



Research Article

The Role of the Western Balkans Cyber Capacity Center in Enhancing Energy Security through Regional Governance

Megghi Pengili

Visiting Research Fellow, School of Politics and International Studies, University of Leeds, UK, <https://www.leeds.ac.uk>

Abstract: The Western Balkans Cyber Capacity Center (WB3C) was inaugurated in 2024. In line with the Berlin Process's initiatives to improve the regional countries' capabilities in energy security, energy transition, and cybersecurity, the WB3C aims to meet regional needs for cyber protection and to foster a regional cybersecurity culture for energy infrastructure. The WB3C's activities are expanding as the Western Balkans' renewable energy potential attracts investments from a range of global players, including the European Union, the United States, the United Kingdom, Russia, China, and Türkiye. This article analyzes the potential of the WB3C as an emerging regional cyber governance framework for the energy sector. The qualitative analysis incorporates elements of both the capability approach and institutional analysis and design. The work underscores the importance of the region in cyber governance, where the role of the state is transferred to an infrastructure that transcends borders.

Keywords: Western Balkans, Cyber Capacity Center, energy transition, energy security, energy systems, regional cyber governance.

Introduction

Sergiu Mitrescu notes that the Western Balkans (WB) is facing a critical juncture in its energy landscape, defined by fatigue in complying with the EU energy acquis, internal and external geopolitical developments,¹ and the WB's commit-

¹ Sergiu Mitrescu, "Energy Diplomacy in the Western Balkans," *Foreign Policy Review* 16, no. 1 (2023): 78-90, <http://doi.org/10.47706/KKIFPR.2023.1.78-90>.

ment “to increase their share of renewable energy sources (RES) by 2030 to reach between 25 % and 40 % of their energy mix.”² The energy transition is driven by rapidly scaling digital technologies and comes with complex cyber risks, the management of which requires governance capacity generated through “collective cybersecurity governance frameworks and multilateral norms.”³

The Western Balkans face complex issues related to foreign energy investments, transparency, and cyber vulnerabilities. In late 2020, the European Union announced a €9 billion plan to improve infrastructure, support green energy, and boost digitalization in the region.⁴ These economies are largely controlled by state-owned companies, whose lack of transparency and poor management have obstructed competition and delayed energy investments.⁵ Additionally, cyberattacks on Albania in 2022 and on Montenegro’s electrical power systems in 2022⁶ suggest that critical energy infrastructure is a potential target for malign actors, particularly considering the region’s ambitions regarding renewable energy. Nevertheless, this debate remains largely overlooked in the current literature on the Western Balkans. This is problematic because energy security is considered an integral part of national security, especially given these countries’ ambitions toward renewables.⁷

With the growth of renewable energy generation, the sector has experienced an increase in attacks against its critical infrastructure over the last five years. Nordex and Deutsche Windtechnik control centers, as well as South China Sea wind-energy businesses, were compromised in 2022.⁸ According to Cyber Energia, more than 200 cyberattacks targeted the energy industry in 2023, with over

² Michalis Mathioulakis, “Strategic Elements of the Energy Union and the Role of Regulation in Energy Security,” in *Aspects of the Energy Union: Application and Effects of European Energy Policies in SE Europe and Eastern Mediterranean*, ed. Michalis Mathioulakis (London: Springer, 2021), 73-101, https://doi.org/10.1007/978-3-030-55981-6_4.

³ Paul Rosenzweig, “The International Governance Framework for Cybersecurity,” *Canada-United States Law Journal* 37, no. 2 (2012): 405-432, 407, <https://scholarlycommons.law.case.edu/cuslj/vol37/iss2/10>.

⁴ Luigi Scazzieri, “Reviving European Policy towards the Western Balkans,” Policy Brief, Centre for European Reform, December 15, 2021, <https://www.cer.eu/publications/archive/policy-brief/2021/reviving-european-policy-towards-western-balkans>.

⁵ Matthew Bryza, “Western Balkans Must Pursue More Competitive Energy Sectors,” Issue Brief, Atlantic Council, February 26, 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/western-balkans-must-pursue-more-competitive-energy-sectors/>.

⁶ Vasko Popovski et al., “Crisis Prevention and Critical Infrastructure in the Western Balkans,” IDSCS Policy Brief (Skopje: Institute for Democracy “Societas Civilis,” 2023), 20, <https://idscs.org.mk/wp-content/uploads/2023/05/Second-Paper-Online.pdf>.

⁷ Mitrescu, “Energy Diplomacy in the Western Balkans.”

⁸ Sarah G. Freeman et al., “Attack Surface of Wind Energy Technologies in the United States,” Idaho National Laboratory, January 2024, 5, <https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf>.

half affecting Europe.⁹ The extent of cyber insecurity underscores the urgent need to invest in cybersecurity to safeguard operational efficiency, maintain public trust in this energy subsector, and ensure that the benefits of innovation do not come at the expense of security.¹⁰ While the global cybersecurity market is projected to grow at a compound annual growth rate (CAGR) of 12.3 % through 2030,¹¹ cyber insurance increased by eight percentage points in the Americas and by 11 percentage points in Europe.¹²

Considering that cyber resilience is a pillar of the security of energy systems, the WB countries, namely Albania, Bosnia and Herzegovina, Montenegro, Kosovo, North Macedonia, and Serbia, are prioritizing cyber capability building across national jurisdictions under the WB3C umbrella,¹³ which seems to lay the foundations for regional cyber governance.¹⁴ This article defines cyber governance as the implementation of decision-making processes focused on risk management through enhanced participation, transparency, and accountability. Cyber capability building, in turn, is the process of acquiring the skills, know-

⁹ ENISA, “2024 Report on the State of the Cybersecurity in the Union,” December 3, 2024, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>.

¹⁰ “Navigating Cybersecurity Risks in Europe’s Wind Energy Sector: The Challenge of Non-EU Infrastructure,” Forvis Mazars, November 29, 2024, www.forvismazars.com/uk/en/insights/energy-infrastructure-and-environment-insights/the-challenge-of-non-eu-infrastructure.

¹¹ “Cybersecurity Market (2026–2033),” Grand View Research, June 2025, www.grandviewresearch.com/industry-analysis/cyber-security-market.

¹² “Cyber Budgets Increase, Executive Overview Improves, but Challenges Lurk under the Surface,” Moody’s, Special Report by Moody’s Ratings, September 26, 2023, <https://www.moody.com/web/en/us/insights/data-stories/2023-cyber-survey-highlights.html>.

