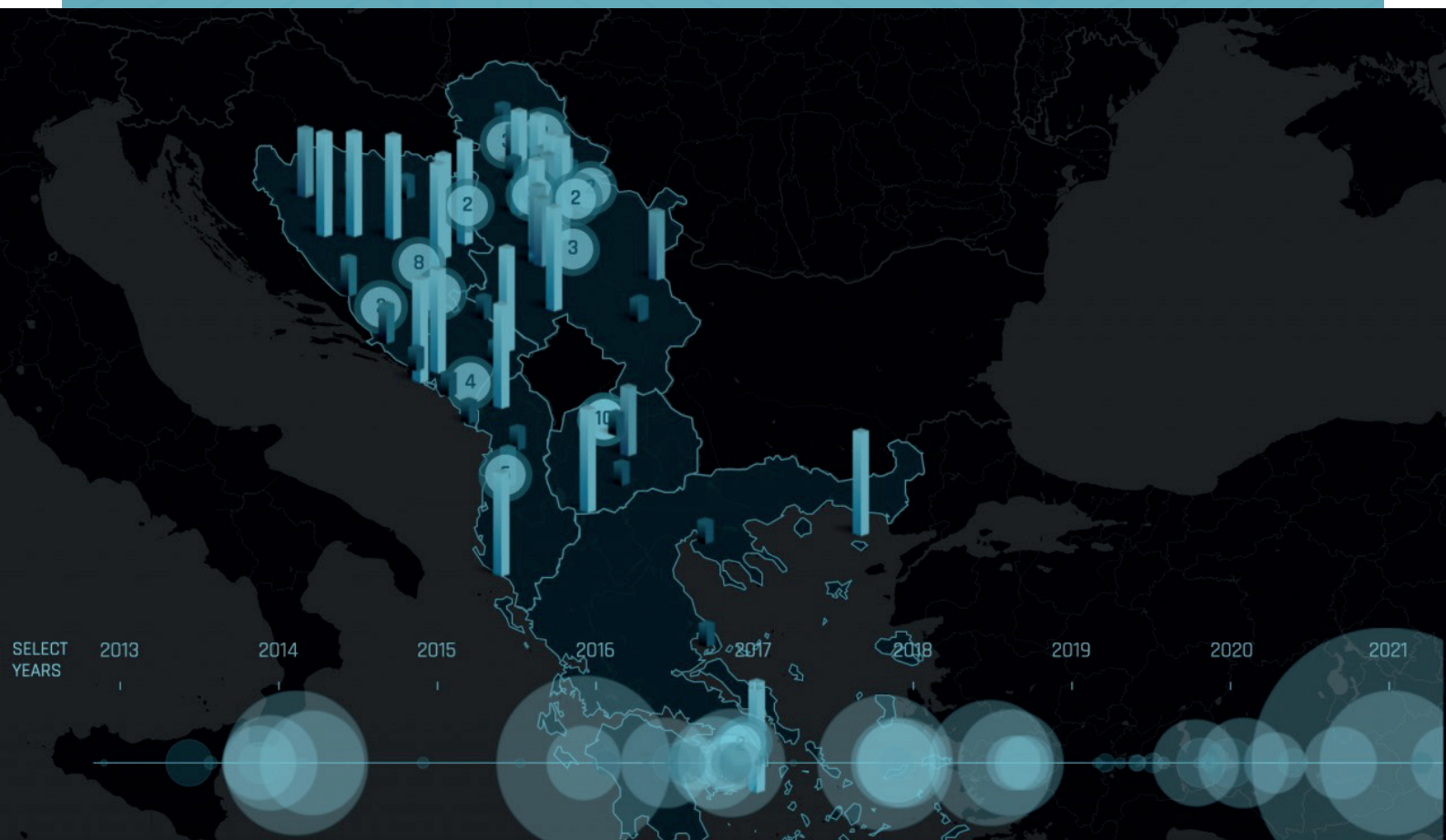


BSFocus 1

JULY 2025

CURRENT THREATS AND AREAS OF COOPERATION IN THE BALKANS IN THE CONTEXT OF CYBERSECURITY

Tolga Erdem



BSFocus 1

CURRENT THREATS AND AREAS OF COOPERATION IN THE BALKANS IN THE CONTEXT OF CYBERSECURITY

Tolga Erdem

iDEFE

Introduction

Although endowed with a profound historical and cultural heritage, the Balkans have been persistently marked by a climate of insecurity and instability, often manifesting in turbulent and disorderly dynamics. Seen from a geopolitical perspective, the Balkans clearly matter in terms of Europe's overall security. What happens in the region often shapes how stable the European Union (EU) can remain, so treating the two as separate is unrealistic. It is equally untenable to argue that the instability and conflict in the Balkans would remain without consequences for Europe at large and the broader international security framework. Hence, the Balkans represent a geostrategically significant nexus central to both European affairs and the wider international order. Their prominent status in the tangible geopolitical arena is poised to maintain equal significance within cyberspace, which constitutes the new operational domain of 21st century international relations.

In the current century, rapid technological change and widespread digital integration are reshaping virtually every dimension of human activity. Cyber issues in international relations have changed a lot and don't fit the old models anymore. With many different players active in cyberspace today, it's more complicated than ever to predict and control what happens on a global level. Considering the intricate and opaque

nature of cyberspace, the offensive and defensive capabilities and tools possessed by actors in cyber international relations may be increasingly favored as a testing ground for competition between major powers in a region such as the Balkans, which is plagued by instability and insecurity in the real world. Recent increases in cyberattack incidents within the Balkans substantiate this assessment. Therefore, the complete adaptation of the Balkans to global technological transformation and the establishment of a cybersecurity architecture across the region is essential for the national security of Balkan countries, EU security, and international security.

