„dot.pl" - czasopismo
Rejestru domeny .pl

The Iranian Cyberattacks in Albania: Actors, Tactics, Targets

"The attack on Albania is a reminder that while the most aggressive Iranian cyber activity is generally focused in the Middle East region, it is by no means limited to it. Iran will carry out disruptive and destructive cyberattacks as well as complex information operations globally"[1].

John Hultquist, Mandiant Vice President

Tal Pavel
Communication Science, Alma Mater Europaea – European Center, Maribor, Slovenia
ORCID: https://orcid.org/0000-0002-4046-0867
E-mail: Tal@cybureau.org

Abstract

The paper aims to analyze the Iranian cyber-attacks in Albania, a small yet strategically vital nation in the Balkans. It examines the cyber incidents attributed to Iranian actors, focusing on the objective behind these operations, the tactics employed, and the sectors targeted. Given the escalating geopolitical tensions between Iran and Albania, particularly due to Albania's support for an Iranian dissident group, Tehran has increasingly used cyber warfare as a means of influence and retaliation. By assessing the effectiveness of these cyber campaigns and their implications for Albania's

Received: 01.12.2024
Accepted: 03.12.2024
Published: 03.12.2024

Cite this article as:
T. Pavel, "The Iranian Cyberattacks in Albania: Actors, Tactics, Targets"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/196772

Corresponding author:
Tal Pavel
Communication Science, Alma Mater Europaea – European Center, Maribor, Slovenia
E-mail: Tal@cybureau.org

[1] L. Semini, *Albania Cuts Diplomatic Ties with Iran over July Cyberattack*, AP News, 7 September 2022. https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a accessed 10 October 2024.

national security, the study provides insights into how state-sponsored cyber activities function as tools of foreign policy.

The goal of this study is to illuminate the complex dynamics of state-sponsored cyber aggression and its implications for national and regional security. Specifically, it examines how cyber-attacks serve as instruments for achieving political objectives, as demonstrated by Iran's use of cyber warfare against Albania. Additionally, the study explores the potential for future Iranian cyber activities targeting other Balkan states as part of its broader strategy and that of its allies.

To achieve its objective and goal, this study employs a methodical approach to source selection, ensuring a comprehensive and balanced analysis. Sources were carefully chosen for their relevance, reliability, and diversity, drawing from academic articles, cyber research company analyses, journalistic reports, and official publications. This methodology provides a solid and credible foundation for understanding the nature and implications of Iranian cyber-attacks on Albania.

Keywords: Albania, Cyber Security, Strategy, Balkans, Iran

Introduction

Over the years, Iran launched multiple cyber-attacks against various states around the globe[2]. Some of them caused much damage and gained international resonance, including a massive power outage in Turkey (2015)[3], "the biggest hack in history" against Saudi Aramco, one of the world's largest oil companies (2015)[4], the British Parliament

[2] American Coalition Against Nuclear Iran, *History of Iranian Cyber Attacks and Incidents*, 2024. https://www.unitedagainstnucleariran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat.pdf; accessed 1 September 2024; Chuck Freilich, *Major Iranian Cyeberattacks Around the World*, "The Iranian Cyber Threat", Institute for National Security Studies, 2024 https://www.inss.org.il/wp-content/uploads/2024/02/Part-3.pdf; accessed 2 September 2024.
[3] M. Halpern, *Iran Flexes Its Power by Transporting Turkey to the Stone Age,* "Observer", 22 April 2015. https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/ accessed 1 September 2024.
[4] J. Pagliery, *The inside Story of the Biggest Hack in History*, "CNN Business", 5 August 2015. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html accessed 1 September 2024.

(2017)[5], and many more various cyber-attacks against diverse sectors in the U.S.[6] and Israel[7] across the years, in addition to vast disinformation campaigns worldwide[8].

Vast literature analysed the widespread Iranian-affiliated cyber-attacks. Some refer to cybersecurity in Albania: Organised and cybercrime threat assessments (2015)[9] and regulations[10], cybersecurity awareness[11], cyber resilience[12], cyber regulations[13], and teaching cyber security in higher academic institutions in Albania[14].

Aleksander Biberaj and others (2022) examined cyber-attacks against Albania and its digital assets, including against the national database (e-Albania)[15]. Annita Larissa Sciacovelli (2023) covers the Iranian cyber-attacks in Albania relating to technical and legal attribution and the role of private security tech companies in the attribution[16].

---

[5] The Telegraph, *Iran Blamed for Cyberattack on Parliament That Hit Dozens of MPs, Including Theresa May*, 14 October 2017. https://web.archive.org/web/20171206135812/https://www.msn.com/en-gb/news/uknews/iran-blamed-for-cyberattack-on-parliament-that-hit-dozens-of-mps-including-theresa-may/ar-AAtpPag?li=AAmiR2Z&ocid=spartanntp accessed 2 September 2024.

[6] Cybersecurity & Infrastructure Security Agency (CISA), *Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad*, 4 October 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-006a accessed 2 September 2024.

[7] Ch. Freilich, *The Iranian Cyber Threat to Israel*, "The Iranian Cyber Threat", Institute for National Security Studies, 2024. https://www.inss.org.il/wp-content/uploads/2024/02/Part-4.pdf accessed 2 September 2024.

[8] Paul de Souza, *Iran's Assault on Our Democracy and a Closer Look at Their Disinformation Tactics*, LinekdIn, 28 August 2024. https://www.linkedin.com/pulse/copy-irans-assault-our-democracy-closer-look-tactics-de-souza-96baf/?trackingId=Vb8cw2ZO%2FflLSLUMKGsTcg%3D%3D accessed 2 September 2024.