¹³ “Berlin Process Summit 2024, 10th Anniversary, Chair’s Conclusions,” *BerlinProcess.de*, October 14, 2024 https://www.berlinprocess.de/uploads/documents/chairs-conclusions-2024_1728992421.pdf; Western Balkans Investment Framework, “€1 Billion Energy Support Package for the Western Balkans,” December 14, 2022, www.wbif.eu/news-details/1-billion-energy-support-package-western-balkans-approved-5-december/; Francesco Siccardi, “Understanding the Energy Drivers of Turkey’s Foreign Policy,” *Carnegie Europe Papers*, February 28, 2024, <https://carnegieendowment.org/russia-eurasia/research/2024/02/understanding-the-energy-drivers-of-turkeys-foreign-policy>; Vladimir Spasić, “Alcazar Secures USD 50 Million from US DFC for Investments in Western Balkans, Other Markets,” *Balkan Green Energy News*, April 26, 2024, <https://balkangreenenergynews.com/alcazar-secures-usd-50-million-from-u-s-dfc-for-investments-in-western-balkans-other-markets/>; Panos Kefalas, “The Future of Energy in the Western Balkans: A Renewables Revolution,” *Aurora Energy Research*, October 7, 2024, <https://auroraer.com/insight/the-future-of-energy-in-the-western-balkans-a-renewables-revolution/>.

¹⁴ “CybilProject – WB6-EU Cooperation for Improving Cybersecurity in the Western Balkans,” Cybil, 2024–2025, <https://cybilportal.org/projects/wb6-eu-cooperation-for-improving-cybersecurity-in-the-western-balkans/>.

ledge, and resources necessary for the maturity and efficiency of cyber governance. In the context of economic digitalization, regional digital governance arrangements would facilitate the integration of these countries into the European Union, contribute to the EU Digital Single Market, and enhance the region's potential as a renewable energy market in Europe.¹⁵

Natural gas and renewable energy markets are of common interest to the Western Balkans (WB) for the following reasons. First, all WB countries are engaged in adopting Chapter 15 of the EU *acquis* on energy policy.¹⁶ Second, there are several planned and projected pipelines in the region, stretching from Russia and the Caspian countries to the European Union. These projects have emerged given the rising importance of the Balkans as a principal transit corridor for the transit of Caspian and Middle Eastern natural gas to Europe, especially via Türkiye,¹⁷ through projects such as TANAP, which in turn feeds into the Trans-Adriatic Pipeline (TAP) across Greece and Albania and under the Adriatic Sea to Italy. Except for Albania and Montenegro, which rely heavily on hydropower and less on coal,¹⁸ with hydropower accounting for almost 95 % of their energy generation, the rest of the WB group, led by Kosovo, still uses coal to generate energy.¹⁹ Further, with the Berlin Process and the energy conditionality it entails, achieving the EU's long-term goal of carbon neutrality by 2050 will require decarbonizing energy systems. Thus, Albania, North Macedonia, Bosnia and Herzegovina, and Montenegro are also considering significant investments in natural-gas infrastructure.²⁰ These developments suggest that the intersection of cybersecurity and renewable energy is a critical area requiring energy-transition-ready governance based on functional, mission-specific solutions that depend on information and instructions generated and transmitted through cyberspace.²¹

¹⁵ Chiara Mihalčatinová, "Is Albania a New Regional Champion in the Energy Transition?" Strategic Analysis, 2024, <https://www.strategicanalysis.sk/is-albania-a-new-regional-champion-in-the-energy-transition/>.

¹⁶ Nicole Lindstrom, "Power Trips: Europeanization, Market-governance, and Energy Policy in the Western Balkans," *Policy and Society* 30, no. 3 (2011): 197-207, <https://doi.org/10.1016/j.polsoc.2011.07.004>.

¹⁷ Mehmet Efe Biresselioglu, "Assessing the Energy Security in the Balkan Region: Existing Challenges," *Valahian Journal of Historical Studies*, no. 18 (2012): 17-42.

¹⁸ Barbara Frey, "The Energy Transition in the Western Balkans: The Status Quo, Major Challenges and How to Overcome Them," *Policy Notes and Reports* 76, Vienna Institute for International Economic Studies, May 2024, <https://wiiw.ac.at/the-energy-transition-in-the-western-balkans-the-status-quo-major-challenges-and-how-to-overcome-them-dlp-6896.pdf>.

¹⁹ Lindstrom, "Power Trips: Europeanization, Market-governance, and Energy Policy"; Dimitar Bechev, "Energy in the Western Balkans," The Balkans in Europe Policy Advisory Group, May 24, 2023, www.biepag.eu/publication/energy-in-the-western-balkans/; Frey, "The Energy Transition in the Western Balkans."

²⁰ Bryza, "Western Balkans Must Pursue More Competitive Energy Sectors."

²¹ Jasper, "Cyberspace," 344, note 24.

The establishment of Western Balkans cyber governance depends on processes of learning and organizational integration, fostered by the Western Balkans Cyber Capacity Center (WB3C). The Center's mission is to strengthen the cyber pillar of the Berlin Process,²² with four G7 members among its partners: France, Italy, the United Kingdom, and Germany – all ranked among the world's leading cyber powers in the 2022 National Cyber Power Index.²³ These four partners are members of the G7 cybersecurity working group, which was the first instance of clustered cyber governance emerging from a security community.²⁴ Furthermore, the WB6-EU Cooperation for Improving Cybersecurity in the Western Balkans, a project initiated in 2024 within the Center, aims to stimulate regional cooperation by strengthening national Computer Security Incident Response Teams (CSIRTs)²⁵ and reflecting best practices derived from transnational experiences.

Considering these brief points, the WB3C case enables us to address the research question of whether regional cyber governance is, in fact, materializing through the WB3C. The Center's regional programs since its inception, as the analysis will show, already reflect a concerted agency for cybersecurity, which becomes visible through four dimensions of collective governance: coordination, collective action, learning, and resources.²⁶ In this light, the article proceeds in four parts. After the introduction, the literature review outlines the interplay between energy-cybersecurity dynamics and cyber threats within the strategic context of the Western Balkans. The next section frames the methodology around Institutional Analysis and Design (IAD) and the capability-building framework. The final section analyzes national cyber capabilities and discusses the effectiveness of the WB3C as a form of regional cyber governance for the renewables sector. The conclusion reflects on the role of regional cyber governance in enhancing resilience to cyber threats in the renewable energy sector, making both

²² "Government Adopted Training Needs Analysis for Civil Servants and State Employees at Central and Local Level," Government of Montenegro, August 25, 2021, www.gov.me/en/article/244593--government-adopted-training-needs-analysis-for-civil-servants-and-state-employees-at-central-and-local-level.

