PUBLIC ATTRIBUTION OF CYBER INTRUSIONS BY SMALL STATES: A COMPARATIVE STUDY OF THE WESTERN BALKANS (2022-2023)

Aleksandar BOGIĆEVIĆ, PhD Candidate
Researcher, Strategic Research Institute, University of Defence, Belgrade, Serbia
aleksandar.bogicevic@mod.gov.rs, ORCID: 0009-0006-7450-5193

***Abstract**: Cyber deterrence presents unique challenges for small states operating under structural and geopolitical constraints. Lacking extensive retaliatory or cross-domain capabilities, these states often elevate the public attribution of cyber intrusions into a key instrument of strategic signalling. This paper examines the responses of Serbia, Albania, and Montenegro to major cyber incidents during 2022 and 2023, asking: under what political and strategic conditions do small states publicly attribute cyberattacks? Using a comparative case study approach, the research analyses official statements, policy documents, and public communication to assess how foreign policy orientation and institutional capacity shape attribution practices. The paper argues that public attribution in small states is not merely a technical determination but a politically embedded act of signalling within asymmetric security environments. The findings suggest that the decision to attribute is more closely aligned with international security frameworks and internal political considerations than with technical certainty alone.*

***Keywords**: public attribution; small states; Western Balkan; cyberattack; signalling.*

Introduction

In recent years, the cyber domain has become one of the most significant, but also growing, sources of threat for both states and societies, as digital transformation accelerates and societies become increasingly dependent on advanced technologies. Due to the absence of clear geographical boundaries, cyberattacks can be launched from virtually anywhere and directed at a wide range of targets for different purposes, including financial gain through ransomware, theft of sensitive data, influence operations, or disruption of critical infrastructure. At the same time, the anonymity inherent to cyberspace significantly complicates the process of identifying those responsible for such attacks (Libicki 2009, 41-52), regardless of whether they are state actors, criminal organisations, or proxies operating with varying degrees of state support. As the source of cyberattacks is unclear, attribution is especially important for defending states, as it allows the defender to decide how to respond politically and strategically.

Because cyberspace tends to favour aggressive behaviour and attackers, the development of credible deterrence has become one of the most important parts of state cyber strategies. The majority of existing academic work on this topic has focused on well-known, high-profile incidents and on how technologically developed states have dealt with them – StuxNet being perhaps the most cited example (Farwell and Rohozinski 2011; Lindsay 2013), alongside cases such as NotPetya (Krasznay 2020). Comparatively little attention has been paid to small states, and in particular to those located in the Western Balkans, which, in the context of this paper, are defined as states that possess limited material and cyber capabilities. Such states are generally more exposed to asymmetric threats than major powers, and when their capacity to respond through cyber or other means is limited, the act of publicly naming an attacker becomes one of the very few instruments of strategic action that remain available to them. Public attribution, as the term is used in this paper, refers to the official and explicit identification of a responsible actor by state authorities (Eichensehr 2020, 527). This is not simply a technical decision – it is a political one, and it requires governments to carefully weigh whether publicly disclosing who carried out an attack serves their national interests or whether it creates more problems than it solves.

This paper examines cyberattacks on Albania, Montenegro, and Serbia during 2022 and 2023 and their responses by analysing official statements and public discourse. The central research question is concerned with identifying the conditions under which small states decide

to engage in public attribution. The contribution of this study to the existing literature is twofold: first, it shifts the analytical focus away from major cyber powers and toward smaller and less studied states; and second, it approaches public attribution not as a technical procedure but as a decision that is shaped by political considerations. The findings of the analysis suggest that decisions to publicly attribute a cyberattack are determined more by a country's international alignment and domestic political dynamics than by what the available technical evidence actually indicates. The study also shows that the three Western Balkan states have developed quite different approaches to attribution, and that these differences can be explained by their distinct foreign policy orientations and internal political circumstances.