[9] F. Zhilla, B. Lamallari, *Organised Crime Threat Assesment in Albania*, 2015. https://globalinitiative.net/wp-content/uploads/2018/02/Threat_Assessment_of_Albanian_Organised.pdf accessed 1 September 2024.

[10] A. Shkembi, I. Shtupi, A. Qafa, *The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation*, "Academic Journal of Interdisciplinary Studies", 2016, vol. 5, No.1, https://pdfs.semanticscholar.org/cd34/8906b7b5170601c731763dde70a27ed159f4.pdf accessed 1 September 2024.

[11] E. Moci, *Cybersecurity Awareness in Albania*, European Journal of Social Science. Education and Research, 2021, vol. 8, No. 3. https://revistia.com/files/articles/ejser_v8_i3_21/Moci.pdf accessed 1 September 2024.

[12] R. Bahiti, J. Josifi, *Towards a More Resilient Cyberspace: The Case of Albania*, Information & Security: An International Journal, 2015, vol. 32. https://connections-qj.org/system/files/3310_albania.pdf accessed 1 September 2024.

[13] E. Tiri, E. Aliaj, *Cyber-Security Regulation in Albania*, Perspectives of Law and Public Administration, 2023, vol.12, No. 2. https://www.ceeol.com/search/article-detail?id=1221788 accessed 1 September 2024.

[14] E. Ceko, *Cyber Security Issues in Albanian Higher Education Institutions Curricula,* 2021, CRJ, vol. 1(1). https://albanica.al/CRJ/article/view/2728 accessed 1 September 2024.

[15] A. Biberaj et al., *Cyber Attack Against E-Albania and Its Social, Economic and Strategic Effects,* The Journal of Corporate Governance, Insurance, and Risk Management (JCGIRM), 2022, vol. 9 (2). https://www.ceeol.com/search/article-detail?id=1161455 accessed 1 September 2024.

[16] A. L. Sciacovelli, *Taking Cyberattacks Seriously: The (Likely) Albanian Cyber Aggression and the Iranian Responsibility*, WORKING PAPER OSSERVATORIO SULLE ATTIVITÀ DELLE ORGANIZZAZIONI INTERNAZIONALI E SOVRANAZIONALI, UNIVERSALI E REGIONALI, SUI TEMI DI INTERESSE DELLA POLITICA ESTERA ITALIANA, 2023, https://ricerca.uniba.it/handle/11586/438480 accessed 1 September 2024.

Jakub Vostoupal's research (2024) analyses the attribution of the Stuxnet, WannaCry, and the 2022 cyber-attacks against Albania[17]. Therefore, the current literature does not comprehensively analyse various aspects of the Iranian cyber-attacks in Albania.

To address the literature gap, the research will analyse the following research questions: (1) What strategies and tactics have Iranian cyber actors employed in their attacks in Albania? (2) What are the threats to the Balkans from Iranian cyber-attacks?

Methodology

This study focused on choosing as diverse and reliable sources as possible. The selection of sources was based on several principles:

Relevance – the selected sources are relevant to the research topic and questions.

Reliability – choosing the most reliable and trustworthy sources.

Diversity – The research includes diverse primary and secondary sources, including academic articles, analyses by cyber research companies, journalistic articles, and official publications.

Findings

Attacks – 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[18], 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[19] (4) and September 2022[20] against the Albanian government computer system that **destroyed**

---

[17] J. Vostoupal, *Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial,* Computer Law & Security Review, 2024, vol. 54. https://www.sciencedirect.com/science/article/abs/pii/S026736492400075X accessed 1 September 2024.

[18] 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.

[19] E. Elezi, N. 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.

[20] 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.

data and disrupted government services. (5) Cyber-attack on the Albanian Parliament in December 2023, **disrupting** the Parliament services[21]. (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[22].

Methods – The National Institute of Standards and Technology (NIST) defines Computer Network Operations (CNO) as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace"[23]. CNO includes three known types of attacks:

(1) Computer network Exploitation (CNE) – "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[24].

(2) Computer Network Attack (CNA) – "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[25].

(3) Computer Network Influence (CNI) – "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[26].

The Iranian cyber-attacks in Albania consisted of the three known categories:

[21] D. Antoniuk, *Albanian Parliament, Telecom Company Hit by Cyberattacks,* Recorded Future News, 27 December 2023. https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks accessed 19 October 2024; 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.
[22] The National Authority for Cyber Security (AKSK), *Deklaratë Zyrtare, 1* February 2024 https://aksk.gov.al/deklarate-zyrtare-5/ accessed 19 October 2024. D. 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.
[23] National Institute of Standards and Technology (NIST), *Computer Network Operations* (CNO), https://csrc.nist.gov/glossary/term/computer_network_operations accessed 12 October 2024.
[24] National Institute of Standards and Technology (NIST), *Computer Network Attack* (CNA), https://csrc.nist.gov/glossary/term/computer_network_attack accessed 12 October 2024.
[25] ibidem
[26] ibidem

The Iranian cyber-attacks in Albania included **CNE** activities of ransomware attacks[27], deletion of national data[28], and **CNA** activities of leaks and publication of personal data of thousands of Albanians[29], including Albanian government data and details of emails from the Prime Minister and Ministry of Foreign Affairs[30].