²³ Julia Voo, Irfan Hemani, and Daniel Cassidy, "National Cyber Power Index 2022," Report (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022), <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.

²⁴ Hidetoshi Nakamura, "Regional Security Communities," in *Globalisation, Multilateralism, Europe: Towards a Better Global Governance?* ed. Mario Telò (London: Routledge, 2014), 333-345; "First G7 Cyber Group Agrees on Info-sharing to Defend Democracies," *DeCode39 Geopolitical Insights from Italy*, May 17, 2024, <https://decode39.com/9058/first-g7-cyber-group-agrees-on-info-sharing-to-defend-democracies/>.

²⁵ "CybilProject – WB6-EU Cooperation for Improving Cybersecurity in the Western Balkans."

²⁶ Jitske van Popering-Verkerk et al., "A Framework for Governance Capacity: A Broad Perspective on Steering Efforts in Society," *Administration & Society* 54, no. 9 (2022): 1767-1794, <https://doi.org/10.1177/00953997211069932>.

an empirical and conceptual contribution by bringing regionalism back into the cyber governance of energy systems in the Western Balkans.

Energy Security Dynamics and the Imperative for Cyber Regional Governance

This section explores whether the Western Balkans Cyber Capacity Center applies emerging regional cyber governance to the energy sector. It analyzes the strategic context, security dynamics, the goals of Western Balkan nations, and the development of cyber capabilities amid significant threats.

In November 2022, the Western Balkans Summit in Berlin endorsed the Declaration on Energy Security and the Green Transition in the Western Balkans.²⁷ The operationalization of such complex policy objectives has not been without precedent in the region, especially in light of efforts “to reduce the competitiveness of Russian gas versus (insufficiently competitive) LNG terminals in the region.”²⁸ Recognizing the significant political risks associated with their energy dependence on Russia, many governments in the region are actively pursuing connections to TANAP and TAP, which cross the Western Balkans, to enhance their energy security and independence.²⁹ However, gas supplies to the Western Balkans “are subject to competition for influence, where political interests of national and foreign actors often outweigh rational arguments in this debate.”³⁰

The Western Balkans lack indigenous energy resources. There are abundant coal deposits scattered across the region, with Kosovo even claiming the fifth-largest reserves in the world,³¹ while Serbia’s proven reserves correspond to 192 times its annual consumption.³² By contrast, most oil and natural gas entering the region are imported, given the absence of oil production and the low vol-

²⁷ Western Balkans Info Hub, “Declaration on Energy Security and Green Transition in the Western Balkans,” Berlin Process Summit, Berlin, November 3, 2022, www.berlinprocess.de/uploads/documents/energy-declaration-bp-2022_1678468873.pdf.

²⁸ RFE/RL’s Bulgarian Service, “Bulgaria Defends Decision to Impose Tax on Russian Gas Transit as Hungary, Serbia Vow to Respond,” *Radio Free Europe/Radio Liberty*, October 18, 2023, <https://www.rferl.org/a/bulgaria-defends-tax-russian-gas-hungary-serbia/32643100.html>.

²⁹ Pablo Ruiz Castello, Hrvoje Medarac, Julian Somers, and Mandras Giovanni, “Recent Trends in Coal and Peat Regions in the Western Balkans and Ukraine,” EUR 30837 EN (Luxembourg: Publications Office of the European Union, 2021), <https://doi.org/10.2760/81752>.

³⁰ Petr Čermák, “New Gas Supplies for the Western Balkans Facilitates a Geopolitical Game Rather Than the Green Energy Transition,” *Visegrad Insight*, February 14, 2024, <https://visegradinsight.eu/new-gas-supplies-for-the-western-balkans-facilitates-a-geopolitical-game-rather-than-the-green-energy-transition/>.

³¹ Castello, Medarac, Somers, and Giovanni, “Recent Trends in Coal and Peat Regions in the Western Balkans and Ukraine.”

³² Bechev, “Energy in the Western Balkans”; Frey, “The Energy Transition in the Western Balkans.”

umes of domestic natural gas production.³³ In the context of renewables, since the adoption of the Economic and Investment Plan (EIP) in October 2020, the European Union has approved €1.8 billion in investments in the Western Balkans, focusing on 40 flagship projects, most of which are related to clean energy.³⁴ According to EU statistics on renewable energy, Western Balkan countries accounted for 22% of their gross final energy consumption from renewable sources, with Albania leading the region in electricity production.³⁵

The deadlock in the region's energy transition is exploited by foreign investors who serve their governments and are in direct contact with their Western Balkan counterparts. Often, the connection is between political leaders, who act as the ultimate guarantors for external investors and effectively substitute for the rule of law.³⁶ In this sense, foreign influence in the Western Balkans' energy sector serves as a state policy tool that shapes the political economy of the region.³⁷ To promote employment and reduce energy prices for the population, Western Balkan countries have engaged in several regional initiatives, including the European Energy Union, the Energy Community, the Southern Gas Corridor Initiative, the EU Emissions Trading System, and the USAID Clean Energy Investment Project.³⁸

Table 1 summarizes the energy security dynamics in the Western Balkans' sectoral development relative to the EU average and key foreign influences in the region.

Control over energy resources is directly linked to the concept of energy security and its principles, including diversification of sources and routes, a country's position in the global energy market, its security margin, the efficient functioning of energy markets, and the formation of relationships with exporting nations.³⁹ In addition to these principles, control over energy resources is shaped

³³ Frey, "The Energy Transition in the Western Balkans," note 35.

³⁴ Marilen Martin, "More Than Just Money? EU Investments for Green Western Balkans," *OBC Transeuropa*, August 16, 2023, www.balkanicaucaso.org/eng/Areas/Balkans/More-than-just-money-EU-investments-for-green-Western-Balkans-226134.

³⁵ Eurostat, "Statistics Explained: Renewable Energy Statistics," December 2024, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.

³⁶ Tena Prelec, Nikolaos Tzifakis, and Dimitar Bechev, "Green Power Politics: External Actors and Energy Transition in the Western Balkans," HAL Open Science, March 2024, <https://hal.science/hal-04526114v1>.

³⁷ Sotirios Manolkidis, "Geopolitical Challenges and Cooperation in the European Energy Sector: The Case of SE Europe and the Western Balkans Six Initiative," in *Aspects of the Energy Union: Application and Effects of European Energy Policies*, 101-114, https://doi.org/10.1007/978-3-030-55981-6_5; Bechev, "Energy in the Western Balkans"; Frey, "The Energy Transition in the Western Balkans."