1. Determinants of public attribution in cyberspace

The attribution of cyber-attacks is central to academic debates on cyber deterrence (Egloff 2020, 1). Identifying the perpetrator is both a technical requirement and a key precursor to an appropriate political and strategic response by the victim. The types of actors in cyberspace have evolved alongside technological advancements, shifting from loosely organised criminal groups and hacktivists of the early 2000s, who conducted small-scale attacks with low impact, to highly professionalised formations with links to states (Cavelty 2012, 112) capable of performing highly destructive cyber operations. Numerous state proxies and intelligence units now pose as independent hacker groups, such as hacktivist group KillNet, or ATP 28, which is tied directly to Russia's military intelligence (GRU) (Radware n.d; NSA and FBI 2020). The central issue in such an uncertain context is less about the identity of the perpetrator and more about the conditions under which states choose to publicly attribute responsibility and leverage that identification for political purposes. Consequently, attribution has moved from a matter of simple identification by technical means to one of political judgment and strategic messaging.

The technically demanding process of identifying actors, described by Egloff as "sense-making" (2020, 2), lacks political significance unless officials interpret the event and base their actions on that interpretation – "meaning-making" (2020, 2). Technical attribution involves forensic analysis in the process of solving cases of cyberattacks; in contrast, public attribution is an act of political actors in which the officials formally identify the attacker to both domestic and international audiences. Political leaders are often less concerned with the perpetrator's identity than with the actions to take following attribution and the potential effects of those actions (Egloff 2020, 2). Attribution, therefore, functions as strategic communication, enabling states to signal intent, assign blame, and manage perceptions. Attribution is shaped by states to serve their political and strategic objectives, or, as Rid and Buchanan pointed out, "it is what states make of it" (2015, 7). The decision to move to public attribution is always political, not merely technical, and is central to strategic signalling in cyberspace.

The process of public attribution can be operationalised at various levels, from identifying the digital infrastructure used in the attack and the immediate perpetrator to pinpointing the entity that issued the operational order (Lin 2016, 8). Attributing cyber-attacks to sovereign governments can generate significant international and domestic pressure to undertake retaliatory measures (Eichensehr 2020, 550), making public attribution a key component of deterrence through cost imposition. Within this framework, possible responses include legal actions such as filing charges, economic measures such as sanctions, and public shaming of the perpetrator (ibid, 532). Some scholars argue that deterrence in cyberspace may also involve the threat of cross-domain measures like kinetic responses (Farrell and Glaser 2017, 10), thereby enhancing the credibility of the threat. However, these solutions are reserved for a small number of states with advanced military, economic, and political resources. On the other side, smaller states, with limited resources, have reduced capacity for credible retribution, which means that public attribution is often one of the few available instruments of strategic action.

The political dimension of public attribution is inherently multi-layered, involving the balancing of resources, foreign policy relations and domestic political situation that, together, shape the decision to publicly disclose an attacker's identity. States do not solely seek to establish responsibility during the public attribution process; they also aim to understand the opponent and his intentions, and anticipate the reactions of key international actors (Egloff 2020, 7). Public attribution thus serves as an instrument for positioning in foreign policy, particularly in relations with regional actors, allies and potential adversaries. Simultaneously, it fulfils a significant domestic political function by shaping threat perceptions, mobilising political support, or managing crisis narratives (Schulzske, 2018). This dual logic means that the decision to make a public attribution results from balancing external actors with domestic political imperatives. For small states, balancing all actors and pressures can be especially challenging, as possible mistakes during public attributions can lead to disproportionate foreign policy consequences.

Public attribution can be understood as a strategic signalling which results from the interaction of international and domestic factors. While technical attribution establishes the basis for identifying a potential attacker, deciding what to do with that information depends on evaluating the possible advantages and disadvantages for domestic and foreign policy. Thus, public attribution results from a political assessment that balances foreign policy pressures, allied expectations, and domestic imperatives. For small states with limited capacity for retribution or punishment of the attacker, public attribution becomes especially significant as a means of signalling and managing perceptions. Therefore, analysing public attribution requires attention to the conditions under which states choose to publicly identify the attacker, with foreign policy coordination and domestic political context serving as key determinants.

2. Cyber incidents and attribution dilemmas in small states: evidence from the western balkans

With the intensification of geopolitical rivalry between great powers, the space for neutral or small states is shrinking. The polarisation of international order between the USA and its allies on one side and challengers of the post-Cold War order on the other side creates pressure on smaller states to position themselves, which often manifests itself in the form of hybrid actions of great powers (Bogićević 2025, 225). As small states located in the sensitive region of the Western Balkans, Albania, Montenegro, and Serbia can serve as relevant case studies: they have limited material capabilities to face sophisticated foreign threats on their own. Their reactions to significant cyber incidents during 2022-2023 reveal not only the cybersecurity challenges facing small states but also the political dilemmas associated with public attribution of attacks amid rising foreign policy pressures.

