Tal Pavel

DOI: 10.2478/cmc-2026-0018

VELIKA TEHNOLOŠKA PODJETJA IN KIBERNETSKA ODPORNOST NA BALKANU: PRIMERJALNA ANALIZA KIBERNETSKIH INCIDENTOV LETA 2022

BIG TECH AND CYBER RESILIENCE IN THE BALKANS: A COMPARATIVE ANALYSIS OF CYBER INCIDENTS IN 2022

Povzetek Ta raziskava preučuje vlogo velikih tehnoloških korporacij pri oblikovanju kibernetske odpornosti med pomembnimi kibernetskimi incidenti na Balkanu leta 2022. Študija izvaja primerjalno analizo osmih balkanskih držav (Albanije, Bosne in Hercegovine, Hrvaške, Kosova, Črne gore, Severne Makedonije, Romunije in Srbije) s poudarkom na oblikah in gonilnih silah vključevanja velikih tehnoloških podjetij. Ugotovitve razkrivajo tri vzorce: celovito operativno vključevanje, omejeno in zapoznelo vključevanje in minimalno ali brez vključevanja. Razlike oblikujejo medsebojno delujoči dejavniki, vključno z geopolitično usklajenostjo, jasnostjo pripisovanja odgovornosti, vidnostjo incidentov in institucionalno pripravljenostjo. Raziskava razvija večplastni pojasnjevalni okvir, v okviru katerega so velika tehnološka podjetja obravnavana kot kvazi suvereni akterji, katerih vključevanje je selektivno in odvisno od konteksta, kar vpliva na kibernetsko odpornost in digitalno suverenost v manjših državah.

Ključne besede ***Balkan, velika tehnološka podjetja, politika, odpornost, kibernetska varnost.***

Abstract This research examines the role of major technology corporations in shaping cyber resilience during significant cyber incidents in the Balkans in 2022. This study conducts a comparative analysis of eight Balkan nations (Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro, North Macedonia, Romania, and Serbia), focusing on the forms and drivers of Big Tech engagement. The findings identify three patterns: comprehensive operational involvement; limited and delayed engagement; and minimal or no involvement. Interacting factors, including geopolitical alignment, attribution clarity, incident visibility, and institutional preparedness, shape these differences. The research develops a multi-level explanatory framework and conceptualises Big Tech as quasi-sovereign actors whose engagement is selective

© Author(s) 2026. This is an open access article licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/).

and context-dependent, with implications for cyber resilience and digital sovereignty in smaller states.

Key words ***Balkans, Big Tech, policy, resilience, cybersecurity.***

Introduction

In 2022, cyber incidents across the Balkans varied significantly in scale, attribution, and character. Albania and Montenegro experienced large-scale attacks attributed to state-linked actors. Bosnia and Herzegovina and Romania faced both cybercriminal attacks and Distributed Denial-of-Service (DDoS) attacks, whereas North Macedonia experienced nationalist-oriented cyber activity. In Croatia and Kosovo, incidents largely targeted specific sectors and often lacked clear attribution.

From 2021 to 2024, Albania experienced multiple waves of cyberattacks believed to be orchestrated by Iranian state-sponsored actors. The most severe cyberattacks occurred between July and September 2022, targeting government computer systems and resulting in data loss and service disruptions. Hackers accessed, deleted, and leaked sensitive and classified information from both public and government sources, including financial records, data of individuals crossing Albania over 17 years, and the identities of undercover intelligence officers. Prime Minister Edi Rama stated, "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" (Cybersecurity & Infrastructure Security Agency (CISA), 2022; Starks, 2022; Oghanna, 2023).

In September 2022, Bosnia and Herzegovina was hit by an extensive ransomware attack targeting the Parliamentary Assembly's central server. This attack disrupted parliamentary functions and led to the shutdown of the server, email, and website. The assault occurred amid political unrest, as concerns mounted about secession efforts by Republika Srpska, three weeks before general elections in Bosnia and Herzegovina (Greig, 2022; Kurtic, 2022; OSCE Mission to Bosnia and Herzegovina, 2022; Sarajevo Times, 2022).

Furthermore, Bosnia and Herzegovina experienced over 9.2 million cybersecurity threats between mid-November and mid-December 2022. The majority of these threats were DDoS attacks originating from Brazil, the Netherlands, the United States, Russia, Germany, and China. This was primarily due to attackers employing Virtual Private Networks (VPNs) to conceal their actual locations and simulate origins from other regions. A report by Mahmutovic and Hodzic (2023) from the Balkan Investigative Reporting Network of Bosnia and Herzegovina (BIRN BiH) noted that "Many of these attacks are consistent with the methods and capabilities observed from Russia and China," but explicitly stopped short of formal attribution. Additionally, the report stated that "Western European countries and NATO have also expressed growing concern regarding Russian influence in Bosnia and Herzegovina,

particularly in the lead-up to the 2022 elections". No official attribution has been made. This study treats the case of Bosnia and Herzegovina as unattributed, and avoids causal inferences with regard to perpetrator identity.

Croatia's phone provider, A1 Hrvatska, revealed a data breach affecting about 10% of its customers, approximately 200,000 people, in February 2022 (Paganini, 2022). A month later, the daily website Slobodna Dalmacija was hacked by an unknown assailant who managed to replace "a couple of older articles with articles promoting Russian propaganda in the war with Ukraine" (Grgurinovic, 2022). Like other countries, Croatia has experienced a rise in the number of detected cyberattacks. The Security Intelligence Agency identified 14 attacks in 2021, and in 2022, this number grew to 19 (Lozančić, 2023). Neither the perpetrators nor the Croatian authorities made any claims of responsibility or attribution.

In January 2022, Kosovo's media regulatory authority, the Independent Media Commission (IMC), faced a significant cyberattack which caused data loss and disrupted access to official email and internal systems for nearly two months (Isufi, 2022). In the first week of September 2022, government IT systems were targeted by DDoS attacks, leading to intermittent internet outages across government offices and occasional service disruptions in the Ministers` Offices, the Kosovo Police, the e-Kosova Platform, some media outlets, and Kosova Telekom. Its technical director stated that the attacks were unidentified, originating from various foreign IP addresses, and were executed by 30,000 computers. A local IT expert estimated that the attacker used more than 8,000 infected computers to carry out the attacks (Fetahaj, 2022; KOHA, 2022; Вистиномер.мк, 2022). The Prime Minister's Office announcement indicated that "In cooperation with external experts, applying adequate measures, the cyberattack has been overcome and attempts to continue the attack have been prevented" (Qeveria e Republikës së Kosovës, 2022).

