FRIEDRICH EBERT STIFTUNG

POLITICAL TRENDS & DYNAMICS

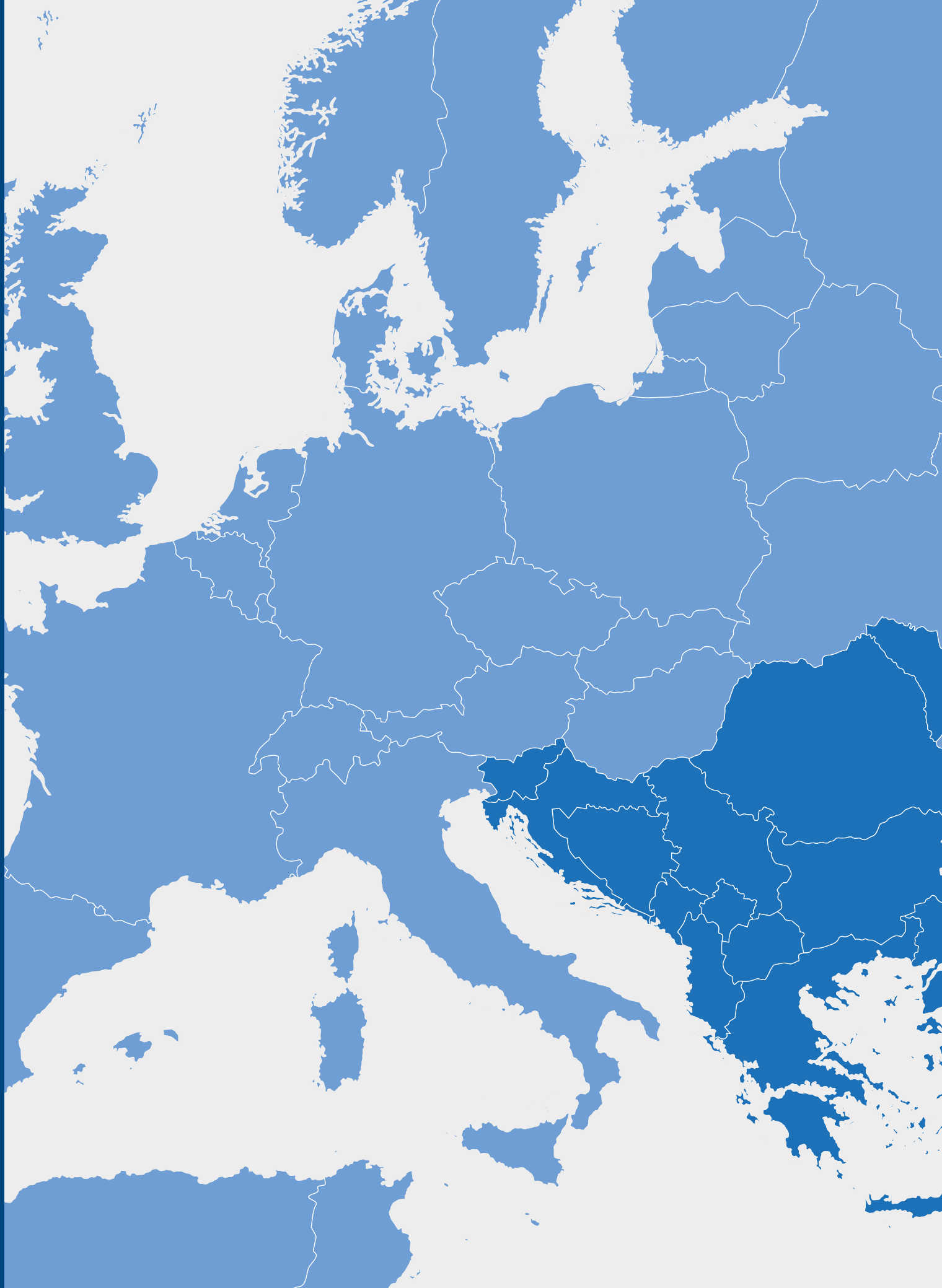
CYBER SECURITY IN SOUTHEAST EUROPE: PAST, PRESENT, AND FUTURE

BRIEFING

Volume 2 | 2023

SEE Dialogue South-East Europe

FRIEDRICH-EBERT-STIFTUNG



EDITORIAL

In our modern society, the internet and cyberspace have assumed an irreplaceable role in various aspects of our daily lives, serving as the backbone for public and private services, as well as facilitating our daily interactions. As a result, our collective security is intricately intertwined with the seamless functioning of cyberspace, leaving us susceptible to an array of risks, including but not limited to data breaches, ransomware attacks, and instances of cyber violence. Responding to this evolving landscape, both the European Union (EU) and the United States (US) have embarked on proactive initiatives to expedite the establishment of a comprehensive regulatory framework. This framework is designed to confront a diverse array of challenges that span from national security concerns, exemplified by the NIS2 Directive aiming to fortify cybersecurity across the EU, to the preservation of fundamental rights, as addressed by the EU Digital Services Act.

Authorities in Southeast Europe have displayed obvious inertia in confronting cybersecurity challenges, despite the region's geographic proximity to Eastern Europe, where significant cyberattacks, often originating from Russia, have been documented for years – such as the infamous 2007 cyber onslaught against Estonia and the ongoing cyber campaigns targeting Ukraine since 2014.

Nonetheless, the landscape has taken an abrupt turn as Southeast Europe itself has fallen prey to severe and disruptive cyberattacks in recent times. These incidents, which occurred in several countries including Albania, Montenegro, and Bosnia and Herzegovina in 2022, have cast an unwavering spotlight on the region's vulnerabilities. They have further underscored the region's delicate geopolitical positioning within the broader international context. The pressing question now centers on whether this newfound realization will galvanize these nations into hastening their reform efforts and, if so, what precise measures are imperative for bolstering their cybersecurity resilience.

In this edition, our objective is to analyze and assess the contemporary cybersecurity threats that directly impact Southeast Europe and the broader Eastern European region, as well as to to evaluate the preparedness of these nations in addressing the assorted challenges that loom on the digital horizon.

In this issue, Valentin Weber initiates us into the intricate experiences of Ukraine, Moldova, and Georgia in grappling with the pervasive threat of cyberattacks. His analysis examines the different dimensions to these cyber-attacks, and the responses of multiple actors. Robert Mikac and Predrag Puharić provide an in-depth exploration of the cybersecurity capacities and limitations of Croatia and Bosnia and Herzegovina, accompanied by a strategic roadmap for enhancing their cybersecurity prowess. Furthermore, Megi Reci presents the compelling case of Albania – a unique story that spotlights the perils and consequences entailed by a sweeping government-led digital transformation. Her analysis in particular underscores the profound impact of this transformation on social and human rights within the nation.

The authors of this publication offer a comprehensive set of strategic recommendations intended to chart a coherent path forward for the countries of Eastern and Southeast Europe. These recommendations are the culmination of an exhaustive analysis of the prevailing cybersecurity landscape in the region, considering the challenges that have been painstakingly delineated in the preceding articles. The overarching aim is to empower these nations to fortify their digital defenses, safeguard their national interests, and ensure the well-being of their citizenry as we collectively navigate an increasingly interconnected digital territory.

Vivien Savoye, Ioannis Armakolas and Alida Vračić

CONTENTS OF THIS ISSUE

CYBERSECURITY CHALLENGES IN THE WESTERN BALKANS: A LOOK INTO SOLUTIONS AND CONCERNS

Predrag Puharić

Predrag has over 20 years of experience in cybercrime, cyber forensics, and cyber security. He is leading the establishment of the Cyber Security Excellence Centre and Academic CSIRT facility, and recently served as a national consultant for EGA EU-funded cybersecurity identification and formulation study in the Western Balkans. He also was a part of the international consultant team for UNDP support for the CIAT project as a Data Collection expert.

KEY TAKEAWAYS

The Western Balkans region is grappling with an increasing threat from cyber-attacks, impacting critical infrastructure and government entities. A significant challenge is the absence of a unified governance framework for cybersecurity, making cross-border defence difficult. Bosnia and Herzegovina, for example, lacks a national cybersecurity strategy and centralized threat response entity. The Cyber Security Excellence Centre (CSEC) in Sarajevo is striving to bridge this gap by offering expertise and serving as a functional CERT. To counteract these threats, the region needs unified cybersecurity measures, investments in expertise, and enhanced public awareness.

