Public-private Partnerships for Inclusive Cyber Crisis Response in Developing Countries: Western Balkan Region

ANDREJA MIHAILOVIĆ & BOJAN BOŽOVIĆ

Abstract This chapter critically examines the role of public-private partnerships (PPPs) in promoting cybersecurity in the Western Balkans and emphasises their growing importance in the digital economy. The study navigates the complexities arising from the EU's support for PPPs against the backdrop of historical centralisation and public sector reluctance in the region. Through a comprehensive analysis, the authors find that PPPs significantly improve cybersecurity when public expertise is synergised with the innovative capacities of the private sector. These partnerships not only improve local cybersecurity infrastructure, but also act as catalysts for economic and innovative activities that are crucial for regional development. The research findings show that PPPs close the technological and skills gaps in developing countries, strengthen their defence against cyber threats and facilitate deeper integration into the global digital economy. The importance of PPPs also extends to their role as a critical enabler for the WB region's alignment with EU cybersecurity standards, a necessary step towards EU integration and regional prosperity. The chapter emphasises that PPPs should be a central part of national security policies, as they are essential for sustainable development in the digital age. It concludes by advocating a structured approach to PPPs that includes clear objectives, risk-sharing and confidence-building in order to fully realise their potential to strengthen the cybersecurity framework of local and regional environments.

Keywords: • PPPs • cybersecurity • developing countries • Western Balkan • EU

CORRESPONDENCE ADDRESS: Andreja Mihailović, Ph.D., Teaching Associate, University of Montenegro, Faculty of Law, 13. Jula, br.2, 81000 Podgorica, Montenegro, e-mail: andreja@usg.ac.me. Bojan Božović, Ph.D. candidate, University of Montenegro, Faculty of Law, 13. Jula, br.2, 81000 Podgorica, Montenegro, e-mail: bojan.bozovic@mep.gov.me.

https://doi.org/10.4335/2024.1.9 ISBN 978-961-7124-21-7 (PDF)
Available online at http://www.lex-localis.press.

1 Background

Over the past decade, a notable focus on cybersecurity has emerged at the international level, leading to the exploration of collaborative frameworks aimed at effectively combating the complex and broad spectrum of cyber threats. The field of cybersecurity has undergone remarkable changes, particularly with the development of public-private partnerships (PPPs) as an essential tool for improving comprehensive responses to cyber crises (Ampratwum et al., 2022; Deák, 2021). PPPs in cybersecurity refer to collaborations between government bodies and private sector groups. These collaborations have been recognised as a potentially effective strategy for improving cyber resilience at both national and global levels. PPPs are of utmost importance in the global effort to combat cyber threats by efficiently combining valuable resources, specialised experience, and actionable intelligence.

This strategy is especially crucial in developing countries, where governments frequently lack the resources and expertise to adequately address the intricate and constantly changing nature of cyberthreats. Private sector involvement in PPPs provides emerging economies with access to cutting-edge technology, knowledge transfer, capacity building and additional funding, all of which may significantly improve cybersecurity capabilities (Guitton & Frechette, 2023). These countries may benefit from the resources and knowledge of multinational corporations that have extensive experience in combating cyber threats by working with the private sector. This can help bridge the knowledge and technical gap and help countries with limited resources to better defend their digital assets and vital infrastructure against cyberattacks.

2 The prospects of public-private partnerships in cybersecurity

In general, public-private cooperation in the field of cybersecurity offers several advantages. First, integrating the technological capabilities of the private sector with public sector regulators serves to optimise the performance and effectiveness of cybersecurity measures. This collaboration enables a comprehensive approach to cybersecurity that incorporates both the technological and regulatory dimensions. In addition, the establishment of PPPs in the area of cybersecurity serves to improve information sharing and promote effective coordination between different parties. This promotes a more thorough understanding of the cybersecurity environment and accelerates the exchange of information on new threats, vulnerabilities and best approaches. In addition, building these cybersecurity partnerships serves to promote innovation and the advancement of cutting-edge technology. By working together, the public and commercial sectors may combine their resources and expertise to promote the development of novel approaches to cybersecurity problems (Dharmawan et al., 2019). These collaborations allow government agencies to utilise the technical developments and creative solutions offered by private sector organizations, while leveraging their own regulatory and enforcement capabilities. Bringing together different resources and

