedings-vol-1.pdf> accessed 3 October 2020

Microsoft Threat Intelligence, 'Microsoft Investigates Iranian Attacks against the Albanian Government' (Microsoft Security Blog, 8 September 2022) <https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/> accessed 7 September 2024

Miller M, 'Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack' (POLITICO, 5 October 2022) <https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347> accessed 21 October 2024

Ministry of Foreign Affairs of the Islamic Republic of Iran, 'The Iranian Ministry of Foreign Affairs Strongly Condemns Albania's Anti-Iran Measure' (8 September 2022) <https://en.mfa.gov.ir/portal/newsview/692576> accessed 13 December 2024

National Cyber Security Authority (NCSA), 'Addressing Cyber Security Challenges, in the Focus of the Discussions of the "Cyber Security Challenges in Albania" Conference' <https://aksk.gov.al/en/addressing-cyber-security-challenges-in-the-focus-of-the-discussions-of-the-cyber-security-challenges-in-albania-conference/> accessed 17 December 2024

NATO, 'Speech by NATO Deputy Secretary General Geoană at the Prague Cyber Security Conference 2022 in Prague, Czechia, 03-Nov.-2022' (3 November 2022) <https://www.nato.int/cps/en/natohq/opinions_208702.htm> accessed 17 December 2024

North Atlantic Treaty Organization (NATO), 'Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania, 08-Sep.-2022' (8 September 2022) <https://www.nato.int/cps/en/natohq/official_texts_207156.htm> accessed 19 October 2024

Oghanna A, 'How Albania Became a Target for Cyberattacks' (25 March 2023) <https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/#selection-1123.0-1123.44> accessed 19 October 2024

ORF America, 'Global Cyber Policy Dialogues: Western Balkans' (20 November 2024) <https://orfamerica.org/recent-events/western-balkans-cyber-experts-meeting> accessed 17 December 2024

Permanent Mission Of The Islamic Republic Of Iran - New York, 'Reply of the Delegation of the Islamic Republic of Iran to the Statement by Albania. Before the 77th Session of the United Nations General Assembly. On "General Debate" New York, 26 September 2022' (Ministry of Foreign Affairs of I.R.Iran, 26 September 2022) <https://newyork.mfa.ir/portal/product/9700/451/Reply-to-the-statement-by-Albania-UNGA> accessed 16 December 2024

——, 'Letter Dated 16 June to the President of the UN Secretary General' (Ministry of Foreign Affairs of I.R.Iran, 16 June 2023) <https://newyork.mfa.ir/portal/product/10810/451/Letter-Dated-16-June-to-the-President-of-the-UN-Secretary-General> accessed 17 December 2024

——, 'Right of Reply to Anti-Iran Allegations During UNSC Session on Cybersecurity' (Ministry of Foreign Affairs of I.R.Iran, 20 June 2024) <https://newyork.mfa.ir/portal/newsview/748245/Right-of-Reply-to-Anti-Iran-Allegations-During-UNSC-Session-on-Cybersecurity> accessed 17 December 2024

Ppruckova M, 'Cyber Attacks and Article 5 – a Note on a Blurry but Consistent Position of NATO' (The NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), 2022) <https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/> accessed 19 December 2024

SealingTech, 'Sealing Technologies Selected For Nearly $60M Agreement By US Cyber Command's Cyber National Mission Force' (21 April 2022) <https://web.archive.org/web/20220421185855/https://www.sealingtech.com/press/sealing-technologies-selected-for-nearly-60m-agreement-by-us-cyber-commands-cyber-national-mission-force/> accessed 16 December 2024

Seldin J, 'US, Albania on "Hunt" for Iranian Cyber Actors' (Voice of America (VOA), 23 March 2023) <https://www.voanews.com/a/us-albania-on-hunt-for-iranian-cyber-actors/7018167.html> accessed 16 December 2024

Semini L, 'A Cyberattack Targets Albanian Parliament's Data System, Halting Its Work' (27 December 2023) <https://apnews.com/article/albania-cyberattack-parliament-iran-cc1a03b58bd753bbe935ad74f1abc0f7> accessed 19 October 2024

Starks T, 'Albania Is the First Known Country to Sever Diplomatic Ties over a Cyberattack' (The Washington Post, 8 September 2022) <https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/> accessed 13 December 2024

——, 'How Albania Reckoned with Alleged Iranian Hackers' (The Washington Post, 26 September 2022) <https://www.washingtonpost.com/politics/2022/09/26/how-albania-reckoned-with-alleged-iranian-hackers/> accessed 20 October 2024