> **In addition to cybercrime, the Western Balkans is also facing a threat from nation-state actors**

The Western Balkans region is facing a growing threat from cyber-attacks. In recent years, there have been a number of high-profile attacks on critical infrastructure, government agencies, and businesses in the region. These attacks have caused significant damage and disruption and have raised concerns about the region's cybersecurity resilience.

One of the key challenges facing the Western Balkans in terms of cybersecurity is the lack of a unified governance framework. Each country in the region has its own set of cybersecurity laws and regulations, which can make it difficult to coordinate a response to cross-border attacks. In addition, there is a lack of resources and expertise in many countries, which makes it difficult to effectively defend against cyber threats. Bosnia and Herzegovina in particular, exemplifies these challenges. The country lacks a national or state-level cybersecurity strategy and a related legal framework. Furthermore, there's no national CERT (Computer Emergency Response Team) or centralized point of contact for cyber threat intelligence sharing. This deficiency impacts not only inter-team communication within Bosnia and Herzegovina and with other regional teams but also the timely dissemination of advisories to the public.

One of the key initiatives to improve cybersecurity in Bosnia and Herzegovina, as the Western Balkans stance should also benefit from this, is the establishment of the Cyber Security Excellence Centre (CSEC). The Cyber Security Excellence Centre is an organisation based in Sarajevo that provides an academic approach to cyber security as well as training, support, and awareness. It is also the only currently functional CERT in Bosnia and Herzegovina, especially focused on academia, independent media and civil society. It plans to serve as a national CERT-of-last-resort until an official national CERT is established. The Cyber Security Excellence Centre helps to improve the coordination and cooperation between teams in the country and greater region, which should make the region more resilient to cyber-attacks.

Another challenge is the proliferation of cybercrime in the region. The Western Balkans has experienced a rise in cybercrime incidents with organised criminal groups operating from countries like Albania, Kosovo, and Montenegro. These groups are often well-funded and sophisticated, and they pose a significant threat to the region's cybersecurity.

In addition to cybercrime, the Western Balkans is also facing a threat from nation-state actors. Countries like Russia and China have been accused of carrying out cyber-attacks against the region to steal sensitive information or disrupt critical infrastructure.

Data from the 2022 annual report of the Cyber Security Excellence Centre highlights the cybersecurity vulnerabilities in Bosnia and Herzegovina. In a span of just one month, from November 17th to December 17th, 2022,

> **Despite these challenges, there are several steps that the Western Balkans can take to improve its cybersecurity posture**

the country witnessed over 9.2 million cybersecurity threats, with DDoS attacks being the most common. This alarming figure, coupled with recent institutional audit reports reveals the absence of a strategic and legal framework for cybersecurity in BiH, and underscores the significant risks facing its citizens, businesses, and crucial sectors like law enforcement, the economy, energy, health, and education.

Interestingly, the Centre's records pinpoint Brazil as the primary source of these cyberattacks, followed by countries such as the Netherlands, USA, Russia, Bangladesh, Germany, China, and Costa Rica. Although initial data suggested that the majority of attacks originated from the Netherlands and Germany, the Centre believes this might be misleading. It's assessed that attackers often employ Virtual Private Networks (VPNs) to obfuscate their true locations, making it appear as though attacks are coming from elsewhere. Worryingly, many of these attack patterns are in line with tactics and techniques associated with nation-state actors like Russia and China.

Despite these challenges, there are several steps that the Western Balkans can take to improve its cybersecurity posture. One of the most important steps is to establish a unified cybersecurity governance framework or at least to harmonise responses and procedures. This would help to ensure that all countries in the region are working together to protect themselves from cyber threats. In addition, the region needs to invest in resources and expertise to improve its ability to defend against cyber-attacks. Finally, the region needs to raise awareness of cybersecurity threats among businesses and individuals.

If a cyber-attack targets a critical infrastructure facility in one country, it may be difficult for the authorities in that country to get the cooperation of the authorities in other countries to investigate the attack and bring the perpetrators to justice.

A unified cybersecurity governance framework would help to address this challenge by providing a common set of rules and procedures for all countries in the region to follow. This would make it easier for countries to cooperate in the event of a cyber attack, and it would help to ensure that all countries are taking the necessary steps to protect themselves from cyber threats.

Initiatives such as the Bosnian and Herzegovinian Cyber Security Excellence Centre or Serbia's Cybersecurity network foundation are a positive step towards improving cybersecurity in the Western Balkans. However, there is still much work to be done. The Western Balkans also needs to invest in resources and expertise to improve its cybersecurity posture. This includes investing in training for cybersecurity professionals, developing

cybersecurity tools and technologies, and establishing cybersecurity research centres such as the Cyber Security Excellence Centre.

Finally, the Western Balkans region needs to raise awareness of cybersecurity threats among businesses and individuals. Many people in the region are not aware of the risks posed by cyber-attacks, and they do not take the necessary steps to protect themselves. This includes using strong passwords, keeping their software up to date, and being careful about what information they share online.

It is a region with economic challenges, and it may be difficult for countries in the region to afford to invest in cybersecurity. However, it is important to remember that the cost of not investing in cybersecurity can be much higher. A major cyber-attack could cause significant damage to a country's economy, and it could also lead to loss of life as happened in the first known such case when hackers disabled computer systems at Düsseldorf University Hospital and a patient died while doctors attempted to transfer her to another hospital.

The Western Balkans has significant growth potential and a promising future. Despite this, it faces numerous challenges, including the looming threat of cyberattacks. By enhancing its cybersecurity posture — through strengthening educational programs, improving incident response capabilities, and deepening the trust between countries for better regional cooperation — the Western Balkans can ensure it remains a safe and vibrant place for residents and businesses alike.

Technical terms

- **Cybersecurity governance**: The set of policies, processes, and structures that are used to manage cybersecurity risks.
- **Critical infrastructure**: Systems and assets that are essential to the functioning of a society or economy.

Key words

- **Cyber threat**: Any action that could exploit a vulnerability in a computer system or network to cause harm.
- **Cybersecurity best practices**: Guidelines for protecting computer systems and networks from cyber threats.
- **CERT**: A Computer Emergency Response Team is an organization that is responsible for responding to and mitigating cyber incidents.
- **DDoS**: Distributed Denial of Service attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic
- **Virtual Private Networks (VPN)**: a service that allows users to securely connect to the internet by encrypting their data and routing their connection through a server, often to mask their location or access restricted content.

References

- Enhancing cybersecurity governance in the Western Balkans: https://www.dcaf.ch/enhancing-cybersecurity-governance-western-balkans
- Cybersecurity Study on the Western Balkans: https://ega.ee/project/cybersecurity-study-western-balkans/
- Cybersecurity and human rights in the Western Balkans: mapping governance and actors: https://www.dcaf.ch/cybersecurity-and-human-rights-western-balkans-mapping-governance-and-actors
- Bosnia and Herzegovina Cyber Security Threat Assessment - March 2023: https://www.csec.ba/threat-info

INTERVIEW

Valentin Weber

Dr. Valentin Weber is a Senior Research Fellow at the German Council on Foreign Relations (DGAP) and a China Foresight Associate at LSE IDEAS, the foreign policy thinktank of the London School of Economics and Political Science

Ukraine, Moldova, and Georgia have been the targets of Russian influence and destabilization campaigns for years. What exactly did these cyber operations look like and what were their effects? Were these countries able to build up their resistance capacity? What risks exist today?