³⁸ "Balkan Energy Strategies," Balkan Economic Forum, 2023, <https://www.balkaneconomicforum.org/initiatives/events/balkan-economic-conference-2015/balkan-energy-strategies/>.

³⁹ Mathioulakis, "Strategic Elements of the Energy Union and the Role of Regulation."

Table 1. Energy Security Dynamics in the Western Balkans.

Country	Coal	Oil	Natural Gas	Renewables	Pipelines	Influence
Serbia	49.6%	22.0%	12.5%	15.8%	South Stream Serbia AG S. Caucasus Corridor	Russia China
North Macedonia	31.6%	41.4%	11.7%	15.2%	Alexandroupolis	Russia Türkiye
Montenegro	37.8%	32.5%	—	29.7%	IAP	—
Kosovo	57.4%	27.6%	—	15%	ALGOKAP	Türkiye
EU Average	11.0%	31.9%	25%	18.5%	—	—
BiH	53.8%	20.6%	2.3%	23.2%	IAP	Russia China
Albania	7.7%	53%	2.1%	37.3%	IAP-TAP ALGOKP S. Caucasus Corridor	—

Source: Adapted from Frey, “The Energy Transition in the Western Balkans.”

by the relationship between importers and exporters. The importer relies on the energy resource, while the exporter seeks a stable market. This interdependence is crucial, as it affects the foreign policy and energy security strategies of the countries involved. This consideration underscores the growing importance of the energy revolution, “where security, sovereignty, and solidarity shape a revised geopolitical energy landscape.”⁴⁰

To achieve energy sovereignty, a nation must also ensure cyber sovereignty.⁴¹ As the global clean energy race intensifies, countries are aiming for resource self-sufficiency. The dynamics of change will hinge on innovation, making

⁴⁰ Michael Carnegie LaBelle, “Breaking the Era of Energy Interdependence in Europe: A Multidimensional Reframing of Energy Security, Sovereignty, and Solidarity,” *Energy Strategy Reviews*, no. 52 (2024): 101314, <https://doi.org/10.1016/j.esr.2024.101314>.

⁴¹ On UN principles in cyber and energy sovereignty, see Megghi Pengili and Slawomir Raszewski, “Transnational Cyber Governance for Risk Management in the Gas Sector: Exploring the Potential of G7 Cooperation,” *Gases* 4, no. 4 (2024): 327-350, <https://doi.org/10.3390/gases4040019>. For the principles of the UN Charter and cyber operations, see UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, June 24, 2013, paras 19–20; UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, July 22, 2015, para 28(b). The 2015 UN GGE also agreed on 11

investments in energy infrastructure essential. Especially given the rising conflicts in areas such as Lebanon and Russia, where attacks have surged amid the ongoing invasion of Ukraine, energy infrastructure around the world is at risk.⁴² Additionally, technologies such as artificial intelligence and elastocalorics are influencing renewable energy supply chains.⁴³

Following the unprecedented series of cyberattacks between 2022 and 2023, the Western Balkan economies have taken steps to enhance the cybersecurity of critical infrastructure at both the national and regional levels. In response, in September 2024, the WB3C, in collaboration with the Dutch National Cyber Security Center (NCSC-NL), conducted training sessions for Western Balkan governments that were also relevant to energy security. The sessions focused on operational technology, cyber-resilient ecosystems, and critical information infrastructure protection.⁴⁴

While the national framework includes the establishment of CIRTs, as well as legal and institutional management frameworks, the regional dimension was consolidated with the establishment of the WB3C in Podgorica in 2024. The center's regional scope provides EU-standard training activities to strengthen national cyber capabilities in the fields of cybercrime, cybersecurity, and digital diplomacy. In addition, WB3C aims to strengthen regional operational and institutional responses to cyber threats and attacks.⁴⁵

To ensure the cyber secure operation of critical energy infrastructure, the Western Balkan countries have taken several measures. For example, Albania has implemented key legislative measures to improve electronic communications and cybersecurity, including a law on the development of electronic communication networks and the first national cybersecurity regulation for the electricity sector.⁴⁶ In 2017, the Albanian Parliament approved a comprehensive cybersecurity law. Additionally, essential elements are included in the National

voluntary, non-binding norms, rules, and principles of responsible state behavior in the ICT environment (para 13).

⁴² Adam Taylor, "Data Shows Global Conflict Surged in 2024," *The Washington Post*, December 12, 2024, www.washingtonpost.com/world/2024/12/12/conflict-war-2024-israel-gaza-ukraine/. Conflicts have doubled over the past five years, according to the Armed Conflict Location & Event Data Project, "Conflict Index Results: December 2024," <https://acleddata.com/report/conflict-index-results-december-2024>.

⁴³ "Top 10 Emerging Technologies 2024," World Economic Forum, <https://intelligence.weforum.org/collection/59bc981b-9585-4171-9573-4f78e0fbea51>.

⁴⁴ Western Balkans Cyber Capacity Centre (WB3C), "Operational Technology, Cyber Resilient Ecosystems, and Critical Information Infrastructure Protection: Enhancing Cybersecurity Proficiency for Western Balkans Administrations," September 6, 2024, <https://wb3c.org/event/7/operational-technology-cyber-resilient-ecosystems-and-critical-information-infrastructure-protection-enhancing-cybersecurity-proficiency-for-western-balkans-administrations>.

⁴⁵ "CybilProject – WB6-EU Cooperation for Improving Cybersecurity in the Western Balkans."

⁴⁶ Popovski et al., "Crisis Prevention and Critical Infrastructure in the Western Balkans."

Civil Protection Plan, with major operators such as the Electricity Distribution Operator and the Trans Adriatic Pipeline working on robust business continuity plans.⁴⁷

In North Macedonia, the critical infrastructure law is under development, and critical infrastructure aspects are significantly mainstreamed in other acts, such as the regulation on integrated risk and hazard assessment. In conclusion, in addition to these national efforts, Western Balkan countries have demonstrated their regional orientation toward alignment with EU policies and strategies, as exemplified by the adoption of the NIS Directive, which also includes provisions related to the energy sector and the protection of its infrastructure.