This study will examine the overall cybersecurity landscape in the Balkans, followed by an analysis of prominent cybersecurity threats in the region based on recent cybersecurity incidents. Ultimately, the study will highlight areas where cooperation needs to be developed. In today's world, where the impact of the digital domain on the physical world has reached unprecedented levels, a sensitive and fragile region like the Balkans requires even greater attention than ever before.

This study explores recent cyberattacks and threats in the Balkans to highlight potential areas for cooperation. This analysis provides a fresh perspective on the Balkans' role in cyberspace and the development of its cybersecurity. In doing so, it contributes meaningful insights to the broader academic conversation.

Fifth Domain of International Relations: Cyberspace and Security

It is clear that the shift initiated in contemporary international relations during the mid-20th century has progressively developed into a comprehensive transformation driven by information and technology in the early 21st century. Information now plays a significantly larger role in how countries and global actors interact, particularly through advancements in science and technology. This change has prompted many international relations scholars to reassess key theories by considering how science and technology are shaping today's global landscape. To such an extent that traditional concepts have been redefined within the cyber domain: Threats are now framed as 'cyber threats', weapons as 'cyber weapons', attacks as 'cyber attacks', wars as 'cyber wars', security as 'cybersecurity' and power as 'cyber power'. The traditional domains of power rivalry in international relations –land, sea, and air– have been expanded to include two novel domains: outer space and cyberspace. The ongoing competition within these emerging domains has produced significant and direct ramifications for the structure and functioning of the global international system. Cyberspace is now widely regarded as a new arena of international relations, often referred to as the 'fifth domain' (Rid, 2013). Its rise has challenged long-standing ideas about state

control, physical borders, and national sovereignty (Withers, 2015).