Major DDoS attacks (malicious behavior that aims to overwhelm target servers with considerable internet traffic), targeted Georgian state websites in 2019. They were attributed to Russia's military intelligence agency, the GRU. As a result, many government websites were unavailable during the attack period. These types of attacks are seen as low in sophistication and can be mitigated. It appears that Georgia has not yet built sufficient resistance capacity. Estonia, for instance, experienced large scale DDoS attacks in 2007, which resulted in cash machines and government email services being disrupt-

> **Many sectors have chronically underinvested in cybersecurity, since security investments do not bring profit**

ed among other services. In 2022, Estonia was again targeted through considerable DDoS attacks, but websites were only disrupted minimally due to Estonian cyber resilience. Moldova too, experienced large-scale attacks since Russia's renewed invasion of Ukraine in 2022. Russian activities weren't limited to DDoS attacks but also included hack and leak operations against Moldovan officials who were to be discredited through disinformation.

Ukraine has experienced every imaginable type of cyberattacks against targets that included the energy grid, banking sector, transportation and military. This constant exposure to Russian malicious actors, has given Ukraine considerable experience in knowing their tactics and techniques. Recently Ukrainian counterintelligence units disrupted a cyber operation by Russian military intelligence who were using and subverting captured Ukrainian military Android devices to further their military goals.

Sizeable Russian cyber risks remain for all three countries today and they do not relate to physical destruction. Recent years have shown that cyberspace is not well-suited for destructive effects, but rather for gathering intelligence that can in turn further Russia's aims (i.e. leaking of data, informing Russian military decisions).

When we think of cyber-attacks, we often think about the state apparatus, but the private sector, civil society, and media are also vulnerable. Have these sectors adapted to protect themselves? How so?

Many sectors have chronically underinvested in cybersecurity, since security investments do not bring profit, but rather prevent loss. I see the major danger in privately-owned critical infrastructure that is vital to the functioning of society, I'm thinking here of the electrical grid especially, which is highly interconnected across Europe and where a malicious cyber operation could cause cascading effects across countries, but also across critical infrastructure sectors. All other critical infrastructure sectors rely on the electricity grid to operate. We would think that those most vital entities are well prepared, but in the past investigators found malware in Germany's

> Cyber espionage operations often serve as enablers of disinformation campaigns

nuclear power plants and the successful attacks against the Ukrainian power grid and the US's Colonial Pipeline have shown that most systems remain vulnerable. The EU has made stricter security guidelines obligatory and will punish non-implementation through penalties with its new NIS2 Directive. Hence critical sectors will need to improve their security. I do not yet see significant improvements made to smaller entities of the private sector and civil society either. Those entities lack the financial means and personnel to improve security. This weakness has been exploited by ransomware groups, which resulted in a true pandemic of attacks in recent years.

How would you describe the relationships between cyber-attacks and disinformation campaigns?

Cyber espionage operations often serve as enablers of disinformation campaigns. Genuine information is often gathered during clandestine operations and then mixed with false data, thereby providing a veil of authority to disinformation. Those operations are known as hack and leak operations. How do we combat these operations? Germany acted exemplarily in 2021. A few weeks before the German Federal Elections, which took place at the end of September 2021, Germany made suspected Russian cyber attempts, that were intended to gain information on German lawmakers public, and condemned them. Germany could have notified Russia about its concerns only in private, but it decided against this option. This act of public pre-bunking (alerting the public of information before it is released) has been successful. It appears that surrounding these elections, no major Russian influence operation took place. Pre-bunking is especially valuable as it breaks the relationship between cyber operations and disinformation campaigns by exposing malicious behavior to citizens.

Countries such as Estonia, a member of NATO, have been the target of cyberattacks by Russia since at least 2007. How have Western allies responded to these threats, and have they upgraded their capacity to defend against cyber operations since the Russian invasion of Ukraine?

In response to Estonia removing a statue representing a Russian soldier in Tallinn in 2007, Russia launched DDoS attacks, against the Estonian parliament, media and banks. NATO member states responded by establishing the NATO Cooperative Cyber Defence Centre of Excellence

(CCD COE) in Tallinn. In Estonia's capital, CCD COE member states gather each year for the world's largest cyber defense exercise, also known as Locked Shields. These annual meetings help with preparing for potential cyber events by simulating likely scenarios. The center also offers trainings and research on the most pressing topics and helps with increasing interoperability in cyber defense. Since the Russian invasion of Ukraine, Kyiv joined the CCD COE as a contributing participant, thereby joining a handful of mostly non-NATO countries that do not have full membership of CCD COE, e.g. Austria, Japan, South Korea, Switzerland, and closely works with the center to improve cyber defense capabilities.

Southeast Europe has also been the target of several cyber-attacks in recent years and their resistance infrastructure is desperately lacking. What lessons could the region learn from Ukraine, Moldova, and Georgia?

One of the most valuable lessons for Southeast Europe and other regions, has to do with the defense multiplier that international cooperation can bring. International partners and the private sector have added man- and woman power to the defense of countries that are under attack. During times of crisis, cyber defenders are constantly on alert and any additional support is vital. In the case of Ukraine, international cooperation extended in several areas beyond human resources. This includes giving Kyiv the opportunity to run servers abroad that host vital government data, thereby making Russian missile strikes on data centers inside Ukraine's less effective. As a result, the Ukrainian government was able to continue providing crucial services to its population. This value of international cooperation is not unidirectional. All sides in such partnerships gain by sharing threat intelligence for instance, such as information on Russian malicious cyber actors. In some cases, malware can be found in Georgia or Moldova that is not yet found elsewhere and vice versa. An early sharing of threat activities in one geographical region can help fend off the same threat in other geographical areas.

ALBANIA'S DIGITAL TRANSFORMATION: UNRAVELING INEQUALITIES AT THE INTERSECTION OF CYBERSECURITY AND HUMAN RIGHTS

Megi Reçi

Megi Reçi is a researcher on governance and civic space at the Institute for Democracy and Mediation (IDM), the Officer of the Civic Space Program and part of the Western Balkans Cybersecurity Research Network. She is a lawyer and holds a Master of Science in Public Law.

KEY TAKEAWAYS

In the era of swift digitalisation, human rights risks emerge as a crucial concern. To address these risks, governments must ensure transparent, inclusive, and evidence-based policy-making processes, especially regarding digitalization and cybersecurity, while actively addressing human rights implications. This article highlights the impact of digitalising public services on specific groups in Albania, shedding light on the potential deepening of existing inequalities when cybersecurity and human rights are treated as separate issues.

Over the past years, Albania has undergone a rapid process of digital transformation. This culminated in May 2022 when the government decided to streamline service delivery by transitioning 95% of public services to an e-government platform known as *e-Albania*. This digital shift, however, occurred without prior comprehensive impact assessments or evaluations of potential human rights risks, particularly those that could adversely affect specific demographic groups.

Only a few months after the decision, in July 2022, the Albanian government experienced a severe cyberattack which, among other repercussions, temporarily crippled government websites and disrupted public services. The hackers had managed to enter Albanian networks a full 14 months before executing the attack, which was attributed to Iranian state actors, according to an alert from the FBI and the Cybersecurity and Infrastructure Security Agency. Even before the occurrence of the cyberattacks, Albanian citizens had faced some grave personal data breaches. During 2021, several leaks led to the exposure of private information about the voting population of Tirana, including individuals' identification numbers, current employment, addresses, phone numbers, and assumptions on voting preferences, and later on, even citizens' license plate numbers and salaries.

Despite the gravity of these breaches, those responsible often faced minimal or no consequences, eroding public trust in the system's integrity. Additionally, these breaches underscored the existing vulnerabilities within the system and unveiled potential risks, prompting skepticism not only regarding the digitisation process itself but also the management of citizens' personal data. Public distrust is noticeable in the results of the 2022 national public opinion poll, *Trust in Governance*. Whilst the vast majority of Albanians (90.3%) think that the protection of personal data is important, 59.8% do not trust that their personal data is properly administered by public actors, while 58.8% do not trust that their personal data are properly administered by the private sector. On the other hand, a survey conducted by the Information and Data Protection Commissioner reveals the limited knowledge of the employees of public authorities related to the law for the protection of personal data in Albania, and the need to strengthen capacities in this regard.