Mandiant researchers defined the versatile activities of this Iranian cyber actor as "a formidable threat actor that likely supports various objectives ranging from espionage to network attack operation"[31] that maintains an arsenal of passive backdoors and sophisticated techniques to avoid standard monitoring methods, obtain footholds into victim networks, and set up long-term access without attracting attention.

CNI – A channel of Iranian soft power is propaganda to monitor and expand its public diplomacy, among others, by publishing Albanian-language news items on an Iranian state-sponsored media outlet. An analysis by the Balkan Investigative Reporting Network in Albania sampled 715 articles published by Iran's Pars Today News Agency in Albanian from 27 June to 26 September 2022 to reveal several thematic biases in the news narratives to "shape public perceptions in accordance with its geopolitical interests and ideology"[32]. In addition, the Iranian Sahar TV channel operates in several languages, including Albanian, and addresses the Balkans in a dedicated section of the website[33]. Moreover, researchers claim that besides propaganda, Iran is involved in the dissemination of fake news against the Iranian opposition group Mojahedin-e Khalq

[27] L. Jenkins at al., *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.
[28] ClearSky Security, *Wiper Attack on Albania by Iranian APT,* 2024. https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf accessed 7 September 2024.
[29] Albanian Daily News, *Homeland Justice Published the Detailed Data of Albanians,* 23 June 2024. https://albaniandailynews.com/news/homeland-justice-published-the-detailed-data-of-albanians accessed 13 October 2024.
[30] 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.
[31] S. Shulman et al., *UNC1860 and the Temple of Oats: Iran's Hidden Hand in Middle Eastern Networks,* Google Cloud Blog, 20 September 2024. https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks accessed 12 October 2024.
[32] B. Bino, B. Likmeta, *Iran's Propaganda in Albanian Language,* Balkan Investigative Reporting Network in Albania Tirana, 2023. https://birn.eu.com/wp-content/uploads/2023/07/Media-Analysis_Irans-Propaganda-in-Albanian-Language.pdf accessed 19 October 2024.
[33] Sahar, *SAHAR Balkans,* https://balkan.sahartv.ir/ accessed 27 October 2024.

Organization (MEK) and its attempt to influence the debate about Iran in the Western Balkan, a region that was "among the most vulnerable to the spread of fake news" and therefore "an easier target for (Iranian) disinformation campaigns"[34].

Suspected actors – Various statements and reports indicate that more than one cyber actor has conducted cyber-attacks in Albania. One of them, "Homeland Justice"[35], took credit for the cyber-attacks in Albania conducted from July 2022.

In his message from 7 September 2022, Albania's Prime Minister 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"[36]. 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"[37]. Microsoft researchers assessed "with high confidence that multiple Iranian actors participated in this attack—with different actors responsible for distinct phases"[38].

The Iranian cyber actors are known by different names given by various cybersecurity vendors and researchers and have been active since at least 2014, targeting regional allies and enemies alike (Saudi Arabia, Israel, the United Arab Emirates, Iraq, Jordan, Lebanon, Kuwait, Qatar, Albania, the U.S. and Turkey) or affiliated organisations in the telecommunications, government, defence, oil, chemical manufacturing, and financial services, for espionage and intelligence gathering, and destruction, on behalf of the

---

[34] A. Rrustemi et al., *Geopolitical Influences of External Powers in the Western Balkans,* HCSS Security, Report, 2021. https://hcss.nl/wp-content/uploads/2021/01/Geopolitical-Influences-of-External-Powers-in-the-Western-Balkans_0.pdf accessed 27 October 2024.
[35] AJ. Vicens, *Albania Cuts Diplomatic Ties with Iran after July Cyberattack,* CyberScoop, 7 September 2022. https://cyberscoop.com/albanian-cyberattack-diplomatic-iran/ accessed 13 October 2024.
[36] 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.
[37] Op. cit. (n. 27)
[38] Op. cit. (n. 19).

Iranian government based on infrastructure details that contain references to Iran and is linked to Iran's Ministry of Intelligence and Security (MOIS)[39].

However, Gentian Progni, an Albanian researcher, believes that "Iran was not acting alone", suggesting a collaboration between Russia and Iran in the cyber-attacks in Albania. He mentions that (1) the cyber actors operated from Russian territory. (2) The leaked information was disseminated from a Russian website, justicehomeland.ru (3), and through Telegram channels, which were also used to spread pro-Russian propaganda. (4) Montenegro, Bulgaria, Kosovo and North Macedonia were hit by cyber-attacks by Russian-speaking cyber groups, and during the same period, Albania was attacked. (5) The claim that "the range of the attacks were too big"[40]. (6) The ongoing cyber partnership between Russia and Iran, including a cyber-defence cooperation diplomacy agreement from June 2015 on the "exchange of intelligence, interaction against threats and joint defense"[41], and the January 2021 cyber agreement between the two countries[42], which stipulates broad cybersecurity cooperation, including "coordination of actions, exchange of technologies, training of specialists"[43]. Miad Nakhvali, an Iranian researcher, emphasises the importance of this agreement, which "signals a deeper level of cooperation between the two countries at all administrative levels in the areas of cybersecurity, technological transfer and joint training"[44].