Moreover, the intersection of the physical and cyber realms has expanded the range and diversity of actors engaged in 21st century international relations (Choucri et al., 2012). Within this framework, cyberspace may be broadly conceptualized as a global networked environment wherein various information technology infrastructures – such as the Internet, computers, servers, and processors– are interconnected (Kuehl, 2009). Cyberspace is a rapidly evolving and complex domain where everything is interconnected globally. This unique nature brings both new security risks and opportunities (Choucri, 2012). Information now plays a significantly larger role in how countries and global actors interact, particularly through advancements in science and technology. Many experts in international relations are reevaluating long-held ideas as science and technology continue to transform the world. These changes speed up how quickly things evolve and make regions more connected and dependent on each other. This ongoing transformation, driven by fast technological progress and growing interdependence, is often referred to as 'complexity', a key characteristic of cyberspace (Dunn Cavelty, 2008). Within this complex cyber environment, cybersecurity encompasses any strategy, measure, or policy aimed at securely monitoring priority targets by accounting for both offensive and defensive actions of actors in the cyber domain, alongside safeguarding the confidentiality, integrity, and availability of information (Dunn Cavelty, 2025). The

cyber domain is complex and constantly evolving, rapidly connecting many aspects of the physical world. This creates real challenges for countries and other cyber actors, pushing them to develop stronger cybersecurity strategies and improve their attack and defense capabilities. The rapid growth of cyberspace now affects key issues in international politics. Still, states continue to be the main players in global affairs. Given their importance for security and stability, regions like the Balkans, where security challenges have long affected the EU, are likely to see increased use of cyber offensive and defensive tools. Additionally, the Balkans may be selected as a strategic arena for the testing of cyber capabilities amid rivalries among major powers within the cyber domain. Hence, the full adaption of the Balkans into technological transformation, alongside the formulation of effective cybersecurity strategies and the enhancement of cyber capabilities, is critically important for ensuring both regional stability and the broader framework of international security (Erdem, 2021).

Cyber Portrait of the Balkans

Whereas numerous Western European states have begun implementing national mechanisms to address the rising incidence of cyber threats, countries in the Balkan region appear to be trailing in the development and institutionalization of comparable response mechanisms. The escalating risks and cyber threats emerging from rapid digital transformation across

multiple sectors –ranging from public administration to banking, finance, industry, and critical infrastructure– underscore the inadequacy of operational and institutional frameworks in the Balkans, revealing the region’s limited capacity to effectively confront the disruptive challenges posed within the cyber domain. Estimates suggest that a cyberattack of moderate magnitude on a Balkan country could generate direct financial losses amounting to several million euros per day (Minović et al., 2016).

The European Commission’s introduction of the Digital Agenda for the Western Balkans in 2018 marked a strategic move to embed the region more deeply within the evolving digital order. While framed within the Western Balkans Investment Framework (WBIF), the initiative allocated €30 million in grants to six non-EU states– Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia. These funds aim to address persistent gaps in digital infrastructure, support sectoral modernization, and cultivate digital literacy and research potential. Nevertheless, the extent to which this agenda leads to sustainable digital integration is subject to broader structural and political dynamics (European Commission, 2018). Meanwhile, the emergence of the pandemic of the novel virus known as ‘coronavirus’ in 2019 has had a positive effect on the evolution of the cyber landscape of the Balkans. During this period, several Western Balkan countries, supported by EU funding, launched e-government projects to improve digital public services. Technological changes moved forward rapidly,

especially in healthcare, education, and public administration. At the same time, increasing internet access throughout the region helped speed up the move toward digitalization (Ördögh, 2023). Rapid technological progress is helping the Balkans grow socially and economically. Adapting to these changes not only supports economic growth but also makes everyday life better across the region. Nonetheless, the pronounced digital divide between rural and urban regions in the Balkans, alongside inadequate investment in infrastructure, hinders the full realization of technological transformation and the attendant benefits (Parežanin, 2024). The OECD (2023) report identifies digitalization as one of the five principal factors driving economic convergence as well as sustainable and inclusive growth within the Western Balkans. By 2023, the Western Balkans have shown promising progress in meeting EU standards in cyberspace, especially through improvements in digital infrastructure and technology. However, the region still lags behind when it comes to developing digital skills. Technological progress in the region appears to be driven primarily by the imperative to align with EU accession objectives; however, it is noted that the existing legal frameworks remain insufficiently developed to meet the desired standards (OECD, 2023). Consequently, while national strategies aimed at adapting to the cyber domain have been formulated –especially within Western Balkan states– the overall pace of advancement remains comparatively sluggish. Although the EU has provided financial support, efforts to improve IT education for citizens and invest in digital

infrastructure still fall short of expectations. As a result, the Balkans continue to lag behind the EU in developing a strong cyber presence. Weaknesses in cyber capabilities within the context of 21st century international relations generate a multitude of risks and vulnerabilities.