In addition to the question marks posed on infrastructure and capacities, the process of digitalisation in Albania also raised significant human rights implications. The decision to digitise 95% of public services undertaken without a comprehensive human rights assessment and in the absence of alternative service channels, carries discrimination risks. This disproportionately affects demographic groups such as the elderly, and people with disabilities, who are denied effective access to services that accommodate their needs. Such concerns are also supported by the results of the latest *Trust in Governance* opinion poll. Despite 82.9% of citizens reporting to have used electronic services through the e-Albania portal in 2022, less than half (47.9%) managed to do so independently, without external assistance. Notably, respondents aged 55 and above, those with up to lower secondary education, and residents of rural areas were more likely to rely on assistance when accessing the e-Albania portal. A staggering 71.3% of citizens over 65 years old, and 45.9% of those with up to lower secondary education stated that they always required external support to navigate the e-Albania portal. Moreover, citizens with disabilities rated electronic services lower in terms of functionality, user-friendliness, time efficiency, and the ability to provide feedback compared to those without disabilities.

Denial of reasonable accommodation, according to Albanian law, constitutes a form of discrimination, when adjustments that are both necessary and appropriate to ensure the enjoyment of equal rights and freedom are denied. The digitalisation of services without ensuring accessibility and reasonable accommodation could potentially lead to violations of the Law on Protection from Discrimination and the Law on Inclusion and Accessibility of People with Disabilities.

Even though in Albania 82.6 % of the population are internet users, and 96,5% of the households have access to the internet, those who lack digital literacy, access to the internet or equipment, are also exposed to unfair treatment. While disaggregated data on specific groups with limited access are not available (except for age and gender disaggregation), according to the Albanian Institute of Statistics, 36,9% of individuals who have never used the internet are aged 65 to 74 - an age group that makes 10.15% of the current population. It should be noted that

> **“According to Albanian law, this situation could be classified as indirect discrimination”**

the government indirectly admitted the difficulties its citizens face in accessing e-services by signing an institutional agreement with the National Chamber of Notaries back in 2017. The agreement remains in force to date and enables all registered notaries to directly access personal documents or other necessary information of their clients through e-Albania, with the aim of *assisting citizens and facilitating the process of applying for e-services.*

Disadvantaged groups often bear an additional financial burden, since they increasingly rely on private businesses to receive assistance with online applications for services. For example, the media have reported the concerns of citizens of Roma and Egyptian communities who are unable to use e-services to complete their social housing application procedures. In this situation, they are forced to turn to private offices for assistance to be able to receive public services. Such private offices of assistance have “flourished” after the introduction of the decision of digitalisation of services, and in addition to being costly, raise strong concerns about personal data security. As a result, those mostly in need, are burdened with extra costs and risks, to be able to access services that are intended to be free for all citizens.

According to Albanian law, this situation could be classified as indirect discrimination – a scenario in which a seemingly impartial provision, criterion, or practice unfavorably affects certain individuals or groups (in this case due to age, economic status, education level, disability, etc.) without valid justification or when the means to achieve the intended goal are neither suitable nor proportionate to the circumstances that caused it.

These challenges underline the necessity for policymaking processes that are open, comprehensive, and well-grounded, particularly when it comes to digitalisation and cybersecurity. This requires a proactive approach to addressing potential human rights implications.

Notably, significant political and legal measures in this domain were either approved or amended between 2021 and 2023, including the Digital Agenda 2021+, Law on Protection of Personal Data, Law on Cybersecurity, and Law on E-governance. Despite the critical nature of the developments affecting this sector, there is a lack of transparency concerning the consultation processes held for these documents, as well as insufficient efforts in terms of impact assessment and risk analysis. This implies a limited degree of reflection on recent events by the government. By way of illustration, even though all these documents were published on the e-consultation platform, the Law on E-governance was the only document accompanied by a report on the public consultation process, which aims to provide transparency and accountability on the process. How-

ever, the report offers vague information on the consulted stakeholders, referencing them as "civil societies" and "various economic operators". It also states that the draft law was made available to the participants in the consultation process one week in advance, which is insufficient. Or in the case of the Law on Protection of Personal Data, even though the impact assessment report is mentioned in the accompanying report to the draft law, it is not published.

Ensuring informed decision-making within this domain demands a willingness to reflect and learn from past occurrences, and to address the human rights considerations that have been exposed. A key step involves engaging in all-encompassing and transparent consultation processes. These processes present an opportunity to engage civil society, other interest groups, as well as the affected disadvantaged communities, and to help rebuild trust. In addition, this synergy between making decisions grounded in evidence and fostering inclusivity should be complemented by investments in both technical and human resources. Adequate capacities are crucial for effectively navigating the rapid changes brought about by digital transformation, all while mitigating potential drawbacks related to security and human rights concerns.

References

1 "Microsoft investigates Iranian attacks against the Albanian government", Microsoft Threat Intelligence, 8 September 2022, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

2 "Iranian State Actors Conduct Cyber Operations Against the Government of Albania", Cybersecurity and Infrastructure Security Agency (CISA), 23 September 2022 https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

3 **Reçi, M., Kelmendi, S.** Bridging the Gap Between Cyber Policy Fragmentation and Human Rights. Institute for Democracy and Mediation, Tirana (2022) https://idmalbania.org/bridging-the-gap-between-cyber-policy-fragmentation-and-human-rights/

4 **Semini, I., Kuçi, B., Dauti, M.** Opinion Poll 2022: Trust in Governance, Institute for Democracy and Mediation, Tirana (2023) https://idmalbania.org/publication-of-the-10th-edition-of-trust-in-governance-annual-public-opinion-poll-in-albania/

5 "Questionnaire for assessing the knowledge of employees of the Public Authorities, related to the Law for the Protection of Personal Data in the Republic of Albania", Information and Data Protection Commissioner, Tirana (2022) https://www.idp.al/wp-content/uploads/2022/05/Pyetesori_per_diten_e_mbrojtjes_se_te_dhenave_personale.pdf

6 **Reçi, M., Kelmendi, S.** Bridging the Gap Between Cyber Policy Fragmentation and Human Rights. Institute for Democracy and Mediation, Tirana (2022) https://idmalbania.org/bridging-the-gap-between-cyber-policy-fragmentation-and-human-rights/

7 **Semini, I., Kuçi, B., Dauti, M.** Opinion Poll 2022: Trust in Governance, Institute for Democracy and Mediation, Tirana (2023) https://idmalbania.org/publication-of-the-10th-edition-of-trust-in-governance-annual-public-opinion-poll-in-albania/

8 "The Use of Information and Communication Technology in Families and by Individuals", Albanian Institute of Statistics (INSTAT), 16 January 2023 https://www.instat.gov.al/al/temat/kushtet-sociale/teknologjis%C3%AB-s%C3%AB-informacionit-dhe-komunikimit-tik-n%C3%AB-familje-dhe-nga-individ%C3%ABt/#tab2

9 "Population of Albania", Albanian Institute of Statistics (INSTAT), 16 January 2023 https://www.instat.gov.al/al/temat/treguesit-demografik%C3%AB-dhe-social%C3%AB/popullsia/#tab1

10 "e-Albania, citizens less paper documents before notaries", National Agency for Information Society, 13 September 2017 https://akshi.gov.al/e-albania-qytetaret-me-pak-dokumente-ne-leter-para-notereve/

11 "E-Albania in private offices", closing the counters increases costs and undermines the security of groups in need", Citizens Channel, 2 June 2023 https://citizens-channel.com/2023/06/02/e-albania-ne-kancelari-mbyllja-e-sporteleve-rrit-kostot-dhe-cenon-sigurine-e-grupeve-ne-nevoje/

12 The draft decision "On the approval of the Digital Agenda 2021+ and the Action Plan 2021+", e-consultation portal, 26 October 2021 https://konsultimipublik.gov.al/Konsultime/Detaje/414

13 Draft Law "On the Protection of Personal Data", e-consultation portal, 15 June 2022, https://konsultimipublik.gov.al/Konsultime/Detaje/472

14 Draft Law "On Cybersecurity", e-consultation portal, 26 April 2023 https://konsultimipublik.gov.al/Konsultime/Detaje/626

15 Draft Law "On Electronic Governance", e-consultation portal, 22 October 2021 https://konsultimipublik.gov.al/Konsultime/Detaje/413

16 Report on the results of public consultations for the Draft Law "On Electronic Government", e-consultation portal, 2021, https://konsultimipublik.gov.al/Konsultime/Detaje/413

17 Accompanying Report to the Draft Law "On the Protection of Personal Data", e-consultation portal, 15 June 2022, https://konsultimipublik.gov.al/Konsultime/Detaje/472

CROATIA'S CYBER CAPACITIES AND CHALLENGES

Robert Mikac

Robert Mikac is Assistant Professor in Political Science, International Relations and National Security at the Faculty of Political Science University of Zagreb. During his career he served in Armed Forces of the Republic of Croatia and NATO ISAF mission in Afghanistan, was the Head of the State Centre 112, worked as an independent police inspector within the Ministry of the Interior, and spent four years as Commander of Civil Protection of the Republic of Croatia.