In August 2022, the Government of Montenegro's digital infrastructure was hit by an 'unprecedented' ransomware attack which encrypted and locked data and other important files. The attack resulted in the domain gov.me being down for almost a month, along with all government portals, including the websites of the ministries of defence, finance, and the interior, the government's online platforms, the Property Administration, the Revenue and Customs Administration, the courts, the water supply systems, and transportation services. Even the state-owned power utility, EPCG, switched its operations to manual handling to prevent potential damage from a cyberattack described as "the worst attack on its critical IT infrastructure so far" (Kajosevic, 2022b; Šćekić, 2022). Although a hacker group known as Cuba-Ransomware claimed responsibility, Montenegro's Agency for National Security officially attributed the attack to Russia, although it did not provide public evidence. Separately, Trend Micro Research, a commercial cybersecurity vendor, attributed the Cuba-Ransomware variant to Russia-linked actors based on technical indicators, claiming that "Cuba-Ransomware seems to originate from Russia, as evidenced by its routine of terminating itself when a Russian keyboard layout or language

is detected on the system" (Trend Micro Research, 2022). The outgoing Prime Minister, Dritan Abazovic, added that "it was politically motivated following the fall of his government last week" (Milic, 2022; Reuters, 2022; Stojanovic, 2022; Ivanovic, 2024b, 2024a).

North Macedonia's Ministry of Education was targeted in February 2022 by a cyberattack allegedly carried out by a group called 'Powerful Greek Army', which claimed to have access to the ministry's camera system (Marusic, 2022). In August of the same year a DDoS attack targeted St. Cyril and Methodius University (UKIM), targeting the iKnow electronic support system. The Ministry of Education was hacked again, this time allegedly by the 'Greek Hacking Team Netwatchers', which affected the Ministry's website. The Ministry of Agriculture was targeted by the ransomware group BlackByte (Вистиномер.мк, 2022; Elshani, 2025).

Romania's Rompetrol petrol station network was impacted by a 'complex cyberattack' involving ransomware from the Hive group in March 2022, demanding a $2 million ransom. The attack forced Rompetrol to shut down its websites and the Fill&Go service at its petrol stations. Indeed, in an email to employees, Rompetrol acknowledged that the attack affected "most of the IT services" (Sharma, 2022). A month later, the Romanian government's websites were targeted by a DDoS attack, including those of key public institutions such as the government, the border police, the Defence Ministry, Romanian Railways, and private organisations. The Romanian National Cybersecurity Directorate (NCSD) asserted that the cybercrime group 'Killnet', a pro-Russia hacker group, claimed responsibility for the attack on a Telegram channel, arguing that the attacks were justified by Romania's support for Ukraine in the military conflict with the Russian Federation (Necsutu, 2022; The Romanian National Cybersecurity Directorate (NCSD), 2022; Radware, no date).

In mid-June 2022, two months after general elections, Serbia experienced a significant ransomware attack targeting the Republic Geodetic Authority (RGZ). Because RGZ manages vital data, including real estate and land ownership records, as well as information systems used by external parties such as public notaries, the attack paralysed the Serbian real estate market for several weeks (Sasa, Aleksa, 2022; Freedom House, 2023; Salipur, 2024). The Commissioner for Information of Public Importance and Personal Data Protection completed an extraordinary inspection and stated that there was no violation of personal data (Commissioner for Information of Public Importance and Personal Data Protection, 2022).

The term 'Big Tech' is commonly used to describe the most dominant technology corporations – typically including Google, Apple, Microsoft, Amazon and Meta – whose market capitalisations exceed the GDP of many large economies, and whose platforms, infrastructure, and data capacities give them influence across economic, political, and security domains (Birch, Bronson, 2022; Rosencrance, 2021). While various acronyms, such as GAFA, GAFAM, and FAANG, have been used to delineate

this group, the boundaries remain contested and context-dependent (Rosencrance, 2021; Birch, Bronson, 2022).

Despite the increasing scholarly focus on Big Tech's geopolitical influence, regulatory role, and involvement in major conflicts such as the war in Ukraine, there remains a significant empirical gap in the literature: systematic, comparative analyses of how and under what conditions major technology firms intervene during specific national cyber crises, especially in small and medium-sized states, are limited. The 2022 cyberattacks on the Balkan states offer a comparative perspective for addressing this gap, providing meaningful variation in both attack severity and the presence or absence of Big Tech engagement.

In this study, the term 'Big Tech' refers specifically to large technology firms which (1) provide critical digital infrastructure to governments and (2) maintain dedicated cyber threat intelligence and incident response capabilities. 'Cyber resilience' is regarded as a multidimensional capacity encompassing (1) intelligence, investigation and attribution; (2) incident response and containment; (3) recovery and continuity of services; (4) learning and adaptation following attacks; and (5) governance arrangements which facilitate coordination between state and non-state actors. Therefore, cyber resilience is regarded both as a short-term outcome, measured by the ability to restore services and contain damage, and as a longer-term process involving institutional learning, adaptation, and governance reform. The Big Tech involvement is assessed in terms of its contribution to immediate crisis response and its influence on longer-term resilience (Björck et al., 2015; Linkov, Kott, 2019; Safitra et al., 2023; Alhidaifi et al., 2024).

1 LITERATURE REVIEW

Scientific research covers different aspects of Big Tech; some studies investigate its unique contributions to international and local cyber resilience and their effects on geopolitics, while others examine the countermeasures and mitigation strategies in place.

Big Tech companies hold a vital position in geopolitical and security spheres by shaping infrastructure and technological standards which influence international security and state sovereignty. Kitchen (2025) and Khanal et al. (2025) highlighted the increasing influence of Big Tech in both international and domestic policy and security mechanisms. This influence stems from its technological monopoly over the supply and management of essential digital infrastructure, which is crucial to discussions of national digital sovereignty and frequently plays a fundamental role in geopolitical cyber conflict. Their dual-use technologies (civilian and military applications) help shape what some refer to as the "digital-military-industrial complex". Their operations significantly impact global diplomatic relations and their lobbying efforts against international regulatory bodies. Consequently, governments

increasingly regard Big Tech as sovereign actors, appointing "tech ambassadors" to liaise with these companies, highlighting their quasi-state status.