Motivation – Iran's interest in the Western Balkans, the "Eastern world in the West", reflects the region's growing strategic significance to Iran and a potential "base for future

---

[39] R. Lemos, *As Geopolitical Tensions Mount, Iran's Cyber Operations Grow,* DarkReading, 18 September 2024. https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow accessed 11 October 2024.
[40] A. Oghanna, *How Albania Became a Target for Cyberattacks,* FP Dispatch, 25 March 2023. https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/#selection-1123.0-1123.44 accessed 19 October 2024.
[41] Tasnim News Agency, *Iran, Russia Agree on Cyber-Defense Cooperation: Official,* 13 June 2015. https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defense-cooperation-official accessed 20 October 2024.
[42] TASS, *Russia, Iran Sign Agreement on Cyber Security Cooperation,* 26 January 2021. https://tass.com/politics/1248963 accessed 20 October 2024.
[43] Izvestia, *MFA Reveals Details of Iran-Russia Agreement on Information Security,* 26 January 2021. https://iz.ru/1116475/2021-01-26/mid-raskryl-detali-soglasheniia-irana-i-rossii-ob-informatcionnoi-bezopasnosti accessed 20 October 2024.
[44] Op. cit. (n. 40).

proxy conflicts between Iran and the West"[45]. Iran wants to expand its influence, spread the Islamic Revolution, and develop economic and bilateral relations based on religious, ideological, and geopolitical factors. In this regard, Iran is engaged in various activities, low to medium, through overt political and economic interactions, mainly covert hybrid warfare techniques, including disinformation and cyber-attack campaigns.

The early stage of Iran's involvement in the region was during the Bosnia's war for independence from Yugoslavia in the 1990s, by sending arms and volunteer troops to support the Bosnian Muslim leader Alija Izetbegovic, who had established ties with Iran after the Islamic Revolution.

Future proxy conflicts may used for political purposes. They may translate into a long-term security impact by undermining current regimes and provoking anti-Western and subversive religious and ideologic sentiments. Indeed, Iran has demonstrated increased cultural and religious activities in the Western Balkans due to the similarities in culture, religion, and discourse. Persian was popular in some areas of the Balkans in ancient times, and over 1,700 Persian words are still used in the Bosnian language[46].

Despite the low level of Iranian political interactions and influence in the Western Balkans, due to what Iran perceives as a pro-U.S. Albania stand, mainly against Iranian interests, Iran "now has a direct interest in this region", and Albania is considered a "frontline country in Iran's fight against terrorism"[47]. In 2013, Albania agreed to the U.S. request to host some 3,000 members of the exiled MEK group, which Iran considers a terrorist organisation compared to ISIS[48], allowing them to set up a camp ("Ashraf 3") outside Tirana[49].

---

[45] Op. cit. (n. 32).
[46] IBNA News Agency, *Over 1,700 Persian Words Used in Bosnian Language: Expert,* 24 December 2016. https://web.archive.org/web/20201108112639/https://www.ibna.ir/en/naghli/243605/over-1-700-persian-words-used-in-bosnian-language-expert accessed 26 October 2024.
[47] Nejat Society, *Mojahedin Khalq Terrorist Training Camp in Albania Impacts Whole Balkan Region,* 10 January 2018. https://www.nejatngo.org/en/posts/7862 accessed 28 October 2024.
[48] Nejat Society, *Mojahedin Khalq Supports Daesh, Plans Terrorist Training Camp in Albania,* 25 June 2015. https://www.nejatngo.org/en/posts/6128 accessed 28 October 2024.
[49] P. Dockins, *US Praises Albania for MEK Resettlement,* Voice of America (VOA), 14 February 2016. https://www.voanews.com/a/us-albania/3190311.html accessed 13 October 2024.

The Iranian retaliation was allegedly in both dimensions: physical and cyber-attacks and propaganda.

In October 2019, the Albanian Police announced it foiled several planned attacks during 2018 against MEK members in Albania by "an active cell of the foreign operations unit of the Iranian QUDS forces"[50].

Among their activities, the MEK conducted, beginning in 2016, an annual "Free Iran" conference. The 2002 conference was planned for 23-24 July 2022[51] but was postponed by the organisers "upon recommendations by the Albanian government, for security reasons, and due to terrorist threats and conspiracies"[52]. Indeed, the U.S. Embassy in Albania issued a security alert to U.S. citizens in Albania, stating that "The U.S. government is aware of a potential threat targeting the Free Iran World Summit to be held near Durres, Albania on July 23-24, 2022"[53].

The Iranian motivation and role in the 15 July 2022 cyber-attacks on Albania may be found in an open letter from 23 July to the President of Albania, Ilir Meta, issued by the two of a Pro-Iran and anti-MEK organisation called the Association for the Support of Iranians Living in Albania (ASILA), wondering whether "Albania has entered into a cyber and military conflict with the Islamic Republic of Iran"[54].

After the assassination of Iranian General Qassem Soleimani by a U.S. drone on 3 January 2020, Albania welcomed the assassination. It immediately expelled two Iranian

---

[50] op. cit. (n. 18).

[51] Iran Freedom, *We Can and We Must Free Iran, Take Action: Free Iran World Summit 2022,* 22 July 2022. https://iranfreedom.org/en/news/2022/07/we-can-and-we-must-free-iran-take-action-free-iran-world-summit-2022/35290/ accessed 13 October 2024. National Council of Resistance of Iran (NCRI), Free Iran World Summit 2022. https://www.ncr-iran.org/en/news/free-iran-world-summit/free-iran-2022-world-summit/ accessed 13 October 2024.