KEY TAKEAWAYS

Croatia does well in areas of legal mechanisms, standards and practices, and cooperation when it comes to cybersecurity. Its weakness is mainly in the areas of education and research and development. Overall, despite its small size, Croatia has done well in the field of cyber security and could serve as a model for countries in the region with similar legal structure and shared histories.

In his 1984 novel *Neuromancer*, William Gibson first attempted to describe emergent cyberspace as follows:

> **"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding …"**

Cyberspace, including the information and communication technology that enables numerous processes within it, has developed in many directions with unimaginable speed and possibilities since then. We have all become extremely dependent on cyberspace, and states play a very important role in the regulation of cyber security. States approach and regulate the field of cyber security in different ways, and there is no best solution or model that is directly transferable from one state to another. Each country approaches this area depending on internal opportunities and capabilities and external incentives , such as obligations from membership in international organizations or under the influence of events such as major cyberattacks or events such as the war in Ukraine, which exposed everyone to additional risks and dangers.

The goal of this short text is to analyze the current state of Croatia's cyber capacities and challenges to protect critical infrastructures and essential services, citizens, and businesses from cyber threats. This could apply to other countries anywhere in the world, but is most relevant for countries in the Western Balkans due to numerous links and similarities with Croatia, including a common history, a similar legal system, exposure to identical risks, commonalities in infrastructure, pursuing the same values, and more.

Cyberspace is one of the key bloodstreams of the modern world, on which numerous states, international organizations, various business entities, critical infrastructures, local communities and even individuals strongly depend. The modern world, everyday general progress, and countless processes and activities are simply unimaginable without cyberspace, its functionalities, and the opportunities it provides. Cyberspace has become as important as "real", everyday "physical" space. Although cyberspace makes our lives easier and faster, it also opens numerous risks and dangers that we face daily. Within cyberspace, an enormous number of processes take place that are of crucial importance to issues of security and media, the economy and markets, politics and diplomacy, international relations and social activities, up to the individual needs of citizens for communication and information. All processes within cyberspace are constantly exposed to an increasing number of threats, including state-sponsored attacks. Therefore, it is necessary to pay increased attention to cyber security issues.

Although many stakeholders have important roles in the development of cyberspace, as far as security is concerned, states play an indispensable role because they have both the authority and a responsibility for the development of specific areas and dealing with key issues. The main areas are:

a) **Legal framework** (states establish a legal framework for cyber security, which includes laws and regulations that aim to define responsibilities, sanctions and mechanisms for solving open issues);

b) **Standards and practices** (states develop and promote cybersecurity standards and practices that help different organizations protect their IT systems and data);

c) **Education and training** (states ensure that citizens have adequate cybersecurity education and training that helps people recognize and protect themselves from cyber threats);

> **States control critical infrastructures and essential services, are responsible for protecting citizens and businesses from cyber threats**

d) **Research and development** (states finance research and development in the field of cyber security, which helps in the development of new technologies and solutions for cyber security);

e) **Cooperation** (states cooperate with other states, international organizations and the private sector in the field of cyber security, which is important for exchanging information, coordinating actions and strengthening resistance to cyber challenges).

In addition, states control critical infrastructures and essential services, are responsible for protecting citizens and businesses from cyber threats and have an obligation to ensure that they have adequate resources, expertise, and a legal framework to combat all forms of cyber challenges.

Croatia is a small country with limited opportunities and capabilities that has nonetheless managed to achieve extraordinary results on the foreign policy front, such as full membership in the European Union, NATO, the Schengen zone, and the Eurozone. It is also very successful in other areas such as tourism and sports, include the success of its national football team at several recent world championships, demonstrating that even small countries can achieve respectable results if they have a clear goal and vision, established structures and processes, and the cooperation of institutions and experts. This also applies to the field of cyber security.

In what follows, we focus on the five areas and their current state of play in Croatia, under the authority and responsibility of the state in the field of cyber security.

a) The **legal framework** in Croatia is well established, provides a clear set of rules and responsibilities, and enables the implementation of cyber security measures at a high level. Like many other countries, Croatia has drafted and adopted the National Cyber Security Strategy, the Law on Information Security, the Law on Cyber Security of Operators of Key Services and Digital Service Providers, other relevant laws, and all the necessary by-laws that enable the operationalization of procedures in practice. The above made it possible to establish a robust organizational structure that is responsible for different cybersecurity issues, from the issue of prevention to solving complex cyber crises. Competent institutions in the field of cyber security are mainly located within the security-intelligence system, which will not be specifically listed and named in this analysis, along with two Computer Emergency Response Teams (CERT), and the National Council for Cyber Security (interdepartmental body made up of all relevant institutions for cyber security), which coordinates horizontal national initiatives in the field of cyber security.

Croatia is currently in the process of drafting key legislation called the new *Law on Cyber Security*, expected to be adopted by the end of 2023, which will incor-

porate the provisions of the latest EU directives.[1] It is expected to be passed within a few months and will reorganize the existing cyber security system, mainly by a greater centralization of powers and responsibilities in order to respond to the increased set of obligations. The central role will be granted to the Security and Intelligence Agency. The new organizational approach would continue the transformation of the existing Center for Cyber Security (founded in 2019 and located within the Security and Intelligence Agency), centralizing cyber security management and creating a new National Center for cyber security. The professional public in Croatia unquestioningly supports the adoption of the new law. However, some experts question the correctness of the decision for excessive centralization of the powers provided to the Security and Intelligence Agency. Overall, however, Croatia performs well in this area.

b) The development and application of **standards and best practice**s are necessary to ensure overall data protection and cyber risk management, meaning the application of information and cyber security measures in the planning and implementation of information and communication systems, business continuity and threat analysis. In Croatia, both CERTs at the national level (one currently within the Information Systems Security Bureau, the other in the Croatian Academic and Research Network – CARNET), strongly promote the use of international standards and best practices, create various instructions for users, publish brochures with the latest information on the state of cyber security, conduct vulnerability testing, organize conferences for the exchange of knowledge and experience, communicate openly with the public, and resolve incidents. This is so that all interested subjects and the general public can get all the necessary and relevant information in this section. As a special value, it is necessary to single out the annual public reports on the state of security published by the Security and Intelligence Agency in 2014, and the national CERT in 2015. The public report from the Security and Intelligence Agency gives an insight into the general situation of security in Croatia and its surroundings and lists the number and direction of cyber-attacks against Croatia and its institutions. While the public reports of the national CERTs analyze the number and structure of incidents reported by citizens, there is an upward trend of the number and complexity of cyber incidents and attacks directed at the state, institutions, and critical infrastructure, as well as citizens. Overall, we can again say that Croatia performs well in this area.

c) In terms of **education and training**, Croatia does not fare well in the field of cyber security. In general, the education system is not well connected to the labor market, the population is aging, there has been an irreversible emigration of the working-age population for decades, and brain drain is a special prob-

“There has been an irreversible emigration of the working-age population for decades, and brain drain is a special problem”

> **States have the tools and authority to regulate activities and ensure a general level of security. For that to be feasible, it is necessary to develop and act uniformly in all the areas**

lem. In such circumstances, an additional challenge is that there is no complete education about the needs of cyber policy, cyber management, cyber security at any higher education institution in the country. Rather, only fragments of informational and related knowledge can be found, which is certainly not sufficient for the modern needs of the state and society. Because of this, there is a lack of experts in this field, and state institutions and other organizations in the country are forced to find the necessary expertise in different ways. They do this partly by educating their own personnel, training between the ranks, and deriving support from public-private partnerships with private companies that have the necessary knowledge.