specialised knowledge may lead to improved cybersecurity measures that are more resilient and effective. One example of this phenomenon is the private sector's frequent access to cutting-edge tools and industry-leading methodologies that may be crucial in identifying and mitigating cybersecurity vulnerabilities. In contrast, the public sector has the authority to develop regulatory frameworks and enforce compliance, ensuring the efficient implementation of cybersecurity protocols across different businesses and sectors. In addition, PPPs are able to foster a proactive and collaborative strategy for threat intelligence management and incident response. Through information sharing and joint coordination, both the public and private sectors may improve their ability to respond quickly and efficiently to the ever-changing landscape of cyber threats. Furthermore, their use in cybersecurity has proven effective in strengthening the resilience of essential infrastructure (Serrano, 2018; Shires, 2018). Cybersecurity partnerships also help build trust between the public and private sectors, leading to a more proactive and coordinated response to cyber threats as both sectors work towards a common goal: protecting national security and critical infrastructure. In addition, PPPs promote economic growth and development by creating opportunities for businesses to thrive in a secure digital environment (Xianbin & Qiong, 2021).

Nevertheless, condemnations of PPPs in cybersecurity often point to the unwillingness of the private sector to collaborate, lack of clear strategies or incentives, poorly defined goals and objectives, misalignment of interests between public and private partners, and limitations in enforcement and ability to achieve the best outcomes. Firstly, the heavy reliance on the private sector raises the question of whether profit is being prioritised over safety. Profit is the driving force behind private companies, and protecting their own interests and assets is their top priority. They may put their own cyber security requirements above national security considerations, which could jeopardise the common security of the country. Secondly, transparency and accountability in PPPs are often insufficient. Private companies may be reluctant to provide sensitive information or co-operate fully with government officials out of concern for their public image, competitive advantage or legal consequences. In addition, it may be difficult for the public sector to adequately monitor and enforce private sector compliance with cybersecurity standards and rules (Gottam, 2022).

3 Guarding Europe's digital gates: The role of PPPs in the cybersecurity strategic compass

The European Union (EU) has demonstrated its commitment to progressive cybersecurity legislation by repeatedly emphasising the importance of a collaborative approach in addressing the complex and diverse characteristics of cyber threats. This strategy emphasises the need to protect digital assets, maintain the resilience of vital infrastructures and engage on a multilateral basis to strengthen the EU's digital defences. In addition to emphasising the value of PPPs in building a robust cybersecurity ecosystem, the legislative frameworks set strict standards for protecting data and ensuring

security (European Parliament, 2016). An important step towards recognising the role of PPPs in strengthening the resilience of key infrastructure sectors against cyber-attacks was taken in 2016 with the introduction of the Network and Information Systems (NIS) Directive (European Commission, 2016). This directive promoted an integrated approach that goes beyond traditional segmented defences and emphasised the need to implement a comprehensive accountability structure. Following on from this, the NIS2 Directive, which came into force in 2023, is a gradual improvement to EU cybersecurity law that further expands on the basic principles set out in the 2016 NIS Directive. The increasing prevalence of digitalisation and the evolving landscape of cybersecurity risks were the reason for the adoption of this amended law. To increase the resilience of public and private organisations and their ability to respond to events, the proposed law expands the definition of cybersecurity rules to include more sectors and types of organisations. These preventive measures include ensuring that each Member State has the necessary tools in place, including a competent national authority for networks and information systems and a Computer Security Incident Response Team (CSIRT). In addition, the directive in question aims to promote a security-orientated culture in various industries that rely heavily on information and communication technologies (ICTs). The European Union Agency for Cybersecurity, or ENISA, is essential to the execution of this directive because it provides technical knowledge, helps member states implement it, and supports the process of reporting cybersecurity events throughout the EU. Noteworthy for pointing out is the fact that within this specific context, "directive" relates to the concept that it can be implemented in different ways within each member state to accomplish functional harmonization with local laws. In addition, further legislative efforts to strengthen the EU cybersecurity framework and guarantee that the digital infrastructure is resistant to possible assaults include the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA) (ENISA, 2023).