[52] Iran Freedom, *Iran NCRI: Postponement of the Free Iran World Summit at Ashraf 3,* 23 July 2022. https://iranfreedom.org/en/free-iran-2022/2022/07/iran-ncri-postponement-of-the-free-iran-world-summit-at-ashraf-3/35303/ accessed 13 October 2024. National Council of Resistance of Iran (NCRI), Postponement of the Free Iran World Summit at Ashraf 3, 22 July 2022. https://www.ncr-iran.org/en/ncri-statements/postponement-of-the-free-iran-world-summit-at-ashraf-3/ accessed 13 October 2024.

[53] U.S. Embassy in Albania, *Security Alert – Threat Targeting the Free Iran World Summit (July 21, 2022)*, 23 January 2023. https://al.usembassy.gov/security-alert-threat-targeting-the-free-iran-world-summit-july-21-2022/ accessed 13 October 2024.

[54] O. Jazexhi, G. Thanasi, *Letter to Albania Gov. Concerning the Cyber Attacks against Albania and Iran*, Niejat Society, Albania Media and blogs, 23 July 2022 https://archive.vn/N8yZN#selection-597.0-606.0 accessed 28 October 2024.

diplomats for "engaging in activities deemed unacceptable for diplomats". Iran's supreme leader, Ali Khamenei, referred to that affair by saying, "There is a small but evil European country in which Americans and traitors against Iran got together to conspire against the Islamic Republic"[55].

Albania, a NATO member since 2009, stands on the side of the U.S. as a close ally. In early July 2022, the U.S. Special Operations Command said on social media that it "made the decision to locate a forward-based Special Operations Forces (SOF) headquarters, on a rotational basis, in Albania!" which Albania's prime minister defined as "fantastic news" adding that "It is an expression of a very high credibility and a very close cooperation[56].

Microsoft research indicates that the selected targets and the messaging of the cyber attacker indicate Iran used the cyber-attacks in Albania as retaliation for previous[57] cyber operations of an Iranian hacktivist group, "Uprising till Overthrow", that hacked several Iranian government websites in July 2022 and leaked sensitive official documents[58]. The September 2022 cyber-attacks came several days after Albania cut diplomatic relations with Iran over July 2022 cyber-attacks[59].

Therefore, Iran's motivation to launch the cyber-attacks against Albania lay on strategic, political and ideological motives.

Targets – The Iranian cyber-attacks targeted various Albanian organisations and governmental institutions aiming to paralyse essential infrastructure in Albania, including telecom (One.al, EagleMobile.al), transportation (Albanian airlines), law enforcement (Albanian police force's Total Information Management System (TIMS)[60], a system that the

---

[55] A. Ruci, L. Arapi, *Iran Lashes out against Albania after Soleimani Killing,* Deutsche Welle, 21 January 2020. https://www.dw.com/en/iran-lashes-out-against-albania-after-soleimani-killing/a-52102170 accessed 19 October 2024.
[56] Deutsche Welle, *US Opens Special Forces Base in Albania,* 1 July 2022. https://www.dw.com/en/us-constructs-new-special-forces-regional-base-in-albania/a-60361419 accessed 13 October 2024.
[57] Op. cit. (n. 20)
[58] Iran International, *Hacktivist Group Targets Iran's Government Organization,* 3 July 2022. https://www.iranintl.com/en/202207032504 accessed 20 October 2024.
[59] AJ. Vicens, *Albania Says Iranian Hackers Hit the Country with Another Cyberattack,* Cyberscoop, 12 September 2022. https://cyberscoop.com/iranian-cyberattack-albania-homeland-justice/ accessed 13 October 2024.
[60] K. Kote, *TIMS Functional Quite Soon, Interior Ministry Vows,* Albanian Daily News, 10 September 2022. https://albaniandailynews.com/news/tims-functional-quite-soon-interior-ministry-vows accessed 13 October 2024.

U.S. government helped Albania to deploy in 2007) and governmental sectors (the Albanian government portal, Albanian Institute of Statistics (INSTAT), National Electronic Documentation, Cyber Security Institution (AKCESK))[61]. Implications – 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[62].

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"[63].

Discussion

This study aims to portray Iran's cyber-attacks on Albania during 2021-2024, including the different waves of the cyber-attacks, the methods of operations, suspected actors, motivations, and targets. In addition, the study analyses the implications of those cyber-attacks and their mitigation, including at the local, bilateral, and international levels.

The findings enable answering the different research questions:

(1) During the waves of cyber-attacks attributed by various sources to Iran, three types of cyber-attack tactics were conducted:
   a. Computer network Exploitation (CNE) – **Intelligence Gathering** – the first stage of the cyber-attacks aimed to gain initial access to the Albanian

[61] T. Ozturk, *Albania Blames Iranian-Backed Group for Cyberattack on Its Statistical Institute,* Anadolu Ajansı, 16 February 2024. https://www.aa.com.tr/en/europe/albania-blames-iranian-backed-group-for-cyberattack-on-its-statistical-institute/3137301 accessed 13 October 2024.
[62] Op. cit. (n. 40)
[63] T. 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.

government's network for 14 months, as well as email harvesting and exfiltration.

b. Computer Network Attack (CNA) – **Destruction** – was the next stage of cyber-attacks, which aimed to destroy data and disrupt Albania's government services.

c. Computer Network Influence (CNI) – **Influence** – The cyber-attacker, "Homeland Justice", not only took credit for the attacks but also published pro-Iran and anti-MEK messages that echoed over the Internet, alongside ongoing propaganda in various Iranian media outlets and in the Albanian language as well.