Montenegro illustrates the challenges of public attribution, where technical, political, and international factors intersect. In August 2022, the country experienced a large-scale cyberattack that shut down multiple state agencies and institutions like the Assembly, judicial bodies, and public enterprises (OCCRP 2022). The group responsible for the attack was the Cuba Ransomware group, known for operating from the Russian-speaking world and for targeting critical infrastructure in Ukraine and Western countries (Radio Slobodna Evropa 2023). The relationship between this hacker group and Russian state structures remains unclear: while US security agencies classify the group as a criminal organisation with financial motives (CISA 2022b), some cybersecurity companies classify it as a pro-Russian proxy (TechCrunch 2023). Montenegro’s explicit support for Ukraine, condemnation of Russian aggression, previous history of Russian interference in Montenegro's internal affairs (Bojicic-Dzelilovic 2026, 6) and possible perception of 'weak link' in NATO’s defence further heightened its vulnerability. The vote of no confidence in August 2022 left Montenegro and its administration even more vulnerable to possible hybrid threats.

In the immediate aftermath of the cyberattack, Montenegrin officials approached public attribution from two diametrically opposed positions. While government representatives, led by Prime Minister Dritan Abazovic, maintained that the background to the attack and possible perpetrators could not be further determined (Vijesti, 2022a), the National Security Agency (org. Agencija za nacionalnu bezbednost – ANB) openly accused Russia of being the instigator of this cyberattack (Vijesti, 2022b). Additional confusion was created by the Prime Minister's subsequent statement, which rejected intelligence reports that it was a politically motivated attack, describing them as "politically motivated and premature", while insisting that the background to the attack was financial (RTCG 2022). Despite assurances from the Ministry of Defence that the government would provide a timely and definitive identification of the perpetrators (Vijesti 2022c), no such formal conclusion was ever released (Vijesti 2025). Instead, various officials continued to issue indirect accusations against Russia, while the official state narrative remained unresolved (Vijesti 2022c). The identification process eventually involved international actors, most notably the United States and France. However, Montenegrin officials stated that the final technical reports presented to the Government in early 2023 did not provide a conclusive answer, leaving the issue unresolved (Borba 2023).

Montenegro's fragmented and inconsistent public attribution process stems mainly from internal political constraints and weak institutional protocols for responding to cyber threats. Political instability and a leadership vacuum made it hard to develop a unified, strategic state response. Tensions between political leaders and security agencies led to inconsistent narratives about the attack's origins, which directly undermined the credibility of the government's narrative. In this environment, focusing technical attribution on the Cuba Ransomware group became a tool for plausible deniability – this allows decision-makers to de-escalate and avoid a direct confrontation with Russia, which could lead to further escalation of attacks. However, the lack of open condemnation of Russia drew sharp criticism from opposition parties and further damaged public trust in the government's foreign policy (Danas 2022).

The case of Albania, while less complex in terms of perpetrator identification, illustrates the unique challenges small states face in asymmetric cyber conflict, even after successful public attribution. In July 2022, just a month before the cyberattack against Montenegro, Tirana experienced a sophisticated cyberattack attributed to the hacking group Homeland Justice, a proxy actor directly associated with the Iranian state apparatus (CISA 2022a). The operation primarily aimed to disable state administrative services and exfiltrate sensitive government data (Oghanna 2023). Although Albanian officials issued statements explicitly identifying Tehran as the aggressor, the cyber offensive persisted (Reuters 2022). The continued degradation of digital infrastructure led Tirana to take a precedent-setting action in international relations in September 2022: the severing of diplomatic relations with Iran (Albanian Government Council of Ministers 2022). This marked the first instance in which two states implemented such a measure as a direct consequence of a cyber-attack. International actors, including the United States and the United Kingdom, supported the Albanian claims. After an investigation by the UK's National Cyber Security Centre, Secretary James Cleverly publicly condemned the Iranian actors (Foreign, Commonwealth and Development Office 2022), and the US Department of the Treasury imposed sanctions on Iran's Ministry of Intelligence and Security in response to the attack (Al Jazeera 2022).