Tehran Times, 'Iran Ready to Participate in Investigation into Albania's Cyberattack: Statement' (14 September 2022) <https://www.tehrantimes.com/news/476755/Iran-ready-to-participate-in-investigation-into-Albania-s-cyberattack> accessed 13 December 2024

The Arab Weekly, 'Weeks after a Major Cyberattack, Albanian Police Force Open Iranian Embassy' (9 September 2022) <https://thearabweekly.com/weeks-after-major-cyberattack-albanian-police-force-open-iranian-embassy> accessed 13 December 2024

The Times of Israel, 'Israel Offers Cyber Aid to Albania, Which Severed Iran Ties over Hacking Claim' (13 September 2022) <https://www.timesofisrael.com/israel-offers-cyber-aid-to-albania-which-severed-iran-ties-over-hacking-claim/> accessed 13 December 2024

The White House, 'Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania' (7 September 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/> accessed 13 October 2024

——, 'Readout of Principal Deputy National Security Advisor Jon Finer's Meeting with Albanian Foreign Minister Olta Xhacka' (27 October 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/27/readout-of-principal-deputy-national-security-advisor-jon-finers-meeting-with-albanian-foreign-minister-olta-xhacka/> accessed 16 December 2024

UN Audiovisual Library, 'Albania - Prime Minister Addresses General Debate, 77th Session' (24 September 2022) <https://media.un.org/avlibrary/en/asset/d293/d2938921> accessed 16 December 2024

UN Web TV, 'Albania - Prime Minister Addresses General Debate, 79th Session' (27 September 2024) <https://webtv.un.org/en/asset/k1x/k1xhb91bek> accessed 16 December 2024

U.S. Department of the Treasury, 'Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities' (9 September 2022) <https://home.treasury.gov/news/press-releases/jy0941> accessed 19 October 2024

U.S. Embassy in Albania, 'Remarks by U.S. Ambassador Yuri Kim at the "Cyber Security Challenges in Albania" Conference' (7 February 2023)

<https://al.usembassy.gov/remarks-by-u-s-ambassador-yuri-kim-at-the-cyber-security-challenges-in-albania-conference/> accessed 17 December 2024

EFEKT FALOWANIA: DWUSTRONNE, REGIONALNE I MIĘDZYNARODOWE IMPLIKACJE IRAŃSKICH CYBERATAKÓW NA ALBANIĘ

Streszczenie

W artykule przeanalizowano albańskie dwustronne, regionalne i międzynarodowe konsekwencje irańskich cyberataków na Albanię w latach 2021-2024. Analiza ta bada dalekosiężne konsekwencje irańskich operacji cybernetycznych przeciwko Albanii. Bada, w jaki sposób ataki te wpływają na dwustronne stosunki Albanii z Iranem, stabilność regionalną i szerszy międzynarodowy krajobraz cyberbezpieczeństwa. W badaniu tym priorytetowo potraktowano wybór różnorodnych i wiarygodnych źródeł, aby zapewnić kompleksową analizę. Źródła zostały wybrane na podstawie ich znaczenia dla tematu badań, wiarygodności i różnorodności, w tym artykułów akademickich, analiz firm zajmujących się badaniami cybernetycznymi, raportów dziennikarskich i oficjalnych publikacji. Ustalenia pokazują, że irańskie operacje cybernetyczne miały znaczący wielopoziomowy wpływ. Lokalnie, ataki zakłóciły funkcjonowanie krytycznej infrastruktury Albanii, ujawniając słabe punkty jej gotowości w zakresie cyberbezpieczeństwa i zrywając stosunki dyplomatyczne z Iranem. W skali regionalnej incydent ten zwiększył napięcia na Bałkanach Zachodnich, potęgując obawy o obce wpływy cybernetyczne i stabilność regionalną. Na arenie międzynarodowej ataki podkreśliły rosnące ryzyko cyberagresji sponsorowanej przez państwa, skłaniając do wezwań do ściślejszej globalnej współpracy i ram przeciwdziałania takim zagrożeniom. Badanie podkreśla potrzebę zwiększenia odporności cybernetycznej, zacieśnienia współpracy regionalnej i skoordynowanych reakcji międzynarodowych w celu sprostania zmieniającym się wyzwaniom cybernetycznym.

Słowa kluczowe: Albania, cyberbezpieczeństwo, strategia, Bałkany, Iran, NATO, UE.