Those attacks were catastrophic for Albanian public services, hampering the government's ability to govern and affecting every citizen by gathering, deleting and leaking private and even classified information of the general public and civil servants.

Alongside the various research attributes of the cyber-attacks with Iran, the different stages, duration, complexity, and needed resources of the attacks suggest the involvement of a nation-state, cyber-actor, known as Advanced Persistent Threat (APT), with strategic motivations that may serve a state rather than cyber criminals or hacktivists[64].

(2) Iran's aim in the Western Balkans is to spread the Islamic Revolution and develop economic and bilateral relations based on religious, ideological, and geopolitical factors. Despite a modest economic and political Iranian influence in the Western Balkans, the cultural and religious one is more prevalent, based on similarities in culture, religion, and discourse.

Iran considers Albania as an anti-Iran state due to what Iran perceives as a pro-U.S. stand and the host Albania provided to the MEK organisation, which Iran considers a terrorist organisation. Those cyber-attacks demonstrated that Iran is an active player in the Western Balkans and may conduct various cyber operations for strategic purposes

[64] Kaspersky, *What Is an Advanced Persistent Threat (APT)?*, Kaspersky Lab, 2024 https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats accessed 30 October 2024.

against distant rivals. Therefore, such cyber-attacks may be addressed in other Western Balkan countries, even throughout the Balkans, as another tool for Iran to influence and retaliate against its rivals.

The literature covers various aspects of Iran's cyber capabilities, attacks, motivations, targets, and actors but does not address Albania's cyber-attacks. The research of Aleksander Biberaj and others (2022) indicated the need for "improving essentially the cyber infrastructure to avoid in the future such attacks with high social, economic and strategical cost". Their research showed the failures and, therefore, measures of improvements to avoid such cyber-attacks, "In the institution there was not a team for Cyber Security Monitoring the system, so called SOC (Security Operation Center), who controls in the real time all the logins. It was missing as well as the so-called "Identifying Behavior" as well. There was not e separation of active directory, in physic machines and virtual machines, they were altogether. As the administrator had Full Right Privilege, the hacker doesn't need to create a Privilege Escalation Vertical, so he easily took all the right of Admin"[65].

Conclusions

The research stresses the threat posed by external cyber actors to Albania and the potential proliferation in the Balkans:

Strategic Cyber Operations – The Iranian cyberattacks on Albania demonstrate the increasing use of cyber operations for state-sponsored retaliation, geopolitics, and ideological influence. These attacks were not limited to disruption but also included espionage and the dissemination of propaganda, showcasing the multifaceted objectives of Iranian cyber actors.

Vulnerability of Small States – The attacks and their consequences highlight smaller states' vulnerabilities to advanced persistent threats (APTs) and underscore the importance of robust cybersecurity frameworks to mitigate such risks.

Proliferation – The attacks reveal Iran's broader strategic interests in the Western Balkans, including influencing regional politics and countering perceived adversaries.

[65] Op.cit. (n. 15)

This suggests that similar states in the region could become future targets. Ongoing wars and regional conflicts may expand cyber threats to more regions and by various actors. Indeed, experts believe that the Iranian-Israeli confrontation may enter a full-scale war with spillover that could potentially reach the Balkans due to some Iranian influence in Bosnia and Herzegovina and Serbia and the status of Bulgaria as a top destination for tourists and "digital nomads" from Israel. This threat already materialises in the 2012 explosion in Burgas linked by the Bulgarian authorities to the Lebanese Hezbollah[66]. The conclusion of Mandiant researchers should be a red alert for cyber threats posed by Iran to the Balkan, the E.U. and NATO member states: "This activity is a geographic expansion of Iranian disruptive cyber operations, conducted against a NATO member state. It may indicate an increased tolerance of risk when employing disruptive tools against countries perceived to be working against Iranian interests"[67]. Therefore, cyber actors may pose threats outside the geographical region against those not necessarily considered typical targets.

Future Research

The following research will analyse the implications of the Iranian cyber-attacks on Albania and the various local, bilateral, and international mitigation measures taken, including recommendations to minimise the implications of future cyber-attacks in Albania and the Balkans.

[66] G. Cafiero, *Will the Iran-Israel Confrontation Reach the Balkans?*, Amwaj.media, 8 July 2024. https://amwaj.media/article/will-the-iran-israel-confrontation-reach-the-balkans accessed 9 October 2024.
[67] Op. cit. (n. 27)

References

Albanian Daily News, 'Homeland Justice Published the Detailed Data of Albanians' (23 June 2024) <https://albaniandailynews.com/news/homeland-justice-published-the-detailed-data-of-albanians> accessed 13 October 2024

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

American Coalition Against Nuclear Iran, 'History of Iranian Cyber Attacks and Incidents' (2024) <https://www.unitedagainstnucleariran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat.pdf> accessed 1 September 2024

Antoniuk D, 'Albanian Parliament, Telecom Company Hit by Cyberattacks' (*Recorded Future News*, 27 December 2023) <https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks> accessed 19 October 2024

'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

Bahiti R and Josifi J, 'Towards a More Resilient Cyberspace: The Case of Albania' (2015) 32 Information & Security: An International Journal 1 <https://connections-qj.org/system/files/3310_albania.pdf> accessed 1 September 2024

Biberaj A and others, 'Cyber Attack Against E-Albania and Its Social, Economic and Strategic Effects' (2022) 9 The Journal of Corporate Governance, Insurance, and Risk Management (JCGIRM) 341 <https://www.ceeol.com/search/article-detail?id=1161455> accessed 1 September 2024