By the end of 2019, Albania and North Macedonia had adopted the NIS Directive and included the energy sector. Bosnia and Herzegovina, Montenegro, Serbia, and Ukraine had adopted the directive, without explicitly covering the energy sector, while Georgia, Kosovo, and Moldova were in the process of transposing the NIS Directive.⁴⁸

To address increasing exposure to cyberattacks, the NIS2 Directive (2022) mandates that EU member states adopt national cybersecurity strategies, including policies on supply chain security, vulnerability management, and cybersecurity education and awareness.⁴⁹ This is particularly important given the potential of cyberattacks to cause disruption.⁵⁰ From ransomware to cyber weapons, these attacks fundamentally undermine three crucial cybersecurity principles: confidentiality, integrity, and availability, which are essential for protecting digital assets. Given the interdependence of energy systems and infrastructure, disruptions to access can jeopardize the entire system, making violations of these principles a significant risk. Thus, strengthening our understanding of these categories is vital for robust cybersecurity. The next section details the method used to explore this article's central question: Is regional cyber governance in the energy sector emerging within the framework of the WB3C?

⁴⁷ Popovski et al., "Crisis Prevention and Critical Infrastructure in the Western Balkans," note 48.

⁴⁸ Blueprint Energy Solutions, *Final Report – Study on Cyber Security in the Energy Sector of the Energy Community*, Energy Community, Document No. FINR-CS-EC-211019 (Vienna: Blueprint Energy Solutions GmbH, December 2019), www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf.

⁴⁹ European Commission, "NIS2 Directive: Securing Network and Information Systems," Directive 2022/2555, European Commission – Shaping Europe's Digital Future, 2022, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.

⁵⁰ Don C. Smith, "Cybersecurity in the Energy Sector: Are We Really Prepared?" *Journal of Energy & Natural Resources Law* 39, no. 3 (2021): 265-270, <https://doi.org/10.1080/02646811.2021.1943935>.

Assessing Regional Cyber Governance: Bridging Institutional Analysis and the Capability-Building Approach

This section outlines the combined methodological framework, built upon institutional analysis and the capability approach, used to examine the emergence of the Western Balkans Cyber Capacity Center (WB3C) as a form of regional cyber governance. While institutional analysis outlines governance activities to assess their performance and prompt policy change,⁵¹ the capability-building approach acknowledges that governance agents must possess the capabilities required to operate effectively and generate policy change.⁵² In empirical terms, while institutional analysis examines collective institutional actions within the WB3C, the capability approach explores how the Center, as a concerted agency, is enhanced by national decisions to address regional protection of power plants when national capabilities are limited (see the Data section for related evidence).

Julian Bass and colleagues justify the combination of institutional theory and the capability approach in the information and technology domain because both “share neoclassical economics roots and thus are commensurable.”⁵³ Adding to this consideration, while the capability approach investigates the choices and resources available for policy effectiveness, institutional design analysis considers policy effectiveness as the result of a process of institutional change,⁵⁴ which, for this article, is the emergence of regional cyber governance through the WB3C. This form of regional governance emerges through institutional efforts at the national level, which can promote consensus at the regional level through norms, best practices, technical standards, rules, and priorities, while also endorsing capability-building projects.⁵⁵

⁵¹ Margaret M. Polski and Elinor Ostrom, “An Institutional Framework for Policy Analysis,” in *Elinor Ostrom and the Bloomington School of Political Economy: Volume 3, A Framework for Policy Analysis*, ed. Daniel H. Cole and Michael D. McGinnis (Lexington Books, 2017), 13-47, <https://doi.org/10.5040/9781666993875.ch-002>.

⁵² Stephen L. Esquith and Fred Gifford, eds., *Capabilities, Power, and Institutions: Toward a More Critical Development Ethics* (Pennsylvania: The Pennsylvania State University Press, 2010).

⁵³ Julian M. Bass, Brian Nicholson, and Eswaran Subrahmanian, “A Framework Using Institutional Analysis and the Capability Approach in ICT4D,” *Information Technologies and International Development* 9, no. 1 (2013): 19-35, <https://itidjournal.org/index.php/itid/article/view/1028.html>, 22.

⁵⁴ Sophie Vanhoonacker-Kormoss and Karolina Pomorska, “The Institutional Framework,” in *International Relations and the European Union*, ed. Christopher Hill, Michael Smith, and Sophie Vanhoonacker (Oxford University Press, 2011), 76-100.

⁵⁵ Enrico Calandro and Nils Berglund, “Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case,” University of Cape Town, Graduate School of Business, 2019, https://researchictafrica.net/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf.

In cybersecurity, capabilities are built through expertise, infrastructure, technologies, and other organizational resources.⁵⁶ Capability building serves as a mechanism for transforming institutions and developing competencies, enabling them to contribute effectively to sustaining national development processes. One such process is the digitalization of the economy, which necessitates a form of cyber governance capable of understanding both threats and opportunities in the digital space. The building of cyber capabilities contributes to this situational awareness.

The selection of WB3C as a case study is determined by the geopolitical context, institutional evolution at the national and regional levels, the economic development of the Western Balkans members, and their ambition to strengthen energy and cyber resilience. The foundations of regional cyber governance in the Western Balkans were laid in 2018 with the Regional Cooperation Council (RCC) strategic document “A New Virtual Battlefield – How to Prevent Online Radicalisation in the Cyber Security Realm of the Western Balkans.”⁵⁷ The RCC strategy advances the following objectives: (i) raising awareness among decision-makers; (ii) supporting better cybersecurity coordination at the national level; and (iii) strengthening the capacity of national/ governmental CSIRTs in the Western Balkans to respond effectively to incidents.⁵⁸ This strategy defines cyber governance both as a commitment and as a prerequisite for effective risk-management policies for critical energy infrastructure.⁵⁹ In light of this background, the discussion continues with a brief overview of the methodology and the data supporting the analysis.

Institutional Analysis and Capability Approach

The article builds its methodological framework on the scheme proposed by Bass and colleagues, which links three dimensions: institutional theory, the capability approach, and information and communication technology.⁶⁰ This diagram further connects the six elements of the Institutional Analysis and Design (IAD)

⁵⁶ Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford: Oxford University Press, 2022), 9-10.

⁵⁷ Maura Conway and Sheelagh Brady, “A New Virtual Battlefield – How to Prevent Online Radicalisation in the Cyber Security Realm of the Western Balkans,” Policy Report (Sarajevo: Regional Cooperation Council, 2018); Dražen Maravić, “Cybersecurity Policy Development and Capacity Building – Increasing Regional Cooperation in the Western Balkans” (Geneva: Geneva Centre for Security Sector Governance, 2021), www.dcaf.ch/sites/default/files/publications/documents/CybersecurityPolicyDevelopment_CapacityBuilding_in_WB_mar2021.pdf.

⁵⁸ Geneva Centre for Security Sector Governance, “National Cybersecurity Strategies in Western Balkan Economies” (Geneva: DCAF, 2021), www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf.

⁵⁹ Blueprint Energy Solutions, *Final Report – Study on Cyber Security in the Energy Sector*.