Despite diplomatic isolation, Iran-sponsored cyber activities persisted and intensified in subsequent months. The next campaign targeted the banking sector, focusing on the online services (Balkan Insight 2023) and the security apparatus (Higgins 2023). Other significant incidents included the leak of sensitive data of individuals connected to Albania's intelligence services, as well as a breach of the customs system that destroyed databases of citizens who had entered or left the country, significantly disrupting their operations (Vicens 2022).

The Albanian experience diverges significantly from the Montenegrin case in several key aspects. Primarily, strong institutional unity characterised the process of public attribution in Tirana. While divergent narratives from the executive and security sector fragmented the

Montenegrin response, the Albanian government under Prime Minister Edi Rama maintained a consistent, unified message. In contrast to Montenegro, where political instability and domestic factors hampered a direct condemnation of Russia, Albanian political actors reached a consensus on Tehran's hostile actions, facilitating their attribution. However, the continuous nature of the attacks shows that public attribution does not guarantee deterrence against state-sponsored actors. Although the diplomatic rupture failed to halt these offensives, Albania's clear and unified position allowed the country to mobilise significant international support and attract the attention of more powerful allies with developed cyber deterrence and retribution mechanisms.

The case of cyber-attacks targeting Serbia's critical infrastructure differs significantly from those in Montenegro and Albania, primarily due to Serbia's distinct geopolitical position and doctrinal defence posture. While NATO membership and alignment with collective security systems have played a central role in deterrence and mitigation for Albania and Montenegro, Serbia relies on a strategy of military neutrality. This foreign policy stance, especially amid the war in Ukraine, combines formal support for territorial integrity with a refusal to impose sanctions on the Russian Federation. As a result, Serbia operates within a complex strategic environment where both Western and pro-Russian actors may view it as a relevant target. Although attacks on Serbian institutions were less disruptive than the systemic paralysis experienced by neighbouring countries, these incidents remain highly significant for analysing Serbia's national approach to public attribution.

The case of *Elektroprivreda Srbije*, the principal state-owned energy supplier, demonstrates the substantial impact of cyber-attacks on critical infrastructure. The company was targeted by a hacker group linked to Qilin (Balkan Insight 2023), which employs a Ransomware-as-a-Service (RaaS) model[1] and is internationally recognised for orchestrating or facilitating sophisticated cyber operations, frequently targeting Western organisations (Group-IB 2023). The involvement of such a group in Serbia is analytically significant, indicating that Serbia may be perceived as a legitimate target within broader geopolitical dynamics. This attack can be contextualized by reports of large-scale Serbian ammunition exports to Ukraine (Reuters 2023), which, although indirect, may have positioned Serbia as a de facto adversary to pro-Russian cyber actors. This perception broadens the range of threat actors beyond those motivated solely by financial gain, thereby blurring the distinction between cybercrime and geopolitically motivated operations.

Unlike Montenegro and Albania, Serbia's response to cyber incidents during 2022–2023 was characterized by notable restraint, particularly in terms of public attribution, despite several significant attacks on critical state infrastructure. For instance, in June 2022, the Republic Geodetic Authority (RGZ) information system was compromised, causing a nationwide shutdown of cadastral services (BIRN 2022). Although the attack significantly disrupted administrative operations and raised concerns about the security of sensitive property data, official communications emphasized that no data had been compromised and that the system had been proactively isolated to prevent further harm (N1 2022). This approach prioritized damage control and institutional resilience over transparency regarding the attack's nature and origin.

A comparable communication strategy was observed in subsequent cyber incidents affecting public enterprises and critical infrastructure, including the energy and postal sectors. Despite expert assessments and media reports indicating possible data exfiltration and broader systemic vulnerabilities (BIRN 2022), Serbian officials consistently refrained from explicitly attributing responsibility to any state or non-state actor. Senior state officials and central institutions did not issue public statements; instead, communication was primarily conducted by representatives of the affected entities, who focused on operational recovery and assurances of system security. In contrast, Albania promptly and unequivocally identified Iran as the

[1] Ransomware-as-a-Service (RaaS) is a business model in which sophisticated groups creates ransomware and lease it to other cybercriminals, charging them a fixed price or a percentage of the ransom successfully collected.

perpetrator, while Montenegro's competing narratives included direct accusations against Russia. Serbian authorities, however, avoided publicly naming any responsible actor.