Big Tech focuses on shaping policies on regulation, taxation, and global digital standards to favour their business models. They exert considerable influence over legislative processes and regulatory procedures governing data privacy, antitrust, digital rights, and internet governance through direct lobbying, government consultations, and political contributions. Furthermore, through social media and digital platforms, Big Tech influences public discourse, culture, and information ecosystems worldwide. Its algorithms and content moderation policies shape societal narratives, public opinion, and political mobilisation, producing significant social impacts that extend far beyond economic or political dimensions (Jahangir Khan, 2024).

Passchier (2025) emphasises Big Tech's role as an active political player. Gu (2023) argues that Big Tech has become the new data sovereign that governments must accept in the data era. Tarrant and Cowen (2022) analyse the role of Big Tech in lobbying within the EU concerning the Digital Markets Act. Leclercq-Vandelannoitte and Bertin (2024) coined the term "Big Tech Raj", arguing that "Big Tech firms produce a new form of biopower in the digital era by virtue of their material configurations (constituted by technology, such as applications, algorithms, AI systems), which create conditions for steering people's conduct".

Another significant aspect of policy concerns the climate. Big Tech companies are increasingly involved in climate-related initiatives, including commitments to sustainability in data centres, investments in green technology, and support for global climate governance. Their extensive energy consumption and carbon emissions also position them as key players in discussions of environmental impact (Jahangir Khan, 2024; LaForge, 2025).

Big Tech companies significantly influence the digital ecosystems of developing countries, affecting economic dependence and policy development. They lead technological progress by specialising in areas such as AI, cloud services, digital platforms, and telecommunications. Their investments in research and development and dominant platform control encourage innovation, creating new products and services which transform industries and drive global scientific progress (Khanal et al., 2025).

However, Big Tech's concentration of power also exerts pressure on democratic institutions and the rule of law through potentially opaque and unequal practices. Birch and Bronson (2022) analysed the growing public and political backlash known as the 'techlash', which has led to a decline in trust in these companies and their practices. Parsheera (2023) examined India's policy responses to Big Tech, which combine traditional regulatory approaches with novel strategies. Vrikki (2024) underscored the need for more "rigorous regulatory frameworks and independent

third-party audits to ensure genuine progress towards a sustainable future and proper accountability". Zingales (2022) argued that mitigating Big Tech power can only be achieved through international structural interventions which restore the conditions for competition, since no national regulator can do so. FitzGerald and Parziale (2017) also emphasised the importance of reforming structures and processes to introduce accountability for Big Tech actors.

Building on this gap, this paper explores two research questions: (RQ1) What types of support did major technology firms offer during and after the 2022 cyber incidents in the Balkans, and how did this support affect the immediate responses and long-term resilience? (RQ2) What factors may explain the differences in Big Tech engagement across cases?

2 METHODOLOGY

This study employs an exploratory, qualitative case-study approach to examine how Big Tech's involvement evolved during the major cyberattacks on Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro, North Macedonia, Romania, and Serbia in 2022. Data collection prioritised diverse and highly reliable sources, grounded in three fundamental principles: relevance, which ensures a direct connection to research questions; reliability, characterised by recognised accuracy and methodological soundness; and diversity, encompassing multiple perspectives and source types. Document retrieval was achieved through searches of Google Scholar, institutional repositories, government portals, and threat intelligence platforms. 'Highly reliable' was defined as: produced by or attributable to a named institutional author, government body, peer-reviewed journal, or established investigative outlet with a verifiable editorial process. Key empirical claims, especially those concerning Big Tech's operational involvement, were accepted only if supported by at least two independent sources of different types, such as a threat intelligence report verified by a government statement or a reputable news outlet.

A chronological timeline documented major cyberattacks in the analysed Balkan states in 2022, facilitating the identification of critical junctures and deployment patterns. The final collection comprised 62 primary documents, including: (1) academic publications, (2) official government advisories, (3) threat intelligence corporate reports, and (4) reputable media outlets and think tanks. Sources were included only if they directly documented or analysed the 2022 cyberattacks in the Balkan states in question, contained verifiable factual claims from institutional or expert authors, and were publicly accessible. Conversely, sources were excluded if they were based solely on unverifiable opinion, lacked clear authorship, or originated from outlets with documented records of disinformation.

The documents were analysed using qualitative thematic coding. The coding categories –analysis and investigation, operational support, attribution, infrastructure deployment, and post-incident engagement – were developed inductively from an

initial reading of the source material, and remained aligned with the cyber resilience framework specified in the introduction. The coding process was carried out by the author using a single-coder approach; analytical consistency was maintained through iterative review of category definitions against the entire source corpus.

This study examines Big Tech's role in strengthening cyber resilience in the analysed Balkan states during and after the major cyberattacks in 2022. These countries were selected because each experienced a notable, publicly reported cyberattack which affected national infrastructure or government functions within the same year, enabling a controlled comparison over time. They also display differences in the main outcome variable, making the selection meaningful from a theoretical perspective. The focus is on 2022, a pivotal year characterised by high-severity, high-profile cyberattacks targeting government institutions and infrastructure across the region. The research does not investigate commercial partnerships between Big Tech firms and the Balkan countries beyond the incidents discussed.

This study recognises several constraints: (1) reliance on documentary evidence limits access to lived experiences and classified information, (2) limited understanding of Big Tech's cyber intervention policies in the cyber resilience of foreign states, and (3) the predominance of English-language sources may underrepresent domestic perspectives.

3 FINDINGS

The cyberattacks on Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro, North Macedonia, Romania, and Serbia in 2022 were widespread and devastating, targeting critical national infrastructure and government institutions.

In the analysis that follows, Microsoft and Google are considered Big Tech actors in the full sense defined above. Trend Micro and Oracle, which appear in the Montenegrin case, are described as specialised cybersecurity and enterprise infrastructure vendors whose roles are mainly transactional rather than quasi-operational; they are included for completeness but are analytically distinct.