Current Cyber Threats in the Balkans

The COVID-19 pandemic accelerated digital transformation worldwide, transforming the way governments and companies operate. As a result, cyber incidents became more noticeable, and threats and attacks began to rise, involving a wider range of actors. Since 2020, the global cyber threat landscape has been dominated by a variety of high-impact attack vectors, including ransomware, zero-day exploits, commercial espionage operations, phishing, supply chain compromises, crypto mining malware, and intrusions targeting cloud-based infrastructures. In the context of the Balkans, this region is affected by global cyber actions in two ways: Firstly, rather than being subjected to directly targeted cyber-attacks, the Balkans are often affected by the collateral consequences of cyber-attacks that are disseminated globally. Secondly, prominent state and non-state actors in the cyber domain –most notably Russia and China– may exploit the region as a strategic testing environment to refine and project their cyber capabilities. Therefore, no direct specific interest of the major threat actors of cyber international relations towards various targets in the Balkan

geography has been recorded so far (PwC, 2022).

It can be posited that geopolitical tensions in the region are the predominant factor shaping cyber threats and cyber-attacks in the Balkans. Based on this understanding, the cyber security architecture of the Balkans can be understood through three dimensions: public institutions, media organizations, and critical infrastructure. Particularly in light of developments between 2020 and 2025, it becomes evident that the cyber threat landscape confronting the Balkan cybersecurity architecture has been marked by a steady intensification in both the complexity and frequency of malicious activities. In countries such as Bosnia and Herzegovina, Albania, Montenegro, North Macedonia, Kosovo and Serbia, there has been a notable increase in incidents of ransomware, data breaches, phishing and distributed denial-of-service (DDoS) attacks. These evolving threat patterns hold the potential to severely undermine fundamental societal pillars such as freedom, democracy, and social security. To address these challenges, regional authorities are developing a range of cybersecurity skills. Their efforts include creating new legal frameworks, establishing specialized technical teams, and developing detailed national cybersecurity strategies (Elshani, 2025).

Since 2020, reported cyber incidents worldwide have increased by more than 30%. This pattern is similarly discernible within the Balkan region. Let us briefly examine the prominent and recorded cyber incidents that have emerged in Balkan countries particularly after 2020:

During the parliamentary elections in North Macedonia in 2020, the Election Commission's digital platform experienced a temporary outage as a result of sustained DDoS attacks. Subsequently, in 2022, cyber-attacks orchestrated by a hacker collective identified as 'the Greek Hacking Team Net-watchers' targeted both the public services website and the Ministry of Education's online portal (Marusic, 2022). Between 2021 and 2022, Albania experienced several advanced ransomware and wiper attacks targeting critical infrastructure in both the government and private sectors. These attacks caused significant leaks or losses of confidential data. Attribution points to possible involvement by groups based in Iran and Russia (Oghanna, 2023). In 2022, Montenegro was targeted by cyberattacks that affected its transportation, telecommunications, and public services. Officials called these attacks the most extensive and complex the country has faced. These aggressive intrusions precipitated extensive service outages nationwide, with evidence suggesting that the principal objective was the state-owned energy enterprise, EPCG (Reuters, 2022). As noted by Kurtic (2023), Bosnia and Herzegovina experienced a surge of over 9.2 million cyberattacks in November 2022, directed at a broad spectrum of targets nationwide. Around one-third of these incidents were DDoS attacks, mainly aimed at government agencies and media institutions. In 2022, Serbia was hit by a series of cyber intrusions that put sensitive public-sector data at risk and threatened key parts of its energy infrastructure. Official reports show that these breaches exposed citizens' data without authorization