The lack of public attribution in Serbia should be interpreted not only as a result of technical uncertainty, but as a politically motivated strategy shaped by both external and domestic factors. Externally, refraining from explicit accusations reduces the risk of diplomatic escalation and maintains flexibility in relations with key international actors, particularly given Serbia's balancing position between the West and East (in this case Russia). Domestically, public opinion is influential, as a significant portion of the population views Russia as a vital ally[2], especially among supporters of the incumbent government (BIRODI 2022, 8). In this context, openly attributing a cyberattack to Russian actors could entail considerable political costs. Therefore, strategic ambiguity in attribution functions as an active tool of political management, designed to preserve both external maneuverability and internal legitimacy. However, this approach also diminishes the deterrent effect of public attribution, as the absence of a clearly identified perpetrator limits opportunities for reputational consequences and coordinated international responses.

Strategic considerations reveal that Albania demonstrates how strong institutional cohesion and clear foreign policy alignment facilitate decisive attribution, even under sustained cyber pressure. Montenegro, by contrast, illustrates how internal fragmentation and institutional contestation can result in inconsistent and ultimately inconclusive attribution outcomes. Serbia exemplifies a model of strategic ambiguity, where the deliberate absence of attribution serves as a tool for foreign policy balancing and domestic political management. In this context, attribution is not simply a reactive measure but an instrument of strategic calibration, enabling small states to navigate competing external pressures while maintaining internal stability. These findings indicate that public attribution in small states is best understood as strategic signaling, shaped by geopolitical positioning, domestic political constraints, and the perceived costs of openly assigning responsibility in an increasingly polarized international environment.

Conclusion

Analysis shows that public attribution of cyberattacks in small states is a complex, politically conditioned process that extends well beyond the scope of technical forensics. For states with limited material and cyber capabilities, such as those in the Western Balkans, identifying the perpetrator is not just a search for digital truth, but a key instrument of strategic signalling in asymmetric security environments. As these states often lack the resources for conventional retaliation or cross-domain responses, publicly naming the aggressor serves to mobilise international support, manage domestic threat narratives, and deter by imposing reputational costs on the attacker. The final decision on attribution is the result of a careful balancing act among technical certainty, foreign policy pressures from allies, and potential diplomatic fallout.

The comparative examples of Albania, Montenegro and Serbia illustrate three distinct strategies that directly reflect their geopolitical positions and internal dynamics. Albania has demonstrated a model of decisive attribution, grounded in strong institutional unity and clear alignment with NATO partners, culminating in the unprecedented severing of diplomatic relations with Iran. In contrast, the case of Montenegro reveals how internal political fragmentation and conflicting narratives between the executive and security agencies can lead to inconsistent and unresolved outcomes, where technical attribution (e.g., to the Cuba Ransomware group) is used as a tool for "plausible deniability" to de-escalate relations with great powers such as Russia. Serbia, on the other hand, consistently pursues a model of strategic ambiguity. By avoiding public naming of perpetrators, even in cases of attacks on critical

[2] The results of a public opinion poll conducted in February 2023 by the WFD show that 42% of Serbian citizens believe that Russia should be the primary foreign policy partner, while other actors such as the EU, the USA, and China appear in significantly lower percentages: 26%, 2.6%, and 8%, respectively. For more details on the research, see: WFD. 2023. "Izveštaj sa istraživanja javnog mnjenja: društveno-politički stavovi građana Srbije 2023. godine".

infrastructure such as energy supplier or the land registry, official Belgrade preserves its foreign policy flexibility and avoids the domestic political costs that would arise from directly accusing actors whom a significant portion of the domestic public perceives as allies.

Ultimately, the findings of this paper suggest that for small states, public attribution does not guarantee security nor automatically halt hostile operations, as evidenced by the continuation of Iranian activities against Albania. Nevertheless, it remains an indispensable part of national cyber strategies as it allows a state to interpret an adversary's strategic intent and define its position within global security architectures. As cyberspace continues to evolve as a field of geopolitical rivalry, public attribution of states in the Western Balkans will remain more a matter of political judgement and strategic calibration than of purely technical verification, serving as a mirror of their internal capacities and foreign policy ambitions.