⁶⁰ Bass, Nicholson, and Subrahmanian, “A Framework Using Institutional Analysis and the Capability Approach in ICT4D.”

framework—as illustrated in Figure 1—to the policy problem: “physical and material conditions, community attributes (culture), rules-in-use, action arena, patterns of interaction, and outcomes.”⁶¹

The physical and material environment reflects events and situations that affect regional cyber risk management engagement. The Western Balkans community’s attributes include shared interests, common understanding, political communication, and economic and political features. At the same time, rules-in-use encompass formal and informal regulatory frameworks that legitimize policy actions. The operational activities of all actors are examined in the action arena, which analyzes their decision-making skills and determines interaction patterns, including policy action structures and actor behaviors. By analyzing interaction patterns, it is possible to gauge how effectively cyber policies address uncertainties in the energy sector.

Figure 1 illustrates the methodological framework. It introduces an interdependent relationship between cyber governance, the capability-building approach, and Institutional Analysis and Design (IAD). These elements are organized across three dimensions of relationships. Dimension A links capabilities to institutions; Dimension B links governance to capabilities; and Dimension C concerns the relationship between governance and institutions. In this analysis, each dimension is characterized by promoters and inhibitors of the relationship, as defined by the six IAD areas.⁶² For example, the relationship between institutions and governance in Dimension C can be affected positively or negatively by physical and material conditions. IAD areas strengthen or erode governance and determine institutional arrangements in essential ways. In Dimension B, the relationship between capability and governance can be influenced by two other IAD areas: rules-in-use, including regulations, norms, strategies, and laws; and the operational activity of all policy actors. Dimension A, in turn, centers on capability building and institutions. Since individuals operate within a world of institutions, and institutions in turn operate through actors, “their opportunities depend on what institutions exist and how they function.”⁶³

Data Elaboration

The sources investigated for the study question on regional cyber governance for energy-sector risk management included journal articles, book chapters, government reports, institutional research papers, newspapers, academic studies, and online databases. The data analysis was organized into three distinct sets. The first set examined national cyber governance, regulatory frameworks, cyber decision-making, and research studies and publications from international agencies within NATO, the European Union, the OSCE, and DCAF. The second examined the capacities of Western Balkan countries for cybersecurity of critical in-

⁶¹ Polski and Ostrom, “An Institutional Framework for Policy Analysis,” 16-17.

⁶² Polski and Ostrom, “An Institutional Framework for Policy Analysis,” note 62.

⁶³ Amartya Sen, *Development as Freedom* (Oxford University Press, 1999), 192.

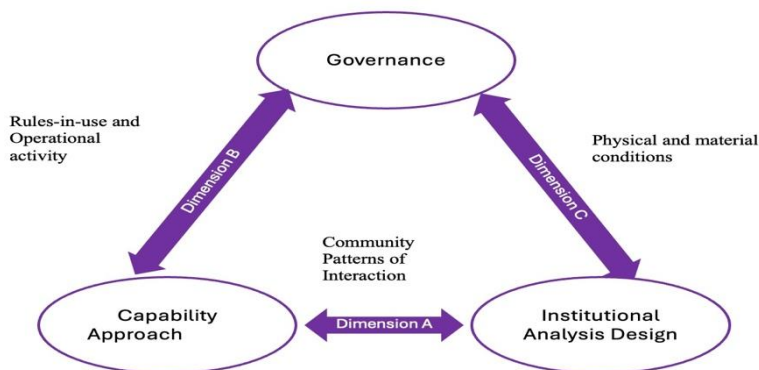


Figure 1: The Methodological Framework.

frastructures. The third set of data addressed the emergence of regional governance and public-private engagement in the cyber protection of energy infrastructure at the national and regional levels.

National Cyber Governance Capabilities

This section examines the dynamics of energy cybersecurity. The discussion begins by addressing cyber risk priorities, moves on to evaluate national cyber governance capabilities, and concludes with an analysis of how these capabilities enhance the effectiveness of cyber governance at the Western Balkans Cyber Capacity Center (WB3C).

Cyber Risk Management

Cyber risk management is a process conceptualized to help public and private sectors, organizations, institutions, and businesses protect assets and mitigate intrusions by detecting vulnerable assets and threats. The process comprises determining the likelihood of a threat and its potential impact on assets, and implementing security measures, incident response plans, and personnel training.⁶⁴ “Cyber risks range from technological dependence and loss of strategic autonomy of the state to anthropogenic threats, in which human error is added to the initiatives of hostile actors, characterized by different degrees of sophistication and driven by different, but equally harmful, intentions.”⁶⁵ These risks range from cybercrime and cyber-espionage to misinformation, intelligence gathering, sabotage, and revenge.

⁶⁴ “What Is Cyber Risk Management?” IBM, 2023, accessed July 18, 2025, <https://www.ibm.com/think/topics/cyber-risk-management>.

⁶⁵ National Cybersecurity Agency of Italy, “National Cybersecurity Strategy 2022–2026,” 2022, www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6, 4-5. – in Italian

Risk management plans in national cyber strategies call for remaining technologically sophisticated and adaptive, and for investing in collaborative civil-military capabilities to mitigate cyberattacks.⁶⁶ General cybersecurity rules and energy system and network guidelines describe the relevant procedures. These standards cover everything from a unified cybersecurity protection system to a cyber threat early warning system. Although these rules govern threat response, resilience by design emphasizes the need for cyber governance capabilities.

National Cyber Governance Capabilities

The countries of the Western Balkans have developed their cyber governance capabilities in alignment with EU-specific regulations, requirements, and obligations, deriving from international commitments, such as Directive 2008/114 on critical infrastructure (CI), the NIS2 Directive, the Council of Europe Convention on Cybercrime, and Directive 2013/40/EU of the European Parliament and of the Council “on attacks against information systems.”⁶⁷ Table 2 summarizes the national-level organizational cyber-energy governance structures and is followed by a brief description of each country’s efforts to enhance cyber proficiency.

Albania is making moderate progress in public administration reform, focusing on regulatory impact assessments, policy planning, e-services, and data transparency. However, managerial accountability remains weak, with centralized decision-making and limited delegation of authority. Governance lacks clear strategic plans and accountability mechanisms.⁶⁸ The National Cybersecurity Strategy 2020–2025 is the latest relevant document,⁶⁹ and Albania ranks between 85th and 95th globally and 40th in Europe for cybersecurity,⁷⁰ reflecting strong legal norms but requiring improvement in collective security measures.