The CRA is intended to complement current legislation, in particular the NIS2 framework, and was introduced as part of the 2020 EU Cybersecurity Strategy. A low level of cybersecurity is common in many products and services, and the resulting lack of regular security upgrades is one of the main concerns that the CRA aims to address. Therefore, this law proposes standardised regulations for the market launch of software or goods with a digital component. It creates a comprehensive set of cybersecurity standards that cover the steps of planning, designing, developing and maintaining such goods. To maintain a duty of care for the life of the product, manufacturers and distributors must comply with these regulations at every point in the value chain. DORA strives to improve the security and resilience of digital systems and services and recognises the growing dependence on digital operations and the associated risks. Information and communications technology (ICT) risks that have the potential to affect the stability and integrity of the financial system must be identified, addressed and mitigated, according to the Act. The DORA aims to promote a consistent approach to digital operational resilience across the European Union by establishing a standardised

set of guidelines and standards. This will enable financial institutions to prevent, adapt to and manage digital disruption (European Commission, 2020).

PPPs are becoming increasingly important as a cornerstone of national cybersecurity plans within the EU cybersecurity framework. This focus underlines the importance of these collaborations in strengthening a country's digital defences. The International Telecommunication Union (ITU), a respected international organisation, has drawn attention to the importance of PPPs, identifying them as essential components in the development and implementation of national cybersecurity plans, particularly with regard to the protection of a country's critical infrastructure (ITU, 2021). Promoting these partnerships is important for the EU because it recognises that while governments can set strategic guidelines and regulatory frameworks, the private sector often has the technological know-how, resources and flexibility to deal with ever-changing cyber threats. To promote research and innovation in the field of cybersecurity, the EU has launched several initiatives, such as the legally binding PPP on cybersecurity, with the aim of keeping the Union at the forefront of cyber defence.

Despite the significant potential of PPPs to improve the EU's cybersecurity, there are still challenges that need to be recognised and resolved. Aligning objectives between public and private institutions, implementing equitable risk sharing and building a culture of trust remain key focus areas. Given the constant evolution of cyber threats, it is also crucial to maintain an ongoing dialogue, promote information exchange and encourage multi-sector involvement. To maintain a competitive edge in the dynamic landscape of security breaches, the EU must prioritise the cultivation of collaborative and mutually beneficial ventures.

4 Synergizing growth: The transformative impact of PPPs in developing regions

Recently, there has been a growing awareness of the important role of PPPs in building cyber security capacity in developing countries. These partnerships are important in large part because developing countries often lack the knowledge and skills needed to successfully defend against cyber-attacks. Technology has transformed with the advent of Industry 5.0, but at the same time, security risks have increased due to the integration of physical systems with digital networks. Small and medium-sized businesses (SMEs), which often lack the capacity to combat complex cyber threats on their own, should pay particular attention to this. Against this backdrop, PPPs are essential for promoting knowledge exchange, exchanging best practises and jointly developing plans to mitigate cyber threats. As part of Industry 5.0, a comparative analysis between Saudi Arabia and the United Kingdom has brought to light the importance of governance and policy in strengthening cyber security measures. The study highlighted the importance of PPPs in achieving these goals and emphasised the need for tailored solutions that take into account

the unique cultural and economic realities of the different countries (Rawindaran et al., 2023).

These countries may strengthen their cyber security capabilities by using PPPs to benefit from the technological know-how and expertise of private actors. Public-private collaborations are essential for strengthening the resilience of critical infrastructure sectors in the area of cyber protection (Michalec et al., 2021). In industries such as transport, public health, finance and innovation, these collaborations enable public agencies and private companies to share information, collaborate effectively and make decisions jointly. Cybersecurity PPPs also give low-income countries access to cutting-edge methods and equipment that would otherwise be out of reach or too expensive. Their remarkable economic impact can be seen in many different areas: in the maritime industry, for example, PPPs offer flexibility in multiple payment options, increase infrastructure funding opportunities and create jobs. Although efficiency improvements are prioritised over infrastructure development, the strategy ensures governments get the most value for their money and are discouraged from overspending. PPPs can provide effective resource allocation and defence mechanisms in the area of cyber defence and extend this economic justification.

5 Grappling with the challenges: Decoding the PPP puzzle

While PPPs in the area of cybersecurity offer immense potential for developing countries, the path to their successful implementation is full of challenges that can only be overcome with a holistic approach.