(Elshani, 2025). In 2022, Bulgaria suffered a major DDoS attack, believed to have been carried out by groups connected to Russia. The assault targeted the digital infrastructure of several high-level governmental bodies, including the Presidency and the Ministries of Interior, Defense, and Justice (Paganini, 2022). In the latter half of 2022, Greece witnessed a marked escalation in ransomware and DDoS attacks targeting a wide array of sectors— including health-care, finance, transportation, and critical segments of both the production and service industries. In light of the scale and intensity of these cyber incidents, Greek decision-makers enacted the establishment of a National Cybersecurity Authority as a strategic institutional response (Stamatoukou, 2023). In 2022, Slovenia documented cyberattacks directed against its Ministry of Defence and national police agency. The following year, the country's leading electricity provider faced a series of cyberattacks. Some sources pointed to China, though details remain unclear. These were among the most serious digital incidents the country had seen. Luckily, most systems stayed online, and major disruptions were avoided (Francesca, 2023). In 2024, Croatia's largest hospital —along with several banks, beverage producers, and chemical companies— was targeted in a series of well-planned ransomware attacks. These breaches temporarily disabled their IT systems, as noted in official reports (Tesiya, 2024).

Recent cyber incidents in the Balkans demonstrate that cyber threats transcend simple electronic system disruptions; they

are strategically designed to capitalize on operational vulnerabilities for economic advantage, gather intelligence advantageous to specific interest groups, and foment widespread societal fear, panic, and disorder. Within this framework, international data shows that the main global cyber threats are DDoS attacks, which block access to services, and data breaches that compromise data privacy (Ceko, 2024). Likewise, the Balkans have recently experienced a significant increase in DDoS attacks, phishing attacks, and ransomware incidents. The COVID-19 pandemic induced acceleration of technological transformation has substantially broadened the cybersecurity threat landscape across the Balkan region, with regional authorities documenting a marked escalation in the frequency of detected cyberattacks. This consistent rise in cybercrime within the Balkans constitutes a predominant factor shaping the threat environment of the region's cybersecurity architecture (PwC, 2022). Building cybersecurity in the Balkans' complex digital environment hinges on forming strong, focused partnerships at both national and regional levels. These efforts should reflect the specific needs and structural realities of each country involved.

Cooperation Areas

Cyber incidents have clearly been on the rise across the Western Balkans in recent years, and this isn't an isolated trend. It reflects a wider global shift where cyberspace has moved to the heart of international politics. Some now even call it the

fifth domain of global rivalry. The problem is that the region isn't well-prepared to handle this shift. Political systems are often fragmented, resources are tight, and digital governance remains patchy at best. This makes the Balkans especially susceptible to cyber threats that go beyond technical disruption, they are usually laced with political messages and strategic intent. Governments can no longer wait to respond only after cyberattacks happen. They must build strong cybersecurity strategies from the ground up and make them a core part of how the country is run. This requires better cooperation, more innovative use of resources, and a mindset change—viewing cybersecurity as essential, not a luxury. A weakened cybersecurity architecture in the Balkans equates to a diminished strategic posture of the region's states within the broader global security order (RegTech, 2025). In this context, moving faster on both regional and international cooperation is essential. Working together across borders makes cyberattacks less likely to succeed and helps ease the damage when they do happen. A clear example of this was seen in Albania in 2022 when the government collaborated with Microsoft and the FBI to mitigate the impact of a major cyberattack (Elshani, 2025).

At the same time, there's still a real need for Balkan countries to take cybersecurity more seriously within their technical systems. That means putting better rules in place and developing national strategies that actually work on the ground. Although many governments in the region have drafted such plans, these efforts often come as

reactions to outside pressure –mainly from the EU and other global actors– rather than from internal priorities. Cybersecurity reforms in the Balkans should originate from within the region rather than being imposed from outside. For these efforts to be sustainable and contextually relevant, local actors must take ownership and shape reform processes in line with their institutional realities and strategic priorities. In parallel, the region would benefit from the establishment of dedicated operational units, improved coordination among key stakeholders, stronger political engagement on cyber matters, and the development of cross-sectoral collaboration capacities (Minović et al., 2016).