In September 2022, during the widespread cyberattacks, Microsoft actively participated in efforts to counter the threats. Shortly after the damaging cyberattacks against the Albanian government in mid-July, the Microsoft Detection and Response Team (DART), together with the FBI and other specialists, was engaged by the Albanian government to lead an investigation and forensic analysis into the attacks and their various phases. At the time of the attacks, Microsoft publicly stated that it "is committed to helping our customers be secure while achieving more. During this event, we quickly mobilized our Detection and Response Team (DART) to help the Albanian government rapidly recover from this cyberattack by isolating its infrastructure and shutting down critical systems to prevent damage. Microsoft will continue to partner with Albania to manage cybersecurity risks while continuing

to enhance protections from malicious attackers". Additionally, Microsoft's investigation attributed the cyberattacks with high confidence to multiple Iranian government-sponsored actors (Microsoft Threat Intelligence, 2022; Starks, 2022).

Indeed, the White House National Security Council statement confirmed that the U.S. government had been "on the ground" working alongside private-sector partners to mitigate, recover from, and investigate the cyberattack (The White House, 2022). Microsoft assisted Albania not only in recovering from the 2022 cyberattacks but also in countering future cyberattacks by deploying its security solutions "to gain comprehensive visibility across its infrastructure and prepare for future attacks". (Microsoft, 2023). Google published its own comprehensive report analysing cyberattacks against Albania and attributing them to Iran (Jenkins et al., 2022)

The FBI and the French National Cybersecurity Agency, ANSSI, as well as cyber experts, assisted in investigating the August 2022 Cuba ransomware attack, which the outgoing Montenegrin Prime Minister, Dritan Abazovic, described as "unprecedented" and "dangerous and politically motivated". However, there were no reports of Big Tech involvement in the analysis, aside from Trend Micro Research's attribution of the Cuba ransomware to Russia (Kajosevic, 2022a; Radio Free Europe/Radio Liberty, 2022; Vujovic, 2023). Since the cyberattack, Montenegro has spent millions of euros across fifteen public tenders to procure servers, IT and communications equipment, and security devices, including Microsoft and Oracle security solutions, rather than open-source software. This spending raised questions from local security experts: "For some reason we tend not to ask such questions in the case of software products, and I strongly believe we should" (Vucinic, 2024).

Public records indicate no involvement by Big Tech companies in enhancing the cyber resilience of Bosnia and Herzegovina, Croatia, Kosovo, North Macedonia, Romania and Serbia during and following the 2022 cyberattacks.

This absence was confirmed through targeted searches of public government communications, Big Tech newsrooms (including Microsoft, Google, and Amazon Web Services), official cybersecurity advisories (such as CISA and ENISA), and investigative reports from BIRN and regional media. No signs of operational activity, advisory roles, or joint statements between Big Tech firms and governments were found.

The lack of documented engagement by Big Tech in Serbia is analytically significant. Serbia's geopolitical stance is ambiguous: although an EU candidate, it maintains close relations with Russia and China and has not acceded to NATO. These alignments may diminish the likelihood of corporate intervention aligned with U.S. interests. The 2022 ransomware incident was attributed to cybercriminals rather than state-sponsored actors, which appears to lessen the incentives for Big Tech to become operationally involved. Furthermore, institutional capacity limitations and

the absence of formal public-private cyber crisis frameworks may have further constrained potential avenues for engagement.

Bosnia and Herzegovina presents a structurally distinct negative case. The attack on the Parliamentary Assembly in September 2022 occurred amid acute political tensions concerning secession, rendering coordinated engagement with external partners politically sensitive. The lack of clear attribution to state-sponsored actors, and the absence of a NATO membership framework similarly diminish the structural conditions which would facilitate Big Tech intervention.

In Croatia, cyber incidents in 2022 mainly affected the telecommunications sector, limiting their impact to specific industries rather than core state infrastructure. Although disruptive, these attacks remained relatively contained, and did not attract significant international attention or clear attribution to state actors. Consequently, responses were handled domestically or through sector-specific mechanisms, with no documented operational involvement by major technology firms.

In Kosovo, the cyberattacks targeted government services and public-facing digital infrastructure, causing temporary disruptions. However, the incidents were relatively limited in scale and duration, and lacked strong attribution to state-sponsored actors. This combination of constrained impact and lower geopolitical visibility likely reduced incentives for external corporate engagement, resulting in no documented involvement by Big Tech.

North Macedonia experienced cyber activity marked by nationalist-leaning attacks, driven by politically motivated actors who were either non-state or of unclear attribution. Although these attacks carried political weight, they did not lead to widespread or systemic disruptions of the country's infrastructure. As a result, the responses mainly remained domestic, with no definitive signs of support from major technology firms.

In Romania, the cyber incidents involved both a cybercriminal attack and a DDoS campaign linked to a pro-Russian hacker group. Despite this mixed threat environment, the attacks did not cause sustained nationwide disruption or escalate into a high-profile geopolitical crisis. The responses were managed through national capabilities and existing partnerships, with no documented direct involvement by Big Tech actors.

Collectively, these cases indicate that the lack of Big Tech engagement reflects genuine structural, political, and geopolitical constraints rather than limitations related to data availability.

Table 1: Cyber attacks on the analysed Balkan states and the implemented countermeasures

State	Measures					Countermeasures	
	Date	Target	Damage	Attribution		Company	Intervention
				To	By		
Albania	July-September 2022	The government's computer system	Gather, delete and leak private and classified information	Iran	Albanian Government, Microsoft, Google	Microsoft	Investigation, analysis, technical recovery, attribution, deploying security solutions
						Google	Analysis, attributions
Bosnia and Herzegovina	September 2022	Ransomware targeting the Parliamentary Assembly	Crippled the parliament's operations	None		None	None
	November - December 2022	DDoS		Originating from Brazil, the Netherlands, the United States, Russia, Germany, and China		None	None
Croatia	February 2022	Phone provider A1 Hrvatska	Breach affecting about 10% of its customers	None		None	None
	March 2022	The daily website Slobodna Dalmacija	Hack and replace old articles with pro-Russian propaganda	None		None	None
Kosovo	January, September 2022	DDoS attacks against government IT systems	Ministers` Offices, the Kosovo Police, the e-Kosova Platform, some media outlets, and Kosova Telekom	None		None	None
Montenegro	August 2022	Ransomware targeting the government's digital infrastructure	Shutdown of all Government portals and services	Russia	Montenegrin Government, Trend Micro	Microsoft, Oracle	Procurement of security solutions
						Trend Micro	Attribution
North Macedonia	February 2022	Ministry of Education	Access to the Ministry's camera system and website	Powerful Greek Army	Claimed responsibility	None	None
	August 2022	St. Cyril and Methodius University (UKIM), Ministry of Education	UKIM's iKnow electronic support system	Greek Hacking Team Netwatchers	Claimed responsibility	None	None
Romania	March 2022	Rompetrol	Shut down of the websites and the Fill&Go service	Hive ransomware	Claimed responsibility	None	None
	April 2022	Government's websites, public institutions and private organisations	DDoS	Killnet	Claimed responsibility	None	None
Serbia	June 2022	Ransomware targeting the Geodetic Authority	Real estate market paralysed for weeks	None		None	None

4 DISCUSSION

This study examined two research questions: (1) What types of support major technology firms offered during and after the 2022 cyber incidents in the Balkans, and how did this support affect cyber resilience? and (2) What factors may explain the observed variation in Big Tech engagement across cases? The findings show a notably uneven pattern of involvement between the states and suggest that such engagement is selective, conditional, and influenced by multiple interacting factors.