Bino B and Likmeta B, 'Iran's Propaganda in Albanian Language' (2023) <https://birn.eu.com/wp-content/uploads/2023/07/Media-Analysis_Irans-Propaganda-in-Albanian-Language.pdf> accessed 19 October 2024

Cafiero G, 'Will the Iran-Israel Confrontation Reach the Balkans?' (*Amwaj*, 8 July 2024) <https://amwaj.media/article/will-the-iran-israel-confrontation-reach-the-balkans> accessed 9 October 2024

Ceko E, 'Cyber Security Issues in Albanian Higher Education Institutions Curricula' [2021] CRJ 56 <https://albanica.al/CRJ/article/view/2728> accessed 1 September 2024

ClearSky Security, 'Wiper Attack on Albania by Iranian APT' (2024) <https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf> accessed 7 September 2024

Cybersecurity & Infrastructure Security Agency (CISA), 'Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad' (4 October 2020) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-006a> accessed 2 September 2024

'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

de Souza P, 'Iran's Assault on Our Democracy and a Closer Look at Their Disinformation Tactics' (*LinekdIn*, 28 August 2024) <https://www.linkedin.com/pulse/copy-irans-assault-our-democracy-closer-look-tactics-de-souza-96baf/?trackingId=Vb8cw2ZO%2FflLSLUMKGsTcg%3D%3D> accessed 2 September 2024

Deutsche Welle, 'US Opens Special Forces Base in Albania' (1 July 2022) <https://www.dw.com/en/us-constructs-new-special-forces-regional-base-in-albania/a-60361419> accessed 13 October 2024

Dockins P, 'US Praises Albania for MEK Resettlement' (*Voice of America (VOA)*, 14 February 2016) <https://www.voanews.com/a/us-albania/3190311.html> accessed 13 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

Freilich C, ‘Major Iranian Cyeberattacks Around the World’, *The Iranian Cyber Threat* (Institute for National Security Studies (INSS) 2024) <https://www.inss.org.il/wp-content/uploads/2024/02/Part-3.pdf> accessed 2 September 2024

‘The Iranian Cyber Threat to Israel’, *The Iranian Cyber Threat* (Institute for National Security Studies (INSS) 2024) <https://www.inss.org.il/wp-content/uploads/2024/02/Part-4.pdf> accessed 2 September 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

Halpern M, ‘Iran Flexes Its Power by Transporting Turkey to the Stone Age’ (*Observer*, 22 April 2015) <https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/> accessed 1 September 2024

IBNA News Agency, ‘Over 1,700 Persian Words Used in Bosnian Language: Expert’ (24 December 2016) <https://web.archive.org/web/20201108112639/https://www.ibna.ir/en/naghli/243605/over-1-700-persian-words-used-in-bosnian-language-expert> accessed 26 October 2024

Iran Freedom, ‘We Can and We Must Free Iran, Take Action: Free Iran World Summit 2022’ (22 July 2022) <https://iranfreedom.org/en/news/2022/07/we-can-and-we-must-free-iran-take-action-free-iran-world-summit-2022/35290/> accessed 13 October 2024

‘Iran NCRI: Postponement of the Free Iran World Summit at Ashraf 3’ (23 July 2022) <https://iranfreedom.org/en/free-iran-2022/2022/07/iran-ncri-postponement-of-the-free-iran-world-summit-at-ashraf-3/35303/> accessed 13 October 2024

Iran International, ‘Hacktivist Group Targets Iran’s Government Organization’ (3 July 2022) <https://www.iranintl.com/en/202207032504> accessed 20 October 2024

Izvestia, ‘MFA Reveals Details of Iran-Russia Agreement on Information Security’ (26 January 2021) <https://iz.ru/1116475/2021-01-26/mid-raskryl-detali-soglasheniia-irana-i-rossii-ob-informatcionnoi-bezopasnosti> accessed 20 October 2024

Jazexhi O and Thanasi G, ‘Letter to Albania Gov. Concerning the Cyber Attacks against Albania and Iran’ (23 July 2022) <https://archive.vn/N8yZN#selection-597.0-606.0> accessed 28 October 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

Kaspersky, ‘What Is an Advanced Persistent Threat (APT)?’ <https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats> accessed 30 October 2024

Kote K, ‘TIMS Functional Quite Soon, Interior Ministry Vows’ (*Albanian Daily News*, 10 September 2022) <https://albaniandailynews.com/news/tims-functional-quite-soon-interior-ministry-vows> accessed 13 October 2024

Lemos R, ‘As Geopolitical Tensions Mount, Iran’s Cyber Operations Grow’ (*DarkReading*, 18 September 2024) <https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow> accessed 11 October 2024

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

Moci E, 'Cybersecurity Awareness in Albania ' (2021) 8 European Journal of Social Science Education and Research 1 <https://revistia.com/files/articles/ejser_v8_i3_21/Moci.pdf> accessed 1 September 2024

National Council of Resistance of Iran (NCRI), 'Free Iran World Summit 2022' (2022) <https://www.ncr-iran.org/en/news/free-iran-world-summit/free-iran-2022-world-summit/> accessed 13 October 2024

'Postponement of the Free Iran World Summit at Ashraf 3' (22 July 2022) <https://www.ncr-iran.org/en/ncri-statements/postponement-of-the-free-iran-world-summit-at-ashraf-3/> accessed 13 October 2024