In many emerging economies, there are insufficiently comprehensive legislation and legal frameworks for cybersecurity, leading to inconsistencies in the allocation of responsibilities and powers. As a result, prosecuting cybercriminals and protecting the digital rights of individuals in these contexts is a major challenge. There is often an insufficient understanding of the critical importance of cybersecurity among the public, business and government entities, resulting in low standards of expertise and competence in cyber risk defence. Although the relevance of cybersecurity cannot be overstated, many developing countries encounter budgetary constraints that make it difficult to allocate resources to cybersecurity efforts, especially in the face of competing priorities such as medical care, educational opportunities and facilities (Otieno, 2020). The use of outdated technologies and systems in these countries makes them vulnerable to cybercriminal activity, while the expenses associated with modernising these systems can be a significant barrier. The phenomenon of talented cybersecurity professionals migrating from low-income countries to advanced economies for better opportunities leads to a lack of expertise in their countries of origin.

Geopolitical tensions or scepticism towards foreign surveillance may make developing countries reluctant to adopt certain cybersecurity measures or technologies. The task of

harmonizing interests and objectives can be challenging due to the involvement of various stakeholders, from government agencies to commercial companies. This complexity arises from the fact that these groups may have different objectives. The phenomenon of rapid urbanisation in several emerging countries is leading to an escalation of digitalisation, but without a corresponding advance in cybersecurity protocols. In some countries, there is a great reluctance to share information, especially when it comes to security breaches or vulnerabilities. This reluctance is a significant barrier to the dissemination of important information that is essential for the implementation of successful cybersecurity measures. The establishment of efficient PPPs may be hindered by a potential lack of trust between the public and private sectors, which may be due to historical or political factors.

Furthermore, it should be noted that the problem of cybersecurity is further intensified by the existence of a digital divide between urban and rural regions in several developing countries (Selfa-Sastre et al., 2022). The term "digital divide" refers to the inequality in the availability and use of digital technology, which includes devices such as computers, internet connectivity, and mobile phones. Residents of metropolitan regions often have better access to these technologies than their rural counterparts. This discrepancy may be attributed to several variables, including infrastructure development and the availability of economic resources. However, it is worth noting that urban residents may have a minimal level of cybersecurity measures in place. On the other hand, rural regions, which are often neglected in the process of digital transformation, become vulnerable targets due to their restricted familiarity and awareness of cyber risks. The uneven distribution of technological progress and varying levels of cybersecurity awareness contribute to the formation of a fragmented defence environment. Furthermore, while the widespread adoption of mobile devices in these countries is beneficial for improving connectivity, it also introduces additional vulnerability. In developing countries, a significant number of people rely on mobile devices as their primary means of accessing the internet. However, these devices often run outdated software versions or lack adequate security measures. As a result, consumers in these regions are particularly vulnerable to cyberattacks that specifically target mobile platforms. Another risk is that emerging markets are overly reliant on single vendor offerings in their search for cost-effective cybersecurity solutions. Over-reliance on a single vendor's solution can lead to potential vulnerabilities if the solution has a security flaw or the vendor discontinues support.

A major obstacle for most countries is the lack of a robust incident response architecture, leading to haphazard and disjointed responses to cyber events. In addition, cultural beliefs prevalent in certain civilisations play a role in the phenomenon of underreporting, as admitting weaknesses or breaches in cybersecurity infrastructure is associated with social shame. The lack of comprehensive reporting and openness is not only a barrier to progress, but also hinders the successful execution of robust cybersecurity measures in these nations. The lack of a clearly defined approach to addressing and mitigating security breaches can result in prolonging and exacerbating the consequences of cyber disasters.

Finally, the issue of international co-operation, or lack thereof, poses a significant difficulty. Cyber threats transcend national borders and perpetrators often operate from countries outside the jurisdiction of the target country. Without solid international coordination and conventions, it will be difficult to bring these perpetrators to justice. The digital age offers unprecedented prospects for progress and development, but also poses complex problems for emerging nations. To effectively address the complexities of cybersecurity, it is essential to not only rely on technological solutions, but also cultivate a cybersecurity mindset, promote a culture that prioritises cybersecurity and build solid international partnerships.