It's still challenging to get people in the Balkans to understand the importance of cyberspace fully. One practical step would be to introduce steady, long-term education on cybersecurity. This kind of effort can grow local know-how and give people the tools they need to handle digital threats better. In this process, the EU and NATO have a central role to play, with international tech companies also in a good position to offer support (Zweers et al., 2025).

Conclusion

The Balkans hold a fragile place in today's global security environment. Its long history of unrest has made it hard to build and sustain peace. Deep divisions –social, political, and cultural– continue to challenge efforts to create lasting political trust. As a result, 'instability', 'tension', and 'conflict' remain central features of the region. The

performance of such a troubled geography in adapting to the technological transformations occurring within 21st century contemporary international relations is anticipated to have direct implications not only for the security and stability of the Balkans themselves but also for global power dynamics. Indeed, the primary arena of the modern international system has shifted into cyberspace –widely recognized as the ‘fifth domain’– where actors, actions, policies, strategies, and capabilities increasingly redefine and reconstruct the global balance of power. In today’s world, virtually all facets of human activity have been inextricably integrated into this digital domain. What is even more striking is the irreversible nature of this transformation. For these reasons, one of the foremost prerequisites for becoming a strong, secure, and stable actor in 21st century international relations is the ability to project strength, security, and stability within cyberspace itself.

Technology and digitalization have advanced rapidly, particularly since the COVID-19 pandemic began in 2020. This has caused a noticeable rise in cyber incidents around the world. The Balkans have seen a similar trend, which has drawn a lot of attention. Due to the region’s long history of conflict, there is growing concern that similar instability could spill over into the digital space, posing even greater risks. Most cyberattacks recorded thus far in the Balkans have not directly targeted the countries themselves. It appears that key global cyber powers have repeatedly used the Balkans as a testing environment for both offensive and defensive cyber operations.

Although the region has not yet experienced the most severe consequences, its overall cyber posture still requires serious and immediate improvement. Across Balkan countries, the most prevalent forms of cyber threats and attacks have been identified as DDoS attacks, phishing attacks, and data breaches. Critical infrastructures, particularly in the industry and energy sectors, frequently face cyberattacks. These threats show serious weaknesses. Cyber risks in the region are hard to ignore now. Leaders need to act more to prevent lasting damage. The difference between digital attacks and real-life effects is getting harder to see. Looking at the Balkans’ cybersecurity situation, it’s clear that many decision-makers still don’t fully grasp how serious these emerging threats are. The line between digital and physical consequences is already beginning to blur. A closer examination of cybersecurity in the Balkans reveals that many leaders still do not fully comprehend the severity of emerging digital threats. Digital governance rarely tops the list for governments, and action typically comes only after a serious issue arises.

Strengthening cybersecurity across the Balkans isn’t just a technical task; it should be part of the region’s long-term strategic thinking. Although some countries have put national strategies in place, many of them still struggle to turn plans into practice due to coordination and capacity issues. International actors –especially the EU and NATO– have launched targeted efforts to support cybersecurity development in the region. But for these efforts to be truly effective, Balkan governments

need to view them not just as sources of funding but as opportunities to strengthen the digital foundations of national sovereignty in an increasingly contested cyberspace. Many people in the Balkans still lack the digital skills needed to navigate today's increasingly connected world. Changing this will take time, as building a stronger digital mindset across societies doesn't happen overnight. At the same time, cooperation between countries on cybersecurity matters has not yet reached its full potential. Better infrastructure, enhanced training for professionals, and easier ways to share knowledge could have a tangible impact if backed by steady effort and long-term thinking. Public education

and well-prepared cyber response centers would also help, especially when they are part of a broader plan to raise awareness and strengthen resilience across society.