BIBLIOGRAPHY

1. Al Jazeera. „US imposes new sanctions on Iran over Albanian cyberattack". September 9, 2022. https://www.aljazeera.com/news/2022/9/9/us-imposes-new-sanctions-on-iran-over-albanian-cyberattack
2. Albanian Government Council of Ministers. „Video message of Prime Minister Edi Rama, regarding the response of the Albanian government to the cyberattack against the digital infrastructure of the Government of the Republic of Albania". September 7, 2022. https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama-lidhur-me-vendimin-e-qeverise-shqiptare-si-kunderpergjigje-ndaj-aktit-te-sulmit-te-rende-kibernetik-ndaj-infrastruktures-digjitale-te-qeverise-se-republikes-se-s/
3. Balkan Insight. „Battle for Balkan cybersecurity: Threats and implications of biometrics and digital identity". June 30, 2023. https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/
4. Balkan Investigative Reporting Network (BIRN). „Hakeri imali pristup mejlovima zaposlenih u katastru Srbije: Stručnjaci kažu da opasnost još nije prošla". September 21, 2022. https://birn.rs/hakeri-imali-pristup-mejlovima-zaposlenih-u-katastru-srbije-strucnjaci-kazu-da-opasnost-jos-nije-prosla/.
5. BIRODI. 2022. *Public Opinion In Serbia And Media*. BIRODI.
6. BOGIĆEVIĆ, Alekdansar. 2025. "Sajber napadi kao strategijski instrument spoljne politike: Zapadni Balkan u eri hibridnog rata". in *Geostrateška budućnost Balkana.* Blagojević, V. and Subotić M. (eds.). Beograd: IMMP i ISI, 223-245.
7. BOJICIC-DZELILOVIC, Vesna. 2026. "Western Balkans as the Frontline of Russian Hybrid Warfare". *Global Policy*, 1-12.
8. Borba. „Misterija: I dalje se ne zna ko stoji iza sajber napada na infrastrukturu Vlade". March 8, 2023. https://borba.me/misterija-i-dalje-se-ne-zna-ko-stoji-iza-sajber-napada-na-infrastrukturu-vlade/
9. CAVELTY, Myriam Dunn. (2012). „From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse". *International Studies Review*, vol. 15(1), 105-122.
10. Cybersecurity and Infrastructure Security Agency (CISA). „Iranian state actors conduct cyber operations against the Government of Albania". September 23, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.
11. Cybersecurity and Infrastructure Security Agency (CISA). „#StopRansomware: Cuba ransomware". December 01, 2022. https://www.cisa.gov/news-events/alerts/2022/12/01/stopransomware-cuba-ransomware
12. Danas. „Predrag Bošković za Danas: Dritan Abazović više nije relevantan sagovornik ni za jednu međunarodnu adresu, mandat vlade biće okončan za par meseci". October 11, 2022. https://www.danas.rs/svet/region/predrag-boskovic-za-danas-dritan-abazovic-vise-nije-relevantan-sagovornik-ni-za-jednu-medjunarodnu-adresu-mandat-vlade-bice-okoncan-za-par-meseci/.