6 The Western Balkan: A unique backdrop

The Western Balkan (WB) is a political designation that comprises six nations, namely Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia. These countries have a rich historical background characterised by various periods of conflict, cooperation and transformation. The dissolution of Yugoslavia in the 1990s led to a series of conflicts that had a lasting impact on the political and economic framework of the area. Governance, policy-making and international co-operation in the area were particularly shaped by its turbulent historical background (Mihailovic, 2023).

From a political perspective, the area currently faces persistent problems related to the consequences of past conflicts, ethnic divisions, difficulties in government, and hopes for inclusion in the European Union. The progress made by the Western Balkans in harmonising their policies was recognised by EU leaders in February 2023, who also urged them to accelerate additional measures. The region is now experiencing significant economic investment, particularly from the European Union. In June 2023, the European Commission initiated a €2.1 billion funding package with the aim of supporting 14 investment flagships in the Western Balkans region. These investments cover many sectors such as transport, energy, environment, human resources and assistance for the private sector (European Commission, 2023). The investment in question is an integral part of the European Union's Economic and Investment Plan for the Western Balkans, which aims to address imbalances in economic development and promote greater regional integration. However, there are still challenges that need to be addressed. These challenges include the need for deeper trade integration, the need for institutional capacity building and harmonisation with the standards set by the European Union. The significance of regional economic integration through trade and connectivity as a primary catalyst for development has been emphasised by prominent entities such as the World Bank, USAID and the Swiss government (World Bank, 2023). These activities serve to improve the economic prospects of the area and further consolidate its aspirations to become a member of the EU. The overall aim is to create a more favourable business environment, attract current investment and at the same time provide employment opportunities.

The WB region has recognised the great importance of cybersecurity as it becomes increasingly involved in global digital networks, as outlined in the 2023 National Cybersecurity Strategy. The increasing evolution of the digital environment and the increasing sophistication and regularity of cyber threats highlight the region's growing dependence on cyberspace for government, business and social interaction, thus emphasising the need for strong cybersecurity protocols (WB Security Report[1], Atlantic Council of Montenegro, 2022). WB countries have demonstrated a proactive approach in formulating their respective national cybersecurity plans, often drawing inspiration from the EU's exemplary practises. In the realm of legislation, there has been a remarkable adoption of international and regional legal frameworks. Organisations such as NATO have played a crucial role in providing strategic direction, promoting cooperation and sharing best practise. As a result, several Western nations currently view cybersecurity as a crucial component of their national security policy and have begun formulating legal frameworks to improve cybersecurity (Berg & Keymolen, 2017).

7 Distinct dynamics: The Western Balkans' challenges in fostering PPPs

The WB, at the intersection of history and digital transformation, presents a unique case for the study of PPPs in cybersecurity. By working together, building trust and adherence to global standards, the region can chart a path to a secure digital future. The proliferation of technology and the growing dependence on the internet in different regions has led to an escalation of cyber threats, which manifests itself in various forms. WB countries have been actively engaged in modernising national infrastructures and promoting integration into global digital networks. However, the rapid implementation of digital transformation has also exposed the area to many cyber threats. These attacks pose a double threat to both national security and the economy, as they can undermine investor confidence and disrupt commercial activities. In 2022, several WB countries experienced a series of catastrophic cyberattacks, mainly targeting government institutions. These attacks caused notable disruptions to their systems and caused significant instability to a variety of objectives that included both political influence and financial gain.

In the WB region, the numerous benefits of PPPs in cybersecurity are increasingly recognised despite significant obstacles. By consolidating resources, specialised knowledge and strategic foresight, these collaborative alliances represent a coherent strategy to address the challenges posed by cyber threats. Ongoing initiatives in countries such as Montenegro and Serbia point to a growing trend towards collaborative partnerships between governmental organisations and business actors. Underlying these activities is the need to effectively utilise the respective capabilities of both sectors to proactively address and mitigate the risks posed by cyber-attacks. Alliances therefore have the potential to provide the necessary financial resources and critical assets to strengthen cyber security activities in WB countries, which often face financial constraints due to competing priorities.