To summarize, cyberspace continues to expand and become increasingly complex. This development is permanent, and everyone involved needs to recognize its importance and respond thoughtfully. The deliberate construction of a 'secure', 'informed', and 'stable' cyber environment in the Balkans –serving as a digital counterpart to the region's entrenched physical 'insecurity'– is critically vital to regional, national, and global security architectures.

REFERENCES

- Ceko, E. (2023). On Relations Between Cyber Security Index and ISO 27001 Standard Index In Western Balkan Countries. *CRJ*, November Issue, 12-17.
- Choucri, N. (2012). *Cyberpolitics in International Relations*, 1st Edition, Massachusetts: The MIT Press.
- Choucri, N. & Goldsmith, D. (2012). Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security. *Bulletin of Atomic Scientists*, 68(2), 70-77. <https://doi.org/10.1177/0096340212438696>
- Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts To Secure The Information Age*, 1st Edition, New York: Routledge.
- Dunn Cavelty, M. (2025). *The Politics of Cyber-Security*, 1st Edition, New York: Routledge.
- Elshani, D. (2025). *Navigating The Evolving Threat Landscape and Institutional Responses To Cybersecurity In The Western Balkans*, Reporting Digital Rights and Freedoms, Bosnia and Herzegovina, Sarajevo: Balkan Investigative Reporting Network (BIRN).
- Erdem, T. (2021). Balkanlarda Siber Güvenlik: Politikalar ve Stratejiler Üzerine Bir Değerlendirme. A. Hüseyinoğlu (Ed.) *Balkan Siyaseti ve Uluslararası İlişkiler Araştırmaları I* içinde (pp. 29-56). Edirne: Trakya Üniversitesi Balkan Araştırma Enstitüsü Yayınları.
- Francesca. (2023, November 29). Slovenia Suffers Significant Cyberattack – Barrier Networks Responds. *Security On Screen*. <https://securityonscreen.com/barrier-networks-slovenia-cyberattack/>
- Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. F. D. Kramer, S. H. Star & L. K. Wentz (Eds.), *Cyberpower and National Security* içinde (pp. 24-42). 1st Edition, Washington D.C.: Potomac Books.
- Kurtic, A. (2023, April 14). Bosnia Lacks Capacity to Fight Millions of Cyber Attacks Monthly, Report Warns. *BalkanInsight*, <https://balkaninsight.com/2023/04/14/bosnia-lacks-capacity-to-fight-millions-of-cyber-attacks-monthly-report-warns/>
- Marusic, S. J. (2022, September 13). North Macedonia Warned Over Cyber Safety amid Ongoing Attack. *BalkanInsight*, <https://balkaninsight.com/2022/09/13/north-macedonia-warned-over-cyber-safety-amid-ongoing-attack/>
- Minović, A., Abusara, A., Begaj, E., Erceg, V., Tasevski, P., Radunović, V. & Klopfer, F. (2016). *Cybersecurity in the Western Balkans: Policy Gaps and Cooperation Opportunities*, Cybersecurity Capacity Building and Research Programme for South-Eastern Europe Project Research Report, Geneva: DiploFoundation.
- OECD. (2023) Economic Convergence Scoreboard for the Western Balkans 2023. No. 2023/01, Paris: OECD Publishing, <https://doi.org/10.1787/2f4b0366-en>
- Oghanna, A. (2023, March 25). How Albania Became a Target for Cyberattacks. *Foreign Policy*, <https://foreign-policy.com/2023/03/25/albania-target-cyberattacks-russia-iran/>
- Ördögh, T. (2023). Digitalisation in the Western Balkans. *AARMS*, 22(3), 91-107. <https://doi.org/10.32565/aarms.2023.3.6>
- Paganini, P. (2022, October 17). Bulgaria Hit By A Cyber Attack Originating From Russia. *Security Affairs*, <https://securityaffairs.com/137230/hacking/bulgaria-hit-cyber-attack-russia.html>
- Parežanin, M. (2024). Bridging Progress: Digital Transformation in the Western Balkans. *Digitalization and Democracy in the Western Balkans*, Aspen Western Balkans Initiative, Berlin: Aspen Institute, 32-41.
- PwC. (2022). *Cybersecurity Ecosystem Report*, Western Balkans: Emerging Cyber Threats, Serbia: International and Security Affairs Centre (ISAC).
- RegTech. (2025). Western Balkans Cybersecurity: Digital Sovereignty Questioned. <https://reg-tech.co/2025/02/24/western-balkans-cybersecurity-digital-sovereignty/>