13. EGLOFF, Florian J. 2020. "Public attribution of cyber intrusions". *Journal of Cybersecurity*, vol. 6, 1-12.
14. EICHENSEHR, Kristen. 2020. „The Law and Politics of Cyberattack Attribution". *UCLA Law Review*, Vol 67 (520). UCLA School of Law, Public Law Research Paper No. 19-36.
15. FARRELL, Henry and GLASER, Charles L. 2017. „The role of effects, saliencies and norms in US Cyberwar doctrine." *Journal of Cybersecurity*, Vol. 3(1), 7-17.
16. FARWELL, James P. and ROHOZINSKI, Rafal. 2011. „Stuxnet and the Future of Cyber War". *Survival, 53*(1), 23-40.
17. Foreign, Commonwealth and Development Office. „UK condemns Iran for reckless cyber attack against Albania". September 7, 2022. https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania.
18. Group-IB. "The Qilin ransomware: Analysis and protection strategies". 15 May, 2023. https://www.group-ib.com/blog/qilin-ransomware/.
19. HIGGINS, Andrew. „A NATO minnow reels from cyberattacks linked to Iran". *The New York Times*. February 25, 2023 https://www.nytimes.com/2023/02/25/world/europe/albania-iran-nato-cyberattacks.html
20. KRASZNAY, Csaba. 2020. „Case Study: The NotPetya Campaign". *Információ-és kiberbiztonság*. Ludovika University of Public Service, 485-499.
21. LIBICKI, C. Martin. 2009. *Cyber Deterrence and Cyberwar*. Santa Monica: RAND Corporation.
22. LIN, Herbert. 2016. „Attribution of Malicious Cyber Incidents: From Soup to Nuts". *Columbia Journal of International Affairs*, 4-57.
23. LINDSAY, John. R. 2013. „Stuxnet and the Limits of Cyber Warfare". *Security Studies*, 22(3), 365-404.
24. N1. „RGZ: Podaci zaštićeni, inspekcija kaže ispravno smo postupili pri sajber napadu". September 16, 2022. https://n1info.rs/biznis/rgz-podaci-zasticeni-inspekcija-kaze-ispravno-smo-postupili-pri-sajber-napadu/
25. National Security Agency (NSA) and Federal Bureau of Investigation (FBI). 2020. *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*. Media Defense.
26. OGHANNA, Ayman. „How Albania became a target for cyberattacks". *Foreign Policy*, 25 March, 2023. https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/
27. Organized Crime and Corruption Reporting Project (OCCRP). „Cyberat-tacks hit Montenegro's state infrastructure". August 30, 2022. https://www.occrp.org/en/news/cyberattacks-hit-montenegros-state-infrastructure
28. Radio Slobodna Evropa. (2023). „FBI predao Crnoj Gori nalaze o sajber napadima u toj zemlji". January 12, 2023. https://www.slobodnaevropa.org/a/istraga-napadi-vlada-sad/32220699.html
29. Radware. (n.d.). „What is Killnet?" *Radware Cyberpedia*. https://www.radware.com/cyberpedia/ddos-attacks/killnet/.
30. Reuters. „Albania cuts Iran ties over cyberattack, U.S. vows further action." September 7, 2022. https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/.
31. Reuters. „Exclusive: Leaked U.S. intel document claims Serbia agreed to arm Ukraine". April 12, 2023. https://www.reuters.com/world/leaked-us-intel-document-claims-serbia-agreed-arm-ukraine-2023-04-12/
32. RID, Thomas and BUCHANAN Ben. 2015. „Attributing Cyber Attacks". *Journal of Strategic Studies*, Vol. 38 (1-2), 4-37.
33. RTCG. „Sajber napadi nijesu politički motivisani". August 26, 2022. https://rtcg.me/vijesti/drustvo/375434/sajber-napadi-nijesu-politicki-motivisani.html.
34. SCHULZSKE, Marcus. 2018. „The politics of attributing blame for cyberattacks and the costs of uncertainty". *Perspectives on Politics*, Vol 16(4), 954-968.
35. TechCrunch. „Cybercriminals who targeted Ukraine are actually Russian government hackers, researchers say". May 15, 2023. https://techcrunch.com/2023/05/15/cybercriminals-who-targeted-ukraine-are-actually-russian-government-hackers-researchers-say/

36. Vicens, Aj. „Albania says Iranian hackers hit the country with another cyberattack.“ *CyberScoop*. September 12, 2022. https://cyberscoop.com/iranian-cyberattack-albania-homeland-justice/.
37. Vijesti. „Abazović: Nekoliko institucija napadnuto, naredne sedmice o nanijetoj šteti”. August 26, 2022. https://www.vijesti.me/vijesti/politika/618947/abazovic-nekoliko-institucija-napadnuto-naredne-sedmice-o-nanijetoj-steti.
38. Vijesti. „Kuba ransomver tvrdi da ima podatke iz Skupštine Crne Gore, povezuju ih sa Rusijom”. August 31, 2022. https://www.vijesti.me/vijesti/619576/kuba-ransomver-tvrdi-da-ima-podatke-iz-skupstine-crne-gore-povezuju-ih-sa-rusijom.
39. Vijesti. „Konjević: Nama je jasno ko bi mogao da ima politički motiv za sajber napad u Crnoj Gori”. September 13, 2022. https://www.vijesti.me/vijesti/politika/621429/konjevic-nama-je-jasno-ko-bi-mogao-da-ima-politicki-motiv-za-sajber-napad-u-crnoj-gori.
40. Vijesti. „Sajber napad nije mnogo ubrzao državu”. December 27, 2025. https://www.vijesti.me/vijesti/drustvo/789395/sajber-napad-nije-mnogo-ubrzao-drzavu.