Furthermore, the historical practise of centralised governance sometimes poses a challenge to the promotion of successful cooperation between the public and private sectors. For example, the establishment of effective PPPs in the context of cybersecurity sometimes encounters obstacles, mostly due to long-standing distrust and conflicting goals between the sectors involved. It is crucial to clearly define the boundaries of responsibility and accountability in these collaborations, as the private sector may prioritise economic progress and focus on the financial and reputational aspects of cybersecurity. The public sector, on the other hand, is tasked with ensuring national security and protecting critical infrastructure (Wallis & Johnson, 2020).

Nevertheless, it is imperative to recognise the unique characteristics of cybersecurity dynamics that may hinder the effectiveness of such collaborations. A study conducted by (Kshetri, 2016) found that the contributions of private companies in PPPs are often not adequately recognised. The study raised concerns about the nature of these partnerships, suggesting that they may be more akin to a "public-private dictatorship" than a true collaboration. Furthermore, criticism of PPPs in the realm of cybersecurity has a variety of causes (Tropina, 2015). The criticism relates to the unwillingness of the private sector to cooperate, the lack of incentives and clearly defined strategies, unclear objectives, divergent interests between public and private partners and constraints in enforcement that hinder the achievement of optimal results. In addition, it is worth noting that the private sector may place more emphasis on economic progress and prioritising financial and reputational dimensions of cybersecurity than national security concerns (Wallis & Johnson, 2020). Effective coordination and communication between the public and private sectors is crucial for a comprehensive response to cyber crises among key stakeholders at the national level. Furthermore, the extensive involvement of the private sector in cyberspace introduces complicated dynamics that make it difficult for the government to respond effectively. Furthermore, the lack of precise and clearly articulated goals could hamper the effectiveness of public-private cooperation in cybersecurity. Therefore, further research is needed to assess the contextual variables, methods and procedures related to the effectiveness of PPPs in cybersecurity.

In the regional context, building trust between the public and private sectors is of paramount importance. Trust plays a pivotal role in promoting effective co-operation and cooperation between the public and commercial sectors. This phenomenon is of particular significance in the realm of policy formulation and political discourse, as the pervasive lack of trust in governmental institutions is widely recognised and lamented by scholars (Neal et al., 2016). In order to foster trust between the public and private sectors, it is important to consider certain crucial variables. Transparency and accountability are crucial elements in fostering trust between the public and private sectors. The definition of transparency refers to the extent to which information, procedures and decisions are open and accessible in both sectors (Zidane et al., 2015). Promoting transparency is of utmost importance in fostering trust between the public and private sectors as it serves to

improve accountability, curb corruption and ensure the fair and unbiased nature of decision-making processes.

Building international collaborations, adherence to global best practises and maintaining ongoing discussions can serve as crucial factors in facilitating effective cybersecurity PPPs. When managed effectively, PPPs have the potential to significantly improve the cybersecurity capabilities of a given region. Through collaborative efforts, policy makers and the business sector have the potential to facilitate entry into an era characterised by improved digital security, thereby achieving broad societal benefits. Empirical research suggests that countries that have effectively implemented PPP programmes tend to benefit from a comprehensive and well-structured PPP governance framework that covers all phases of the PPP lifecycle. This includes the exercise of institutional authority over these partnerships, the implementation of open and competitive procedures for public procurement and contract management, the ongoing monitoring and evaluation of partnership performance, the resolution of disputes and the full management and reporting of fiscal costs and risks.

The WB region, characterised by a variety of cultures and historical backgrounds, has the potential to benefit greatly from these collaborative efforts. In order to fully realise the potential of PPPs, it is imperative that WB economies address the shortcomings in their PPP governance arrangements. This includes implementing comprehensive public investment planning procedures, synchronising the objectives of PPPs with national investment plans and ensuring transparent and competitive tendering procedures.

As digital integration in the region progresses, it is crucial that cybersecurity is prioritised. This includes the continuous assessment of cyber threats, the allocation of resources to improve capabilities, the promotion of cooperation between regional actors and the alignment of cybersecurity measures with internationally recognised human rights standards. It is important to recognise that the field of cybersecurity goes beyond the conventional remit of intelligence and defence organisations, as it has a significant impact on many sectors of society, such as transportation, public health, banking and innovation. As Michalec et al. (2021) have highlighted, PPPs are paramount in managing cybersecurity in critical infrastructures. Successful collaborations can be facilitated through partnerships that have an alignment of interests and provide defined roles and tasks for the specialists involved. Considering that developing countries have long struggled with varying technological capabilities and limited resources, increased collaboration between the public and private sectors is a strategic way to provide financial resources for cybersecurity endeavours. The private sector has a crucial role to play in this context, as it is driven by innovation and government cyber infrastructure relies heavily on goods and services provided by private companies for security purposes.