- Reuters. (2022, August 26). Montenegro's State Infrastructure Hit By Cyber Attack –Officials. <https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/>
- Rid, T. (2013). *Cyber War Will Not Take Place*, 1st Edition, New York: Oxford University Press.
- Stamatoukou, E. (2023, December 11). Greece Moves to Enhance Cyber Security Amid Frequent Attacks. *BalkanInsight*, <https://balkaninsight.com/2023/12/11/greece-moves-to-enhance-cyber-security-amid-frequent-attacks/>
- Tesija, V. (2024, June 5). Wave of Ransomware Attacks is Wake-up Call for Croatia: Expert. *BalkanInsight*, <https://balkaninsight.com/2024/07/05/wave-of-ransomware-attacks-is-wake-up-call-for-croatia-expert/>
- The European Commission. (2018, June 25). European Commission launches Digital Agenda for the Western Balkans. Brussels: Press Release, IP/18/4242, https://ec.europa.eu/commission/presscorner/detail/en/ip_18_4242
- Withers, P. (2015). What is the Utility of the Fifth Domain?. *Royal Air Force Air Power Review*, 18(1), 126-150.
- Zweers, W., Ryck, J. & B. Šliogerytė. (2025). *Security and Stability Scenarios for the Western Balkans: Are the EU, NATO and the Netherlands Prepared?*. Clingendael Report, Netherlands Institute of International Relations 'Clingendael'.

BSF Center for Political, Economic and Social Research is the center of Balkan Studies Foundation based in Skopje. Our mission is to help societies and governments build a sustainably justice, equality, development and regional cohesion.

All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder.

Please direct all enquiries to the publishers.

BSF Center for Political, Economic and Social Research does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Copyright © IDEFE, 2025

Editor: Sevba Abdula

Editorial Board: Bujamin Bela, Dilek Kütük, Mustafa Işık, Enes Turbić

Coordinator: Hanife Etem, Şengül İnce

Design: iyicalismalar.tr

Printed by: Ajgraf

Cite this paper:

Erdem, T. (2025), Current Threats and Areas of Cooperation in the Balkans in the Context of Cybersecurity, BSF Focus, Skopje: IDEFE Publications.

Dr. Tolga Erdem is an academican currently serving as a Research Assistant in the Department of International Relations at the Faculty of Economics and Administrative Sciences, Trakya University, located in Edirne, Turkey. He has been affiliated with the university since 2014 and earned his Ph.D. in International Relations from Trakya University's Social Sciences Institute in 2020. Dr. Erdem's academic work is primarily focused on international security, with particular emphasis on the intersection of technology and global politics. His research interests include cybersecurity, artificial intelligence, autonomous weapon systems, space politics, water security, biosecurity, and the broader implications of emerging technologies within international relations. Throughout his academic career, Dr. Erdem has authored and co-authored numerous scholarly articles published in national and international journals. Notable among his contributions are studies on the disarmament of autonomous weapons under the United Nations framework, the role of artificial intelligence in diplomacy, and the emerging field of astro-politics. His publications reflect a multidisciplinary approach, combining classical theories of international relations with contemporary technological and security challenges. Dr. Erdem contributes as a reviewer for various academic journals on platforms such as Dergi Park. He remains actively engaged in academic networks and continues to develop projects that explore the impact of science and technology on global governance and security.

BSF | B | A | L | K | I | A | N |
S | I | T | U | D | I | E | S |
F | O | U | N | D | A | T | I | O | N