Concerning the first research question, the findings reveal three clear patterns of Big Tech involvement. First, Albania exemplifies comprehensive, operational engagement, in which Microsoft and Google contributed across various areas, including threat intelligence, forensic investigation, attribution, incident response, and post-incident resilience-building. This level of involvement had a noticeable effect on both the immediate recovery and the long-term institutional capacity, effectively positioning Big Tech as a quasi-operational extension of national cyber defence.

In the second pattern, the Montenegro case demonstrates a limited and delayed engagement model, where Big Tech did not play a significant operational role during the crisis but became involved indirectly through post-incident procurement of proprietary security solutions. This distinction emphasises an important analytical difference between operational support during a crisis and technology acquisition after the event, with only the former directly contributing to real-time resilience and institutional learning.

In the third pattern, the remaining cases – Bosnia and Herzegovina, Croatia, Kosovo, North Macedonia, Romania and Serbia – demonstrate minimal or no documented Big Tech involvement, despite cyber incidents of varying severity. In these contexts, the responses were largely managed through domestic capabilities or alternative external actors. This absence is analytically significant, indicating that Big Tech engagement is not an automatic response to cyber incidents, even when critical infrastructure is affected.

These differences in engagement align with variations in resilience outcomes. Albania's swift recovery and strengthened defensive stance demonstrate the advantages of integrated external support, whereas Montenegro's slower, procurement-focused approach highlights the drawbacks of delayed engagement. The other cases indicate more limited recovery paths, possibly due to reliance on fragmented or internally constrained response mechanisms.

Addressing the second research question, the findings suggest that the variation in Big Tech involvement is best understood through a multilevel framework involving structural, situational, interactional, and corporate factors.

At the structural level, geopolitical alignment and institutional capacity influence the conditions under which engagement can occur. Albania's alignment with Western institutions appears to have facilitated cooperation with U.S.-based firms, whereas Serbia's more ambiguous stance and Bosnia and Herzegovina's divided governance structure may have limited such engagement. Institutional readiness also plays a role in whether states can effectively absorb and coordinate external assistance.

At the situational level, the nature, attribution, and visibility of cyber incidents are crucial. Large technology firms are more likely to become involved when attacks are clearly attributed to state-sponsored actors and positioned within broader geopolitical conflicts, as seen in Albania. Conversely, ambiguous attribution (Bosnia and Herzegovina), cybercriminal framing (Serbia and Romania), or lower visibility (Croatia, Kosovo, North Macedonia) tend to diminish the incentives for corporate intervention. The type of targeted infrastructure also plays a role: attacks on central government systems are more prone to prompt engagement than those affecting isolated sectors.

At the interactional level, openness, existing public-private partnerships, and trust influence the depth of engagement. Albania's ability to quickly integrate external actors reflects the presence of supportive institutional interfaces. Legal and regulatory frameworks further shape these dynamics by either enabling or restricting foreign corporate involvement.

At the corporate level, Big Tech firms act as strategic and selective actors, guided by considerations such as geopolitical alignment, reputational benefits, and risk exposure. Their engagement is therefore not purely demand-driven, but reflects internal calculations about where intervention is both feasible and advantageous.

Taken together, these findings indicate that Big Tech's involvement in cyber crises is driven not just by technical needs or attack severity, but by a combination of political, institutional, and strategic considerations. This strengthens the view of Big Tech as a quasi-sovereign actor, whose selective engagement transforms the cyber resilience landscape and alters the distribution of authority in cyberspace.

5 FUTURE RESEARCH

Future studies could (1) expand the geographical scope beyond the Balkans to incorporate comparative analyses of Big Tech involvement in cyber incidents affecting other small and medium-sized states, particularly in Eastern Europe, the Caucasus, and the Global South. Such comparisons would help determine whether the patterns observed in the selected Balkan states reflect wider structural dynamics or region-specific conditions. (2) Broaden the chronological scope of Big Tech involvement in Balkan cyber resilience and evaluate whether patterns of Big Tech engagement changed during subsequent cyber incidents in the Balkans. (3) Examine the long-term impacts of Big Tech involvement on national cyber governance. While

this study primarily focuses on crisis response and short-term resilience, further research is required to assess how sustained reliance on proprietary technologies affects institutional capacity-building, vendor dependence, and digital sovereignty over time. (4) Investigate Big Tech influence in the Balkans across various domains, including the economy, politics, international relations, society, innovation, and legal spheres. (5) Analyse the decision-making processes behind Big Tech intervention, particularly how these companies decide internally whether, when, and how to intervene during state-level cyber crises. (6) Evaluate the legal and accountability frameworks governing Big Tech intervention in national cyber crises, with special focus on transparency, responsibility, and oversight of democratic processes.

Conclusion

This study examined the role of major technology corporations in shaping cyber resilience in Balkan states during significant cyber incidents in 2022. It found that Big Tech involvement varies considerably across cases and is neither automatic nor evenly distributed. Instead, engagement is selective and depends on a combination of geopolitical alignment, institutional preparedness, incident features, and corporate strategic considerations.

The case of Albania illustrates how extensive operational involvement by Big Tech can greatly improve both immediate crisis response and long-term resilience. Meanwhile, Montenegro reveals the limitations of a procurement-focused approach that lacks real-time external support. The lack of meaningful engagement in Bosnia and Herzegovina, Croatia, Kosovo, North Macedonia, Romania and Serbia further demonstrates that even major cyber incidents do not always prompt corporate intervention.