8 Conclusion

This chapter examines the pivotal role of public-private partnerships (PPPs) in strengthening cybersecurity in the Western Balkans, a region facing the dual challenge of adapting to a rapidly evolving digital threat landscape and overcoming a historical legacy of centralised power structures. By integrating the EU's strategic focus on PPPs into regional cybersecurity strategies, the study shows a clear path for developing countries to strengthen their digital defences and adapt to broader European norms.

Furthermore, this study contributes to the understanding of how PPPs can be effectively tailored to regional development needs, especially in contexts where trust between the public and private sectors is limited. The findings show that such partnerships are crucial in bridging the gap between existing capabilities and the stringent requirements of the EU, as reflected in directives such as NIS2. The practical implications show that the WB region needs to proactively embrace PPPs to fulfil EU regulatory expectations and address the region's differentiated socio-political challenges. This proactive approach is essential to protect its digital domain and support its path to EU integration.

Consequently, this chapter applies a methodological framework that thoroughly explores the multi-layered dynamics of PPPs in strengthening regional cybersecurity capacities. By comprehensively analysing the existing literature, which includes a range of policy documents, legal instruments and strategic initiatives, this inquiry lays the foundation for understanding the operational intricacies of PPPs. This synthesis helps to analyse the legal and policy ecosystem that either supports or hinders the functioning of such partnerships, underpinning their operationalisation and effectiveness in a particular area of cybersecurity. Finally, the chapter recommends the promotion of international co-operation, adherence to global standards and the maintenance of a continuous discourse on cybersecurity. These steps are essential for the region to navigate the complex web of cyber threats and capitalise on its strategic position in Europe. The recommendations aim to provide a blueprint for regional development through improved digital security and to ensure that the opportunities arising from the growing digital presence are capitalised on in a secure and regulated manner.

Note:

[1] https://ascg.me/en/western-balkan-security-report-2022/.

References:

Ampratwum, G., Osei-Kyei, R. & Tam, V. W. Y. (2022) Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events: A systematic review, *International Journal of Critical Infrastructure Protection*, 39(C), https://doi.org/10.1016/j.ijcip.2022.100556.

Atlantic Council of Montenegro (2022) *Western Balkan Security Report*, available at: https://ascg.me/en/western-balkan-security-report-2022/ (September 15, 2023).

Berg, B. & Keymolen, E. (2017) Regulating security on the Internet: Control versus trust, *International Review of Law, Computers & Technology*, 31(2), pp. 1-20, https://doi.org/10.1080/13600869.2017.1298504.

Deák, V. (2021) Simulation framework for practical cyber security training in the public service, *Security and Defence Quarterly*, 33(1), pp. 87–104, https://doi.org/10.35467/sdq/132026.

Dharmawan, N. K. S., Kasih, D. P. D. & Stiawan, D. (2019) Personal data protection and liability of internet service provider: a comparative approach, *International Journal of Electrical and Computer Engineering (IJECE)*, 9(4), pp. 3175-3184, http://doi.org/10.11591/ijece.v9i4.pp3175-3184.

ENISA (2023) *Supporting policy developments to achieve a high common level of cybersecurity*, available at: https://www.enisa.europa.eu/news/supporting-policy-developments-to-achieve-a-high-common-level-of-cybersecurity (September 04, 2023).

European Commission (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (September 10, 2023).

European Commission (2020) *Proposal for a regulation on digital operational resilience for the financial sector and amending regulations (EU) No 575/2013, (EU) No 648/2012, (EU) No 600/2014, and (EU) No 806/2014*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0595 (September 14, 2023).

European Commission (2023) *European Commission launched an additional €2.1 billion investment package for the Western Balkans under the Economic and Investment Plan*, available at: https://neighbourhood-enlargement.ec.europa.eu/news/european-commission-launched-additional-eu21-billion-investment-package-western-balkans-under-2023-06-30_en (September 2, 2023).