The most recent document is the Strategy of *Bosnia and Herzegovina* for Prevention and Combating Terrorism 2015–2020.⁷¹ The EU’s 2020 progress report indicates that Bosnia and Herzegovina is still at an early stage of public admin-

⁶⁶ Eric Luijff, Kim Besseling, and Patrick de Graaf, “Nineteen National Cyber Security Strategies,” *International Journal of Critical Infrastructures* 9, no. 1-2 (2013): 3-31, <https://doi.org/10.1504/IJCIS.2013.051608>; Blueprint Energy Solutions, *Final Report – Study on Cyber Security in the Energy Sector of the Energy Community*, 28.

⁶⁷ Blueprint Energy Solutions, *Final Report – Study on Cyber Security in the Energy Sector of the Energy Community*, note 67; BluePrint’s report: ENTSG19 started collaborating in GIE (Gas Infrastructure Europe) Cybersecurity Taskforce to build a common understanding of key areas of importance for strengthening cybersecurity of network code for the gas sector. Albania, Bosnia and Herzegovina, Republic of North Macedonia are observers in ENTSG22.

⁶⁸ ITU, *Global Cybersecurity Index 2024* (Geneva: International Telecommunication Union, 2024), <https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024/en>.

⁶⁹ “Albania – Cybersecurity Policy,” Cyber Policy Portal, <https://cyberpolicyportal.org/states/albania>.

⁷⁰ ITU, *Global Cybersecurity Index 2024*.

⁷¹ “Bosnia and Herzegovina – Cybersecurity Policy,” Cyber Policy Portal, <https://cyberpolicyportal.org/states/bosnia-and-herzegovina>.

Table 2. Assessment of National Cyber Organizational Structures.

Assessment of organizational structures				
Contracting Party	National CS Authority	NIS SPoC	CI protection SPoC	CSIRT
Albania	NAECCS	NAECCS	Not established	NAECCS
Bosnia and Herzegovina	Not established	Not established	Not established	Not established
Georgia	DEA	DEA	Not established	DEA CERT
Kosovo^c	KOS-CERT	KOS-CERT	Not established	KOS-CERT
Moldova	Ministry of Economy and Infrastructure	Ministry of Economy and Infrastructure	Anti-Terrorist Center of Information and Security Service	CERT-GOV-MD
Montenegro	CIRT-ME	CIRT-ME	Not established	CIRT-ME
North Macedonia	Not established	MKD-CIRT	Not established	MKD-CIRT
Republic of Serbia	Ministry of Trade, Tourism and Telecommunications	Ministry of Trade, Tourism and Telecommunications	Ministry of Internal Affairs	RATEL CERT
Ukraine	State Service on Special Communication and Information Protection	CERT-UA	Not established	CERT-UA

Source: Adapted from Maravić, “Cybersecurity Policy Development and Capacity Building” and Blueprint Energy Solutions Report.

istration reform, lacking significant progress in establishing a professional civil service and coordinated policy-making.⁷² While a strategic framework has been adopted, the action plan still requires implementation, and a coordinating political body has not yet been established. Effective governance is crucial for improving cybersecurity.⁷³ Bosnia and Herzegovina ranks between 20th and 55th globally, in Tier 4 among 192 countries, and 43rd in Europe for cybersecurity,

⁷² European Commission, “Key Findings on the 2020 Report on Bosnia and Herzegovina,” Press Corner, October 6, 2020, https://ec.europa.eu/commission/presscorner/detail/en/country_20_1793; European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, “Bosnia and Herzegovina Report 2020,” October 6, 2020, https://enlargement.ec.europa.eu/bosnia-and-herzegovina-report-2020_en.

⁷³ European Commission, “Bosnia and Herzegovina Report 2020,” note 73.

according to the Global Cybersecurity Index 2024.⁷⁴ The Index notes strengths in legal norms but identifies a need for enhanced organizational measures.⁷⁵

Kosovo has made progress in reforming its public administration and improving cybersecurity, but challenges remain. The annual EU progress report notes that political influence in the recruitment of senior civil servants and non-merit-based hiring undermine trust in public administration.⁷⁶ Limited funding for the Kosovo Institute for Public Administration restricts training and professional development for civil servants. Additionally, weaknesses in leading and coordinating the reform process persist, with many institutions still operating independently of centrally developed electronic identification (eID) tools. Systematic feedback mechanisms from citizens and businesses regarding service delivery are also lacking. The latest document in this area is the National Cyber Security Strategy 2023–2027,⁷⁷ and Kosovo is not ranked in the Global Cybersecurity Index 2024.⁷⁸

Montenegro is moderately prepared for public administration reform, as noted in the EU's 2020 progress report.⁷⁹ Significant political will is essential to depoliticize the public sector and enhance managerial accountability. Montenegro must also address systemic issues in its criminal justice system, particularly those related to organized crime. Law enforcement agencies should improve database access, create an interoperable system, employ appropriate investigative measures, and expand expertise in financial investigations and cybercrime. The National Cybersecurity Strategy 2022–2026 is currently in effect. According to the Global Cybersecurity Index 2024, Montenegro ranks between 55th and 85th among 192 countries, in Tier 3 for developing cyber governance, and 41st in Europe for cybersecurity, demonstrating strengths in cooperative measures and capacity development.⁸⁰

North Macedonia is moderately prepared for public administration reform, as noted in the EU's 2020 progress report.⁸¹ The Ministry of Information Society

⁷⁴ ITU, *Global Cybersecurity Index 2024*.

⁷⁵ Cyber Policy Portal, "Bosnia and Herzegovina – Cybersecurity Policy."

⁷⁶ European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Kosovo Report 2024," https://enlargement.ec.europa.eu/kosovo-report-2024_en.

⁷⁷ Kosovo Ministry of Internal Affairs, "National Cyber Security Strategy 2023–2027," September 2023, <https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2692/Strategija%20p%C3%ABr%20Siguri%20Kibernetike%20-%20ENG..pdf>.

⁷⁸ ITU, *Global Cybersecurity Index 2024*.

⁷⁹ European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Montenegro Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/montenegro-report-2020_en.

⁸⁰ ITU, *Global Cybersecurity Index 2024*.