The findings enhance the literature by developing a multi-level explanatory framework for understanding Big Tech engagement in cyber crises, and by conceptualising these firms as quasi-sovereign actors whose decisions reflect strategic selectivity rather than neutral service provision. This perspective challenges assumptions that private-sector involvement in cybersecurity is universally accessible or evenly distributed.

The study also highlights important policy implications. While Big Tech involvement can significantly enhance national cyber resilience, it may also lead to long-term dependencies and raise concerns about digital sovereignty, accountability, and governance. Countries lacking access to such support may remain disproportionately vulnerable, while those relying heavily on external providers risk losing strategic autonomy in cybersecurity decision-making.

Overall, the findings highlight an increasingly complex and uneven landscape of cyber resilience, in which private corporations play a growing yet selective role. Addressing this imbalance requires not only enhanced national capacity but also clearer frameworks for regulating and institutionalising public-private cooperation in cybersecurity.

AI Disclosure Statement

When preparing this article, the author used ChatGPT (GPT-5.4) on 27 March 2026 with the following prompt: "Please evaluate the attached paper," to review the paper. The author subsequently reviewed and edited the output as necessary and accepts full responsibility for the content and integrity of the publication.

References

1. *Alhidaifi, S.M., Asghar, M.R., Ansari, I.S., 2024. A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. ACM Comput. Surv., 56(8): p 196:1-196:48. DOI: 10.1145/3649218.*
2. *Birch, K., Bronson, K., 2022. Big Tech. Science as Culture, 31(1), pp. 1–14.DOI: 10.1080/09505431.2022.2036118.*
3. *Björck, F. et al., 2015. Cyber Resilience – Fundamentals for a Definition. In: A. Rocha et al. (Eds), New Contributions in Information Systems and Technologies. Cham: Springer International Publishing, pp. 311–316.DOI: 10.1007/978-3-319-16486-1_31.*
4. *Commissioner for Information of Public Importance and Personal Data Protection, 2022. Commissioner Completed Extraordinary Inspection of Republic Geodetic Authority – Commissioner for Information of Public Importance and Personal Data Protection. https://web.archive.org/web/20230426152630/https://www.poverenik.rs/en/press-releases/3819-%D0%BF%D0%BE%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%B8%D0%BA-%D0%BE%D0%BA%D0%BE%D0%BD%D1%87%D0%B0%D0%BE-%D0%B2%D0%B0%D0%BD%D1%80%D0%B5%D0%B4%D0%BD%D0%B8-%D0%B8%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%86%D0%B8%D1%98%D1%81%D0%BA%D0%B8-%D0%BD%D0%B0%D0%B4%D0%B7%D0%BE%D1%80-%D0%BD%D0%B0%D0%B4-%D1%80%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D1%87%D0%BA%D0%B8%D0%BC-%D0%B3%D0%B5%D0%BE%D0%B4%D0%B5%D1%82%D1%81%D0%BA%D0%B8%D0%BC-%D0%B7%D0%B0%D0%B2%D0%BE%D0%B4%D0%BE%D0%BC-2.html (Accessed 20 February 2026).*
5. *Cybersecurity & Infrastructure Security Agency (CISA), 2022. Iranian State Actors Conduct Cyber Operations Against the Government of Albania. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264 (Accessed 20 February 2026).*
6. *Elshani, D., 2025. Navigating the Evolving Threat Landscape and Institutional Responses to Cybersecurity Threats in the Western Balkans. Balkan Investigative Reporting Network, pp 1–22. https://balkaninsight.com/wp-content/uploads/2025/02/RDRAF-JAN25.pdf (Accessed 2 February 2026).*
7. *Fetahaj, K., 2022 Analizë e shkurtër e sulmeve kibernetike të..., Facebook. https://www.facebook.com/kastriot.fetahaj/posts/pfbid02ujLLwUTfBaiFRY8CuSHrz382TMuFaNybGPiPptsrw5SmuNvXoG85ovF.*
8. *FdZB5Q5RmLl (Accessed 20 February 2026).*
9. *FitzGerald, B., Parziale, J., 2017. As technology goes democratic, nations lose military control. Bulletin of the Atomic Scientists, 73(2), pp 102–107. DOI: 10.1080/00963402.2017.1288445.*
10. *Freedom House, 2023. Serbia: Freedom on the Net 2023 Country Report. https://freedomhouse.org/country/serbia/freedom-net/2023 (Accessed 22 December 2025).*
11. *Greig, J., 2022. Bosnia and Herzegovina investigating alleged ransomware attack on parliament. https://therecord.media/bosnia-and-herzegovina-investigating-alleged-ransomware-attack-on-parliament (Accessed 22 December 2025).*
12. *Grgurinovic, M., 2022. Hackers Attack Croatian Daily, Post Kremlin Propaganda. Balkan Insight, 23 March. https://balkaninsight.com/2022/03/23/hackers-attack-croatian-daily-post-kremlin-propaganda/bi/ (Accessed 25 March 2026).*