European Parliament (2016) *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (September 10, 2023).

Gottam, M. (2022) How Machine Learning Can Be Used To Improve Predictive Analytics, *International Journal for Research in Applied Science and Engineering Technology*, 10(12), https://doi.org/10.22214/ijraset.2022.48432.

Guitton, M. J. & Fréchette, J. (2023) Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy, *Computers in Human Behavior Reports*, 10, https://doi.org/10.1016/j.chbr.2023.100282.

International Telecommunications Union (ITU) (2021) *Global Cybersecurity Index 2020*, available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (September 12, 2023).

Kshetri, N. (2016) Cybercrime and cybersecurity in India: causes, consequences and implications for the future, *Crime, Law and Social Change*, 66, pp. 313-338, https://doi.org/10.1007/s10611-016-9629-3.

Michalec, O., Milyaeva, S. & Rashid, A. (2021) Reconfiguring governance: How cybersecurity regulations are reconfiguring water governance, *Regulation & Governance*, 16(4), pp. 1325-1342, https://doi.org/10.1111/rego.12423.

Mihailovic, A. (2023) The legal framework for cybercrime accountability in the Western Balkans countries as a turning point for EU integration, In: Delerue, F., Sukumar, A. & Broeders, D. (eds.) *Responsible Behaviour in Cyberspace: Global narratives and practice* (Luxembourg: Publications Office of the European Union), pp. 75-89.

Neal, T., PytlikZillig, L., Shockley, E. & Bornstein, B. (2016) Inspiring and advancing the many-disciplined study of institutional trust, In: Neal, T., PytlikZillig, L., Shockley, E. & Bornstein, B. (eds.) *Interdisciplinary Perspectives on Trust: Towards Theoretical and Methodological Integration* (Berlin: Springer), pp. 1–16.

Otieno, D. (2020) Cyber security challenges: The Case of Developing Countries, *Promoting Creativity, Innovation and Productivity for Sustainable Development*, available at: https://www.researchgate.net/publication/346485466_Cyber_security_challenges_The_Case_of_Developing_Countries (September 10, 2023).

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I. & Hewage, C. (2023) Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom, *Digital*, 3(3), pp. 200-231, https://doi.org/10.3390/digital3030014.

Selfa-Sastre, M., Pifarré, M., Cujba, A., Cutillas, L. & Falguera, E. (2022) The Role of Digital Technologies to Promote Collaborative Creativity in Language Education, *Frontiers in Psychology*, 13, February 9, https://doi.org/10.3389/fpsyg.2022.828981.

Serrano, W. (2018) Deep Learning Cluster Structures for Management Decisions: The Digital CEO, *Sensors*, 18(10), https://doi.org/10.3390/s18103327.

Shires, J. (2018) Enacting expertise: Ritual and risk in cybersecurity, *Politics and Governance*, 6(2), pp. 31-40, https://doi.org/10.17645/pag.v6i2.1329.

Xianbin, T. & Qiong, W. (2021) Sustainable Digital Economy Through Good Governance: Mediating Roles of Social Reforms and Economic Policies, *Frontiers in Psychology*, 12, November 24, https://doi.org/10.3389/fpsyg.2021.773022.

Tropina, T. (2015) *Public–Private Collaboration: Cybercrime, Cybersecurity and National Security* (Cham: Springer).

Van den Berg, B. & Keymolen, E. (2017) Regulating security on the internet: Control versus trust, *International Review of Law, Computers & Technology*, 31(2), pp. 188-205, https://doi.org/10.1080/13600869.2017.1298504.

Wallis, T. & Johnson, C. (2020) Implementing the NIS Directive, driving cybersecurity improvements for Essential Services, *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, https://doi.org/10.1109/CyberSA49311.2020.9139641.

World Bank (2023) *Western Balkan Economies Explore Easier, Faster, and Safer Trade Together*, available at: https://www.worldbank.org/en/news/press-release/2023/05/16/western-balkan-economies-explore-easier-faster-and-safer-trade-together (September 18, 2023).

Zidane, Y. J. T., Johansen, A. & Ekambaram, A. (2015) Project Evaluation Holistic Framework – Application on Megaproject Case, *Procedia Computer Science*, 64, pp. 409-416, https://doi.org/10.1016/j.procs.2015.08.532.