d) Croatia also performs poorly when it comes to **research and development**. The state generally allocates very little for research and development of science, and this includes the field of cyber security. Croatia's comparative advantage is the availability of various EU funds for scientists and companies. What needs to be taken as a positive example are two solutions developed by experts working in state institutions responsible for cyber security. In the first case, it is the SK@UT system, which was built by the Security and Intelligence Agency and the Information Systems Security Bureau. SK@UT consists of a distributed network of sensors and represents the so-called "cybernetic umbrella", which currently covers more than 60 state bodies, operators of key services and legal entities of special interest. In SK@UT, in addition to all ministries and bodies of the security-intelligence system, parts of the national critical and information infrastructure are also included. Another example is PiXi, a platform for collecting, analyzing and exchanging data on computer security threats and incidents. It is a service for joint use with the aim of improving the exchange of data on computer security incidents at the national and European levels. The platform was developed by several state institutions with the participation of the academic community.

e) **Cooperation** in the field of cyber security is very extensive, both between institutions within the country, and through public-private partnerships, where private companies provide additional protection services for state institutions, and at the international level. Croatian institutions are involved in all key international processes and activities and thus have relevant information available for the development and im-

provement of their own systems. In addition, Croatia shares knowledge and experience with neighboring countries, which enables them to have a better level of protection in cyberspace. Croatia's performance in this area is quite high.

This short analysis showed some of the strengths and weaknesses of Croatia's cyber capacities and challenges, which can be relevant to other countries through sharing knowledge and information and joint strengthening of general and especially cyber security. Cyber space is a common platform where everyone has the responsibility to take care of their own cyber security, but it is states that have the tools and authority to regulate activities and ensure a general level of security. For that to be feasible, it is necessary to develop and act uniformly in all the areas analyzed in this research.

References

1 Accompanying Report to the Draft Law "On the Protection of Personal Data", e-consultation portal, 15 June 2022, https://konsultimipublik.gov.al/Konsultime/Detaje/472

2 These are several directives and regulations adopted at the end of 2022 and beginning of 2023, with a special emphasis on the *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

European Western Balkans

POLITICAL TRENDS & DYNAMICS

OVERVIEW

This section aims to provide a comprehensive analysis and understanding of human security, which includes structural sources of conflict such as social tensions brought about by unfinished democratization, social or economic inequalities or ecological challenges, for instance. The briefings cover fourteen countries in Southeast Europe: the seven post-Yugoslav countries, Albania, Greece, Turkey, Cyprus, Bulgaria, Romania, and Moldova.

Note: While accurate at the time of publishing, many situations are evolving quickly and may not be up to date.

In late spring and summer 2023, Southeast Europe witnessed ongoing tensions between Kosovo and Serbia, leading to clashes with casualties in September. The escalation of tensions in September resulted in a gun battle in Banjska monastery in the north of Kosovo, leaving several dead. Simultaneously, the European Union showed renewed interest in enlargement amid the Ukraine conflict.

Political changes were limited. Montenegro held a snap election, yet its government remains unformed. Turkey and Greece saw incumbents re-elected, and Bulgaria overcame parliamentary gridlock through a delicate compromise between established and reformist forces. Bosnia and Herzegovina faced continued disputes between Republika Srpska's leadership, state-level institutions, and the High Representative. Serbia witnessed significant anti-government protests following May tragedies but didn't substantially destabilize the ruling party.

KOSOVO-SERBIA TENSIONS REACH PEAK, LEAVE CASUALTIES

No progress has been achieved during the spring and summer of 2023 in the normalization of relations between Serbia and Kosovo, with tensions rising again on several occasions and reaching their peak in September with a clash between Kosovo police and a group of armed local Serbs, leaving one policeman and several members of the group killed.

The crisis in the north of Kosovo continued following the local elections in four Serb-majority municipalities held at the end of April. The Serb population boycotted the elections, leading to an extremely low turnout and the election of ethnic Albanian mayors. The boycott was a part of the withdrawal of Serbs in the north of Kosovo from the state institutions that began in November 2022. This state of affairs produced a new escalation at the end of May, when Serb protesters tried to prevent Albanian mayors from entering municipal premises. They clashed with KFOR peacekeepers, injuring several. While some politicians and commentators, including Kosovo's leadership, claimed that the protesters were controlled by Belgrade, no definitive proof of this has surfaced.

Following the incident, the European Union, backed by the United States, presented a 3-point plan requiring the de-escalation of the situation in the north, new elections in the area with the participation of the Serbs, and a return to dialogue for the normalization of relations. The West put particular pressure on the Government of Kosovo, led by Albin Kurti, to cease with what they described as escalatory steps, including the use of special police forces in the north of Kosovo. Due to refusal to comply, Kurti's government was placed under diplomatic sanctions from the EU and the US in June 2023, including the cancellation of high-level meetings and freezing some forms of financial assistance.

By the middle of September, the Government of Kosovo had not enabled the conditions for holding snap local elections in the north. Kurti and Serbian President Aleksandar Vučić met in Brussels on September 14, but the meeting failed to produce any breakthrough due to disagreements over the sequence of the implementation of agreements reached in Brussels and Ohrid at the end of February and beginning of March. The events of September 24, however, further deteriorated relations between Kosovo and Serbia.

On the night between September 23 and 24, armed clashes broke out at Banjska, a village near Zvečan in the north of Kosovo, between a group of masked armed men, later confirmed to be Serbs, and Kosovo police.

Vučić-Kurti meeting in Brussels, weeks before deadly clash in Kosovo
Source: X / @JosepBorrellF

The conflict broke out when the police detected a group blocking the road with trucks without license plates. A Kosovo policeman was killed in the clashes, which lasted several hours, after which the group took shelter in the Banjska Monastery, which they relinquished only later in the day. Kosovo police reported that several members of the group were killed in the operations to arrest them. Several other members were allegedly transported to Serbian hospitals. Large amounts of weaponry were seized by the Kosovo government from the group.

Kosovo leadership accused Serbia of coordinating the attacks. On the other hand, during the press conference held on the evening of September 24, Vučić described the group as Serbs resisting "Kurti's terror", blaming the Prime Minister of Kosovo for the event and denying the involvement of the official regime in Belgrade. The exact identity of all members of the group, their goals, and the extent of their ties with Serbia are yet to be determined. But at least one member has been revealed to be a top official of the Srpska Lista, the Belgrade-backed party of the Kosovo Serbs, and an associate of the Serbian leadership. Kosovo Serb politician and businessman Milan Radoičić of the Belgrade-backed Serbian List party took personal responsibility for the events in Banjska and denied the involvement of official Serbian authorities in Belgrade. He was detained in Serbia for 48 hours before being released. Another member killed by Kosovar police was a former bodyguard of Serbia's intelligence agency chief, the pro-Russian politician Aleksandar Vulin.

Western leaders called on Serbia to unequivocally condemn the Banjska attack and to withdraw the newly mobilised military units from the border with Kosovo, but stopped short of announcing any measures against Belgrade. On its part, the European Parliament adopted a resolution highly critical of Serbia and called the Commission and the European Council to adopt punitive measures against Belgrade.

In the spring, Serbian society also experienced the worst instances of mass shootings in recent years. On May 3, a 13-year-old student of an elementary school in Belgrade opened fire on fellow classmates and staff, killing nine children and a member of school security. A day later, a 20-year-old man from Mladenovac near Belgrade carried out a shooting spree in several locations, killing nine people, all of them between 15 and 26 years of age.

The tragic events shocked the public and provoked a series of massive protests labelled "Serbia Against Violence". The citizens demanded that the responsibility of the state institutions for the tragedies be determined, pointing out that there had been several oversights in particular in the case of Mladenovac murderer, who had exhibited prior signs of violence. After several weeks, the "Serbia Against Violence" protests evolved into more general anti-governmental protests, which Serbia has experienced more of in recent years. Following an initial period of small concessions, the government refused to meet most of the protesters' demands. Opposition parties have continued to organize weekly protests over the summer, which gradually reduced in size.