13. *Gu, H., 2023. 'Data, Big Tech, and the New Concept of Sovereignty', Journal of Chinese Political Science, 29(4), pp 591-612. DOI: 10.1007/S11366-023-09855-1.*
14. *Hawley, J., 2021. The Tyranny of Big Tech. Simon and Schuster.*
15. *Isufi, P., 2022. Kosovo Media Regulator Struggling to Recover from Cyber-Attack. Balkan Insight, 10 March. https://balkaninsight.com/2022/03/10/kosovo-media-regulator-struggling-to-recover-from-cyber-attack/bi/ (Accessed 17 March 2026).*
16. *Ivanovic, I., 2024a. Montenegro's Proposed New Cybersecurity Structure Raises Concerns. Balkan Insight, 2 October. https://balkaninsight.com/2024/10/02/montenegros-proposed-new-cybersecurity-structure-raises-concerns/ (Accessed 20 November 2025).*
17. *Ivanovic, I., 2024b. Press Restart: Montenegro Launches New Open Data Portal after Cyberattack. Balkan Insight, 24 September. https://balkaninsight.com/2024/09/24/press-restart-montenegro-launches-new-open-data-portal-after-cyberattack/ (Accessed 20 November 2025).*
18. *Jahangir Khan, W., 2024. Tech Giants as Emerging Diplomatic Players. Centre for Strategic and Contemporary Research [Preprint]. https://cscr.pk/explore/publications/articles/tech-giants-as-emerging-diplomatic-players/ (Accessed 2 February 2026).*
19. *Jenkins, L. et al., 2022. ROADSWEEP Ransomware Targets the Albanian Government. Google Cloud Blog [Preprint]. https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/ (Accessed 12 February 2026).*
20. *Kajosevic, S., 2022a. Montenegro Accuses Russia of Cyber-Attacks on Govt Server. Balkan Insight, 26 August. https://balkaninsight.com/2022/08/26/montenegro-accuses-russia-of-cyber-attacks-on-govt-server/ (Accessed 21 December 2025).*
21. *Kajosevic, S., 2022b. Montenegro Govt Remains Offline Amid Continued Cyber Safety Fears. Balkan Insight, 16 September. https://balkaninsight.com/2022/09/16/montenegro-govt-remains-offline-amid-continued-cyber-safety-fears/bi/ (Accessed 25 March 2026).*
22. *Khanal, S., Zhang, H. and Taeihagh, A., 2025. Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. Policy and Society, 44(1), pp 52–69. DOI: 10.1093/POLSOC/PUAE012.*
23. *Kitchen, K., 2025. The New Superpowers: How and Why the Tech Industry is Shaping the International System. 65. https://www.nationalaffairs.com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system (Accessed 2 February 2026).*
24. *KOHA, 2022. Krasniqi: Sulmi në Telekom u shkaktua nga 30 mijë kompjuterë të huaj, KOHA.net. https://www.koha.net/arberi/krasniqi-sulmi-ne-telekom-u-shkaktua-nga-30-mije-kompjutere-te-huaj (Accessed 20 February 2026).*
25. *Kurtic, A., 2022. 'Bosnia Remains Silent on Hacker Attack on Parliament', Balkan Insight, 28 September. https://balkaninsight.com/2022/09/28/bosnia-remains-silent-on-hacker-attack-on-parliament/bi/ (Accessed 25 March 2026).*
26. *LaForge, G., 2025. 'Big Tech's Foreign Policy Takeover', TechPolicy.Press [Preprint]. https://www.techpolicy.press/big-techs-foreign-policy-takeover/ (Accessed 21 February 2026).*
27. *Leclercq-Vandelannoitte, A., Bertin, E., 2024. How to deal with Big Tech power? The "Big Tech Raj", a new form of biopower in the digital age. Technological Forecasting and Social Change, 208, pp 123732–123732. DOI: 10.1016/J.TECHFORE.2024.123732.*
28. *Linkov, I., Kott, A., 2019. Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: A. Kott, I. Linkov (Eds), Cyber Resilience of Systems and Networks. Cham: Springer International Publishing, pp 1–25. DOI: 10.1007/978-3-319-77492-3_1.*
29. *Lozančić, B., 2023. SK@UT: Increased number of APT cyber-attacks on Croatian infrastructure, Hrvatska radiotelevizija. https://glashrvatske.hrt.hr/en/domestic/sk-ut-increased-number-of-apt-cyber-attacks-on-croatian-infrastructure-10819180 (Accessed 25 March 2026).*

30. *Mahmutovic, A., Hodzic, E., 2023. Bosnia and Herzegovina Cyber Threat Assessment. Sarajevo: Balkan Investigative Reporting Network of Bosnia and Herzegovina (BIRN BiH), pp 1–28. https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-ENG-WEB.pdf (Accessed 7 February 2026).*
31. *Marusic, S.J., 2022. North Macedonia Ministry Confirms New Hacking Attack. Balkan Insight, 7 February. https://balkaninsight.com/2022/02/07/north-macedonia-ministry-confirms-new-hacking-attack/ (Accessed 23 February 2026).*
32. *Microsoft, 2023. Government of Albania recovers from cyberattack in three days, builds resilience with Microsoft Security solutions. https://www.microsoft.com/en/customers/story/1623042714960085027-albania-government-microsoft-security-solutions (Accessed 22 December 2025).*
33. *Microsoft Threat Intelligence, 2022. Microsoft investigates Iranian attacks against the Albanian government. Microsoft Security Blog [Preprint]. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.*
34. *Milic, P., 2022. FBI's team to investigate massive cyberattack in Montenegro. AP News. https://apnews.com/article/russia-ukraine-technology-hacking-montenegro-2a8eb2df87f657b6d7b9971b7419bff9 (Accessed 19 November 2025).*
35. *Necsutu, M., 2022. Cyber Attacks Hit Romanian Government Websites. Balkan Insight, 29 April. https://balkaninsight.com/2022/04/29/cyber-attacks-hit-romanian-government-websites/rd/rd-czechia/ (Accessed 24 March 2026).*
36. *Oghanna, A., 2023. How Albania Became a Target for Cyberattacks. https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/#selection-1123.0-1123.44.*
37. *OSCE Mission to Bosnia and Herzegovina, 2022. Statement of the OSCE Mission to BiH on recent cyber-attack on the BiH Parliamentary Assembly. https://bih.osce.org/mission-to-bosnia-and-herzegovina/526919 (Accessed 22 December 2025).*
38. *Paganini, P., 2022. Croatian phone carrier A1 Hrvatska discloses data breach. Security Affairs, 12 February. https://securityaffairs.com/127919/data-breach/a1-hrvatska-data-breach.html (Accessed 25 March 2026).*
39. *Parsheera, S., 2023. India's Policy Responses to Big Tech: And an Eye on the Rise of "Alt Big Tech". Indian Journal of Law and Technology, 18(1), pp 3–34. DOI: 10.55496/YMGL7324.*
40. *Passchier, R., 2025. How "Big Tech" Undermines Our Democracy. Leiden University [Preprint]. https://www.universiteitleiden.nl/en/news/2025/03/how-big-tech-undermines-our-democracy (Accessed 16 February 2026).*
41. *Qeveria e Republikës së Kosovës, 2022. Gjatë javës së kaluar, në... Facebook. https://www.facebook.com/GOVRKS/posts/pfbid02JhvAptGvRJXbgBdZwe7TFsJNvBq*
42. *7L27KTdQZx6ZLTEt7Tp6eHzHMJ9KxQeHxvjuZl (Accessed 20 February 2026).*
43. *Radio Free Europe/Radio Liberty, 2022. FBI Experts To Investigate Massive Cyberattack In Montenegro. Radio Free Europe/Radio Liberty, 31 December. https://www.rferl.org/a/montenegro-cyberattack-fbi-experts-russia/32012599.html (Accessed 21 December 2025).*
44. *Radware, no date. Killnet, Radware. https://www.radware.com/cyberpedia/ddos-attacks/killnet (Accessed 27 March 2026).*
45. *Reuters, 2022. Montenegro's state infrastructure hit by cyber attack - officials. Reuters, 26 August. https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/ (Accessed 18 November 2025).*
46. *Rosencrance, L., 2021. What is Big Tech?. TechTarget [Preprint]. https://www.techtarget.com/whatis/definition/Big-Tech (Accessed 2 February 2026).*
47. *Safitra, M.F., Lubis, M., Kurniawan, M.T., 2023. Cyber Resilience: Research Opportunities'. Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering. New York, NY, USA: Association for Computing Machinery (ICECC '23), pp 99–104. DOI: 10.1145/3592307.3592323.*