National Institute of Standards and Technology (NIST), 'Computer Network Attack (CNA)' <https://csrc.nist.gov/glossary/term/computer_network_attack> accessed 12 October 2024

'Computer Network Operations (CNO)' <https://csrc.nist.gov/glossary/term/computer_network_operations> accessed 12 October 2024

Nejat Society, 'Mojahedin Khalq Supports Daesh, Plans Terrorist Training Camp in Albania' (25 June 2015) <https://www.nejatngo.org/en/posts/6128> accessed 28 October 2024

'Mojahedin Khalq Terrorist Training Camp in Albania Impacts Whole Balkan Region' (10 January 2018) <https://www.nejatngo.org/en/posts/7862> accessed 28 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

Ozturk T, 'Albania Blames Iranian-Backed Group for Cyberattack on Its Statistical Institute' (*Anadolu Ajansı*, 16 February 2024) <https://www.aa.com.tr/en/europe/albania-blames-iranian-backed-group-for-cyberattack-on-its-statistical-institute/3137301> accessed 13 October 2024

Pagliery J, 'The inside Story of the Biggest Hack in History' (*CNN Business*, 5 August 2015) <https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html> accessed 1 September 2024

Rrustemi A and others, 'Geopolitical Influences of External Powers in the Western Balkans ' (2021) <https://hcss.nl/wp-content/uploads/2021/01/Geopolitical-Influences-of-External-Powers-in-the-Western-Balkans_0.pdf> accessed 27 October 2024

Ruci A and Arapi L, 'Iran Lashes out against Albania after Soleimani Killing' (21 January 2020) <https://www.dw.com/en/iran-lashes-out-against-albania-after-soleimani-killing/a-52102170> accessed 19 October 2024

Sahar, 'SAHAR Balkans' <https://balkan.sahartv.ir/> accessed 27 October 2024

Sciacovelli AL, 'Taking Cyberattacks Seriously: The (Likely) Albanian Cyber Aggression and the Iranian Responsibility.' (2023) 1 WORKING PAPER OSSERVATORIO SULLE ATTIVITÀ DELLE ORGANIZZAZIONI INTERNAZIONALI E SOVRANAZIONALI, UNIVERSALI E REGIONALI, SUI TEMI DI INTERESSE DELLA POLITICA ESTERA ITALIANA <https://ricerca.uniba.it/handle/11586/438480> accessed 1 September 2024

Semini L, 'Albania Cuts Diplomatic Ties with Iran over July Cyberattack' (*AP News*, 7 September 2022) <https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a> accessed 10 October 2024

'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

Shkembi A, Shtupi I and Qafa A, 'The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation' (2016) 5 Academic Journal of Interdisciplinary Studies 1 <https://pdfs.semanticscholar.org/cd34/8906b7b5170601c731763dde70a27ed159f4.pdf> accessed 1 September 2024

Shulman S and others, ‘UNC1860 and the Temple of Oats: Iran’s Hidden Hand in Middle Eastern Networks’ (20 September 2024) <https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks> accessed 12 October 2024

Starks T, ‘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

Tasnim News Agency, ‘Iran, Russia Agree on Cyber-Defense Cooperation: Official’ (13 June 2015) <https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defense-cooperation-official> accessed 20 October 2024

TASS, ‘Russia, Iran Sign Agreement on Cyber Security Cooperation - Russian Politics & Diplomacy’ (26 January 2021) <https://tass.com/politics/1248963> accessed 20 October 2024

The National Authority for Cyber Security (AKSK), ‘Deklaratë Zyrtare’ (1 February 2024) <https://aksk.gov.al/deklarate-zyrtare-5/> accessed 19 October 2024

The Telegraph, ‘Iran Blamed for Cyberattack on Parliament That Hit Dozens of MPs, Including Theresa May’ (14 October 2017) <https://web.archive.org/web/20171206135812/https://www.msn.com/en-gb/news/uknews/iran-blamed-for-cyberattack-on-parliament-that-hit-dozens-of-mps-including-theresa-may/ar-AAtpPag?li=AAmiR2Z&ocid=spartanntp> accessed 2 September 2024

Tiri E and Aliaj E, ‘Cyber-Security Regulation in Albania’ (2023) 12 Perspectives of Law and Public Administration 275 <https://www.ceeol.com/search/article-detail?id=1221788> accessed 1 September 2024

U.S. Embassy in Albania, ‘Security Alert – Threat Targeting the Free Iran World Summit (July 21, 2022)’ (23 January 2023) <https://al.usembassy.gov/security-alert-threat-targeting-the-free-iran-world-summit-july-21-2022/> accessed 13 October 2024

Vicens A, ‘Albania Cuts Diplomatic Ties with Iran after July Cyberattack’ (*CyberScoop*, 7 September 2022) <https://cyberscoop.com/albanian-cyberattack-diplomatic-iran/> accessed 13 October 2024

‘Albania Says Iranian Hackers Hit the Country with Another Cyberattack’ (12 September 2022) <https://cyberscoop.com/iranian-cyberattack-albania-homeland-justice/> accessed 13 October 2024

Vostoupal J, ‘Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial’ (2024) 54 Computer Law & Security Review 106008 <https://www.sciencedirect.com/science/article/abs/pii/S026736492400075X> accessed 1 September 2024

Zhilla F and Lamallari B, ‘Organised Crime Threat Assesment in Albania’ (2015) <https://globalinitiative.net/wp-content/uploads/2018/02/Threat_Assessment_of_Albanian_Organised.pdf> accessed 1 September 2024