INCUMBENTS SCORE ELECTION VICTORIES

On May 28, President of Turkey Recep Tayyip Erdoğan won his third consecutive term as head of state in a runoff against opposition candidate Kemal Kılıçdaroğlu, securing 52% of the vote. Despite being forced into the second round of elections for the first time, facing a six-party opposition alliance and an unfavorable economic situation, Erdoğan managed to prevail and retain most of his base by campaigning on the issues of national identity and security. The observation mission of OSCE/ODIHR assessed that the incumbent enjoyed an unjustified advantage, including through biased media coverage and restrictions on fundamental freedoms of assembly and association, while the campaign itself was competitive and characterized by intense polarization. Erdoğan's AKP party lost about 7% of the vote in the parliamentary election, but kept the majority along with its allies.

Erdoğan, who has now extended his already two decade long rule over the country to 2028, was congratulated by leaders of the United States and the European Union, causing dismay among the critics of President's authoritarianism. The strategic importance of Turkey, however, apparently took precedence. This was visible over the summer, when Erdoğan decided to finally back Sweden's membership in NATO, more than a year after the country applied together with Finland. This took place only after he se-

Leaders at the Athens Summit, August 21, 2023
Source: Prime Minister of the Hellenic Republic

cured various policy concessions from Sweden, the United States, and the EU. As of September, however, Swedish membership has still not been ratified by the Turkish and the Hungarian parliament.

Another regional leader who secured re-election was Greek Prime Minister Kyriakos Mitsotakis. Originally, parliamentary elections were held in Greece on 21 May and produced no outright majority for any party. As no party accepted the President's invitation to form a government, a new snap election was called only two days later and held on 25 June. This time, with a reduced turnout, Mitsotakis's New Democracy won a landslide victory and a necessary number of seats to form a government on its own. As a result of three consecutive election defeats, former Prime Minister Alexis Tsipras resigned as the leader of the left-wing Syriza party.

Mitsotakis began his second term as Prime Minister with a pledge to continue country's economic recovery. Legalizing same-sex marriage "at some point" was also part of his election agenda. In August, Greek PM hosted a meeting in Athens with the leaders of Ukraine, Moldova and the Western Balkans to mark the 20th anniversary of the 2003 of the EU-Western Balkans Summit in Thessaloniki which promised membership perspective to the region. The leaders issued a joint Declaration, which confirmed the support for Ukrainian independence and territorial integrity, as well as "re-energized and re-focused" enlargement.

Election winners: Kyriakos Mitsotakis and Recep Tayyip Erdoğan
Source: Facebook / Presidency of the Republic of Türkiye

There was no representative of Albania at the meeting in Athens. It was widely interpreted that the Prime Minister of the country, Edi Rama, was not invited due to the controversial arrest of ethnic Greek Albanian politician, Fredi Beleri, in May. Beleri was arrested and charged with vote buying shortly before local elections in Albania, and was elected as mayor of the Himarë municipality while in prison. He has alleged that his arrest was politically motivated and orchestrated by the Rama government, while the Greek government, in a series of diplomatic activities, has insisted on respecting presumption of innocence and demanding his release. As of September, Beleri remains in prison, with the government of Albania insisting that it respects judicial procedures.

Himarë was one of the small number of municipalities in which the Socialist Party of Albania failed to win in the May local elections. The party extended its dominance by winning in 52 out of 60 contested municipalities. Irregularities were reported during the process, but the main advantage of the ruling party was the fact that the opposition was split between two faction, one led by former President and Prime Minister Sali Berisha and the other by the leader of the DP parliamentary group Enkelejd Alibeaj. Berisha's faction won the municipalities that voted for the opposition, while Alibeaj resigned as a leader following election results. Lulzim Basha, leader of the DP from 2013 to 2022 who first clashed with Berisha for a leadership position, returned as a leader of the latter faction in June.

Montenegro also held elections in early summer. Following the defeat of longtime leader of the country, Milo Đukanović, in presidential elections in April, the snap parliamentary election on 11 June was regarded as an opportunity to usher a new political era. True to expectations, the recently established "Europe Now" movement, co-founded by former minister of finance Milojko Spajić, topped the polls with 25%, campaigning on economic

issues. It was, however, closely followed by DPS (23%), which is still in the process of finding an identity after Đukanović's leadership. According to some interpretations, the result of "Europe Now" was lower than expected due to the fact that the caretaker government of Dritan Abazović released information on alleged ties between Spajić and arrested Korean crypto-market businessmen Do Kwon during the campaign; Abazović's actions were described as abuse of power by various observers.

In August, Spajić received a mandate to form a government by the co-founder of "Europe Now" and the new President of Montenegro Jakov Milatović. As of September, the government still has not been formed, as Spajić is struggling to reach the necessary number of votes after refusing to include the pro-Serbian parties in the coalition. They, in turn, accused him of being under the influence of Western ambassadors. The centre-right Democrats, led by the former Speaker of Parliament who is expected to return to that position, Aleksa Bečić, are so far the only confirmed major coalition partner of Spajić. The long delay in establishing a functioning government is once again preventing Montenegro from implementing EU-related reforms which are seen as urgent given the country's status as a frontrunner among the candidates and the new momentum given to the process.

EU ENLARGEMENT: IS 2030 A REALISTIC DEADLINE?

After a long period of ambiguity, the European Union finally started seriously discussing a new date for accepting new members: 2030. It was first proposed by the President of the European Council Charles Michel at the Bled Strategic Forum in August, where he said that both the Union and the candidate countries should be ready for enlargement by that date. Several weeks later, a joint German-French working group published an expert report (still not endorsed by respective governments) which included concrete proposals for reforms of EU institutions to make it enlargement-ready by 2030.

A push for enlargement has come from Slovenia, a country traditionally open to the EU enlargement to the Western Balkans. It is clear, however, that not everybody in the EU is on board with the idea, and that the candidates will probably have to look for the signs about the seriousness toward enlargement only after the 2024 European elections. It is also clear, however, that the war in Ukraine and the subsequent candidacies of Ukraine and Moldova have made the issue of enlargement more urgent for the European Union. But where do the candidates currently stand on the preparedness for EU accession?

As a frontrunner country, Montenegro probably has the most serious chance of being ready for EU membership by 2030 if it establishes a stable government which, as mentioned, is a significant challenge. The dispute between Kosovo and Serbia, the resolution of which is a pre-condition for the EU membership of both countries, will be a major stumbling block, along with their internal problems. Another challenge for Serbia is its foreign policy orientation, which was highlighted once again in July when the director of the state intelligence agency Aleksandar Vulin was placed under U.S. sanctions for his close ties with Russia and alleged involvement in corruption and organized crime.

North Macedonia and Albania held their first inter-governmental conferences with the EU in July 2022, launching a process of screening aimed at assessing the current level of alignment between the national and the EU legislation. The process is still ongoing and it is expected to be concluded later in 2023. North Macedonia, however, will not make any further progress until it amends the constitution to include its Bulgarian minority in the preamble, alongside other ethnic groups that live in the country. This condition was set by the Bulgarian government, which has been blocking the advancement of North Macedonia since 2020 due to unresolved issues of history and national identity, topics which many believe should not be a part of EU accession negotiations.

The session on constitutional change in North Macedonia was launched in August 2023, but the vote was postponed due to the lack of necessary majority (80 out of 120 votes). The ruling coalition of the Social Democratic Union of Macedonia, Democratic Union for Integration, and the Alliance of Albanians needs the support from the opposition right-wing VMRO-DPMNE, which has so far refused to provide it. Some commentators have interpreted the recent changes to the criminal law, which reduced sentences for some forms of abuse of office, as an attempt to appease

the opposition, and even the fugitive former Prime Minister Nikola Gruevski, to support constitutional changes.

Bosnia and Herzegovina, still needs to fulfill 14 key priorities outlined by the European Commission in 2019 to advance its EU accession process. In August 2023, the ruling coalition at the state level, consisting of nationalist Serb and Croat parties and moderate Bosniak parties, reached an agreement on adopting several laws which would further this agenda. Only a week or so later, the limits of the political will to reform the country were once again tested by the ruling of the European Court of Human Rights in the case Kovačević v. Bosnia and Herzegovina. The Court stated that the current ethnicity-based political system of BiH undermined the democratic character of elections, proposing that the members of the Presidency of BiH and the members of the House of Peoples of the Parliamentary Assembly of BiH should be elected in a single, state-level constituency, and not on the entity level. Both Serb and Croat nationalist parties criticized the ruling and showed no desire to move towards its implementation.