48. *Salipur, I., 2024. Escalating cybercriminal tactics in the Balkan region. Group-IB, 30 October. https://www.group-ib.com/blog/cybercriminal-tactics-in-the-balkan-region/ (Accessed 22 December 2025).*
49. *Sarajevo Times, 2022. Main Server of the Parliamentary Assembly of BiH was shut down due to a Cyber Attack. Sarajevo Times, 10 September. https://sarajevotimes.com/main-server-of-the-parliamentary-assembly-of-bih-was-shut-down-due-to-a-cyber-attack/ (Accessed 22 December 2025).*
50. *Sasa, D. and Aleksa, 2022. 'Hackers Likely Accessed Emails of Serbia's Cadastre Staff, BIRN Reveals. Balkan Insight, 21 September. https://balkaninsight.com/2022/09/21/hackers-likely-accessed-emails-of-serbias-cadastre-staff-birn-reveals/ (Accessed 22 December 2025).*
51. *Šćekić, S., 2022. Cyber-attacks on the Critical Infrastructure – and what's next for Montenegro | AmCham Montenegro. 22 September. https://www.amcham.me/2022/09/cyber-attacks-on-the-critical-infrastructure-and-whats-next-for-montenegro/ (Accessed 24 November 2025).*
52. *Sharma, A., 2022. Rompetrol gas station network hit by Hive ransomware, BleepingComputer. https://www.bleepingcomputer.com/news/security/rompetrol-gas-station-network-hit-by-hive-ransomware/ (Accessed 25 March 2026).*
53. *Starks, T., 2022. How Albania reckoned with alleged Iranian hackers. The Washington Post [Preprint]. https://www.washingtonpost.com/politics/2022/09/26/how-albania-reckoned-with-alleged-iranian-hackers/.*
54. *Stojanovic, D., 2022. Montenegro wrestles with massive cyberattack, Russia blamed, AP News. https://apnews.com/article/russia-ukraine-nato-technology-hacking-religion-5c2bd851027b56a77eaf9385b7d5d741 (Accessed 19 November 2025).*
55. *Tarrant, A., Cowen, T., 2022. Big Tech Lobbying in the EU. The Political Quarterly, 93(2), pp 218–226. DOI: 10.1111/1467-923X.13127.*
56. *The Romanian National Cybersecurity Directorate (NCSD), 2022. Press Release: DDoS attacks against public and private websites in Romania. https://dnsc.ro/citeste/press-release-ddos-attacks-agains-public-and-private-websites-in-romania (Accessed 25 March 2026).*
57. *The White House, 2022. Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania. https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/ (Accessed 2 February 2026).*
58. *Trend Micro Research, 2022. Ransomware Spotlight: Cuba| Trend Micro (MX). https://www.trendmicro.com/vinfo/mx/security/news/ransomware-spotlight/ransomware-spotlight-cuba (Accessed 22 December 2025).*
59. *Vrikki, P., 2024. Measuring Up? The Illusion of Sustainability and the Limits of Big Tech Self-Regulation. Sustainability 2024, Vol. 16, Page 10197, 16(23), pp 10197–10197. DOI: 10.3390/SU162310197.*
60. *Vucinic, Z., 2024. Montenegro's Cybersecurity Spending Spree Sparks Questions About Cost. Balkan Insight, 23 May. https://balkaninsight.com/2024/05/23/montenegros-cybersecurity-spending-spree-sparks-questions-about-cost/ (Accessed 21 December 2025).*
61. *Vujovic, D., 2023. Meagre Resources Leave Montenegro Exposed to Cyber Threats. Balkan Insight, 9 May. https://balkaninsight.com/2023/05/09/meagre-resources-leave-montenegro-exposed-to-cyber-threats/ (Accessed 21 December 2025).*
62. *Zingales, L., 2022. 'Regulating big tech'. www.bis.org (Accessed 2 February 2026).*
63. *Вистиномер.мк, 2022. Albania, Kosovo, Montenegro and North Macedonia Victims of Cyber-Attacks. Truthmeter, 21 September. https://truthmeter.mk/albania-kosovo-montenegro-and-north-macedonia-victims-of-cyber-attacks/ (Accessed 20 February 2026).*

E-pošta: tal@cybureau.org

ORCID: 0000-0002-4046-0867

Dr. Tal Pavel je doktoriral iz bližnjevzhodnih študij na Univerzi Bar-Ilan v Izraelu (naslov disertacije: Spremembe vladnih omejitev uporabe interneta v Siriji, Egiptu, Savdski Arabiji in Združenih arabskih emiratih med letoma 2002 in 2005). Trenutno je zaposlen naUniverzi v Galatu Dunarea de Jos v Romuniji. Specializiran je za geopolitične vidike kibernetske varnosti – stične točke med mednarodnimi odnosi, politologijo in kibernetskim prostorom.

Tal Pavel, PhD holds a PhD in Middle Eastern Studies from Bar-Ilan University, Israel (Dissertation: »Changes in Governmental Restrictions over the Use of the Internet in Syria, Egypt, Saudi Arabia and the United Arab Emirates between 2002 and 2005«). Currently he is affiliated with the »Dunarea de Jos« University of Galati (Romania). He is specializing in the geopolitical aspects of cybersecurity – the tangent lines between international relations, political science, and cyberspace.

Email: tal@cybureau.org

ORCID: 0000-0002-4046-0867

* Prispevki, objavljeni v Sodobnih vojaških izzivih, niso uradno stališče Slovenske vojske niti organov, iz katerih so avtorji prispevkov.

* Articles published in the Contemporary Military Challenges do not reflect the official viewpoint of the Slovenian Armed Forces nor the bodies in which the authors of articles are employed.