In the meantime, the leadership of Republika Srpska continued to take steps that were described by observers as heading toward the dissolution of the state and increasing authoritarianism within the entity. In June, the Assembly of Republika Srpska adopted a law stipulating that the decisions of the High Representative Christian Schmidt, as well as the Constitutional Court of Bosnia and Herzegovina, would not be published in the Official Gazette of RS. The leadership of the entity does not accept the legitimacy of Schmidt since his appointment was not approved by the Russian Federation, while the decision of Constitutional Court was made after the Court changed its rule of procedure to remove the requirement that a judge elected by the Assembly of RS needs to be present for a quorum.

On July 1, Schmidt exercised his authority by vetoing the proposed law changes. However, these decisions were disregarded, leading the Prosecution of BiH to charge RS President Milorad Dodik and Official Gazette's acting director, Miloš Lukić, with criminal code violations. In response, Dodik filed charges against Schmidt in July, accusing him of "unauthorized activities as the High Representative." Additionally, the ruling parties in RS stirred more controversy by passing a law that criminalizes defamation. This move was criticized by media representatives and the international community as it was seen as a violation of freedom of speech.

Press conference following the 2023 European Political Summit in Moldova
Source: epcsummit2023.md

Moldova, a new EU candidate, lags behind the Western Balkans in EU membership criteria but has drawn increased EU attention due to Russia's invasion in Ukraine. The European Political Community's second meeting convened in Moldova in June, signaling closer ties with the EU. President Sandu and Macron emphasized this, though without specifying a membership date. Moldova also received more EU financial aid and joined the Three Seas Initiative as an associate member.

In July 2023, Moldova reduced Russia's diplomatic presence, leading to 45 diplomats departing in August. Moldova withdrew from the Interparliamentary Assembly of the Commonwealth of Independent States, a body of former Soviet Union members, a move criticized by pro-Russian opposition groups. In June, the Shor Party, accused of violating the country's rule of law and independence, was declared unconstitutional. The party, involved in anti-government protests since the Ukraine conflict's start, denies these allegations.

BULGARIA BREAKS PARLIAMENTARY DEADLOCK FOR NOW, ENLARGEMENT OF SCHENGEN STILL BLOCKED

Following a full year of parliamentary deadlock and two snap elections, which was preceded by an even longer period of political instability, the two largest political forces

of Bulgaria, GERB and PP-DB coalition, finally reached a compromise. On June 6, Bulgarian parliament voted in the new government led by Prime Minister Nikolai Denkov, nominated by the reformist PP-DB. According to the rotating government agreement reached by the parties, Denkov will be succeeded after nine months by GERB member Mariya Gabriel, currently Deputy Prime Minister and Foreign Minister, who previously served as a European Commissioner from Bulgaria.

PP-DB rose to prominence as reformist anti-corruption parties which opposed the 12-year rule of GERB and its leader Boyko Borisov. However, a long period of deadlock overseen by several caretaker governments and as many as five parliamentary elections in two years forced PP-DB to abandon their previous resolve of not to cooperate with GERB. Borisov and Kiril Petkov, the leader of the PP party who served as Prime Minister for six months in 2022, were elected as chairmen of the parliamentary Foreign Affairs and EU Affairs committees, respectively.

Six days after the election of the government, Supreme Judicial Council of Bulgaria voted to remove Chief Prosecutor Ivan Geshev, identified in the 2020 anti-mafia street protests as the central protector of the politicians involved in high-level corruption and organized crime groups. The dismissal of Geshev, however, was itself described as a result of political deals in the context of the formation of the new government, rather than a sign of the real independence of the judiciary. Geshev accused those dismissing him of violating legal principles.

The ruling parties of neighbouring Romania, the Social Democratic Party (PSD), National Liberal Party (PNL), and ethnic Hungarian UDMR, also formed a grand coalition with a rotating government arrangement in 2021. In June 2023, according to the provisions of the agreement, Nicolae Ciucă of PNL was replaced as Prime Minister by Marcel Ciolacu, leader of PSD. The party that headed the government for the most of 2010s, at a time when high-level corruption was the number one political issue in the public, has thus managed to regain the office of Prime Minister. The fact that the change has taken place can be seen as an expression of more stability and political professionalism.

Both Bulgaria and Romania are still waiting for entry into the free-movement Schengen zone, which was blocked by Austria (and, in the case of Bulgaria, the Netherlands). On September 15, European Commission formally closed the Mechanism for Cooperation and Verification, which was established for Romania and Bulgaria as they were nearing their EU membership in 2006 to monitor their progress in implementing EU rules in the area of free movement of people and fight against organized crime. European Parliament also supported the entry of two countries into Schengen. The Austrian government, however, has remained opposed to the enlargement of this inner circle of the EU.

Summer in Croatia was marked by the alleged scandal concerning the state-owned power utility, HEP. The Office for Suppression of Corruption and Organized Crime started investigating the sale of electricity by the company in July, suspecting that the difference in the purchasing and selling price had damaged the company financially. Prime Minister Plenković denied that any scandal existed, saying that government's policy during the energy crisis was to ensure affordable energy products for households and the enterprise sector against a backdrop of Russia's invasion of Ukraine. An extraordinary session of parliament, called by President Zoran Milanović by request of the opposition, discussed the situation in HEP, with the ruling majority rejecting all conclusions of the opposition.

In Slovenia, the row over the public broadcaster continued as the members of the outgoing programme council and supervisory board, appointed by the previous government, challenged the law adopted by the current government which changes the governing structure of RTV Slovenija. According to the new law, none of the members of the council are appointed by parliament. After the Slovenian Constitutional Court reversed its decision to stay the legislative changes, the petitioners challenging the law took their case to the European Court of Human Rights, alleging violation of the right to a fair trial.

Election of the GERB-PP/DB government in Bulgaria
Source: National Assembly of the Republic of Bulgaria

FRIEDRICH-EBERT-STIFTUNG

The Friedrich-Ebert-Stiftung in Southeast Europe

After more than two decades of engagement in southeastern Europe, the FES appreciates that the challenges and problems still facing this region can best be resolved through a shared regional framework. Our commitment to advancing our core interests in democratic consolidation, social and economic justice and peace through regional cooperation, has since 2015 been strengthened by establishing an infrastructure to coordinate the FES' regional work out of Sarajevo, Bosnia and Herzegovina: the Regional Dialogue Southeast Europe (Dialogue SOE).

Dialogue SOE provides analysis of shared challenges in the region and develops suitable regional programs and activities in close cooperation with the twelve FES country offices across Southeast Europe. Furthermore, we integrate our regional work into joint initiatives with our colleagues in Berlin and Brussels. We aim to inform and be informed by the efforts of both local and international organizations in order to further our work in southeastern Europe as effectively as possible.

Our regional initiatives are advanced through three broad working lines:

- Social Democratic Politics and Values
- Social and Economic Justice
- Progressive Peace Policy

Our website provides information about individual projects within each of these working lines, past events, and future initiatives:
http://www.fes-southeasteurope.org

Friedrich-Ebert-Stiftung
Publisher: Friedrich-Ebert-Stiftung Dialogue Southeast Europe
Kupreška 20, 71 000 Sarajevo, Bosnia and Herzegovina
www.fes-southeasteurope.org
Orders / Contact: info.soe@fes.de

Responsible: René Schlee, Director, Dialogue Southeast Europe
Project Coordinator: Harun Cero

Editors: Vivien Savoye, Alida Vračić, Ioannis Armakolas
Managing Editors: René Schlee, Harun Cero
Editorial Assistants: Tea Hadžiristić, Azra Muftić
Communications: Ema Smolo
Design / Realization: pertext, Berlin

This publication has been produced in cooperation with:

European Western Balkans

FRIEDRICH EBERT STIFTUNG
ISSN 2490-4082