⁸¹ European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "North Macedonia Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/north-macedonia-report-2020_en.

and Administration has enhanced its role in managing human resources, but professional development remains unsystematic, with no centralized training database. While the country has made progress in improving managerial accountability and delegating responsibilities, decision-making authority for middle management remains limited. The National Cyber Security Council was established in July 2019.⁸² As part of its Digital Agenda, North Macedonia implemented the 2019–2023 national broadband strategy and the 2018–2022 national cybersecurity strategy.⁸³ The Global Cybersecurity Index 2024 ranks North Macedonia between 55th and 85th globally and 24th in Europe for cybersecurity, highlighting strengths in legal norms while indicating a need for improvement in technical measures.⁸⁴

The EU's 2020 Progress Report for *Serbia* finds that the country is moderately prepared for public administration reform. However, overall, the government has made no progress, as public administration services have not reduced the excessive number of senior management positions.⁸⁵ Digitalization continues to top the list of government priorities. The government adopted the 2020–2024 Strategy for Digital Skills Development in February 2020. In addition, the amended Law on Information Security was adopted in October 2019, aiming to further align the national framework with the EU Directive on security of network and information systems.⁸⁶

RATEL (the consortium of state agencies) became an associate member of the expert group on the resilience and security of communication infrastructure, networks, and services at the European Union Agency for Cybersecurity (ENISA).⁸⁷ The most recent document is the National Cybersecurity Strategy, adopted in 2021. Serbia is ranked 95th–100th out of 192 countries, in Tier 1: Role Modeling, and 25th on a European scale in cybersecurity, according to the Global Cybersecurity Index 2024.⁸⁸ According to the Index, Serbia's strength lies in legal measures, while capacity development remains an area for improvement.⁸⁹

The development of national cyber capabilities is constrained by the Western Balkans' diverse alliances and memberships in international arrangements, which are important for international cybersecurity collaboration and partnerships. Albania, Montenegro, and North Macedonia are all members of the OSCE, NATO, ITU, and the UN. Bosnia and Herzegovina and Serbia are members of the Partnership for Peace/NATO, the OSCE, ITU, and the UN.

⁸² European Commission, "North Macedonia Report 2020," note 82.

⁸³ Maravić, "Cybersecurity Policy Development and Capacity Building."

⁸⁴ ITU, *Global Cybersecurity Index 2024*.

⁸⁵ European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Serbia Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/serbia-report-2020_en.

⁸⁶ ENISA, "2024 Report on the State of the Cybersecurity in the Union."

⁸⁷ ENISA, "2024 Report on the State of the Cybersecurity in the Union," note 88.

⁸⁸ ITU, *Global Cybersecurity Index 2024*.

⁸⁹ ITU, *Global Cybersecurity Index 2024*, 90.

Cybersecurity risks trigger changes in governance systems, encouraging public-private collaboration and decision-making platforms, namely public-private partnerships (PPPs). Western Balkan governments are engaging positively with the private sector, both within and beyond national borders, to develop new managerial practices for cyber resilience based on trust-driven public-private partnerships.⁹⁰ Cooperation with the private sector arises from its capacity and flexibility to address challenges related to the protection of critical infrastructure.⁹¹ Furthermore, cooperation with industry is important for governments in establishing and expanding a single cybersecurity market and aligning cybersecurity regulatory frameworks across countries with regional affinities and strategic interests.⁹² As regards the WB3C, as a regional organization, its current activities demonstrate its key role in stimulating joint capabilities among countries, implementing agreed norms to enhance stability and security, and fostering further progress at the multilateral level.⁹³

Successful examples of collaboration between state agencies and the private sector include North Macedonia's National Center for Computer Incident Response, which facilitates policy discussions and information sharing, and Serbia's Cybersecurity Network Foundation, which integrates various stakeholders, such as medium-sized and small enterprises, telecommunications companies, internet service providers, banks, vendors, and operators of critical infrastructures, including energy companies, academia, and civil society organizations.⁹⁴

⁹⁰ Max Manley, "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership," *Journal of Strategic Security* 8, no. 3 Suppl. (2015): 85-98, <http://dx.doi.org/10.5038/1944-0472.8.3S.1478>.

⁹¹ Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016): 43-62, 56, <https://doi.org/10.1111/1468-2346.12504>.

⁹² European Union Agency for Network and Information Security, "Public Private Partnerships (PPP): Cooperative Models," November 2017, www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-3%203%20Public%20Private%20Partnerships%20%28PPP%29%20Cooperative%20models.pdf. See also European Parliament and the Council, "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)," *Official Journal of the European Union*, December 27, 2022, <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.

⁹³ UN Institute for Disarmament Research & the Center for Strategic and International Studies, "The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities," Report of the 2nd International Security Cyber Workshop Series, Geneva, Switzerland, January 24, 2019, <https://unidir.org/publication/the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability/>.

⁹⁴ Blueprint Energy Solutions, *Final Report – Study on Cyber Security in the Energy Sector of the Energy Community*.

Despite their benefits, contractual collaborations between the public and private sectors can have drawbacks, such as the potential for increased governmental influence in cybersecurity, which can pose challenges related to accountability and conflicts between national and economic interests that do not always align.⁹⁵ Ultimately, enhancing knowledge of cyber threats through collaborative projects between state-level institutions and the cyber industry fosters the sharing of best practices and supports the overall development of cyber governance, infrastructure capabilities, and resilience, based on a common understanding among all stakeholders.

Is WB3C Materializing as Regional Cyber Governance?

The findings from the evaluation of national cyber governance capabilities presented above allow us to extend the analysis to the regional context of the WB3C. Regional cyber governance is gaining momentum amid the development of the renewable energy sector and the presence of shared energy infrastructure and systems. In the energy transition process, energy and natural resources companies operate across borders and must simultaneously manage challenges related to the security of technologies, information, and data.

Even though regional countries have set targets for renewable energy sources (RES) in their energy policies, there are gaps between these targets and actual results, as national governments face various energy challenges related to regulatory frameworks, planning processes, and limited market integration.⁹⁶ Besides these hurdles, the Western Balkans is not immune to the broader energy crisis, which has had a global impact. Anna-Maria Boromisa comments that “the crisis has highlighted the challenge of increasing short-term energy security while implementing a transition to green energy sources.”⁹⁷ In response to this challenge, the countries endorsed, as part of the Berlin Process in 2022, the Declaration on Energy Security and Green Transition in the Western Balkans.⁹⁸ The signatories to the declaration committed to developing regionally coordinated mechanisms and measures to secure the just transition process and energy supply chains, along with joint investment proposals in renewable energy and the

⁹⁵ Nathan E. Busch and Austen D. Givens, “Public-Private Partnerships in Homeland Security: Opportunities and Challenges,” *Homeland Security Affairs* 8, Article 18 (2012), <https://www.hsaj.org/articles/233>.

⁹⁶ Milena Rajić, Emanuele Quaranta, Alban Kuriqi, and Egidijus Kasiulis, “Renewable Energy in the Western Balkans and EU Policy: Pathway to Regional Net-Zero,” in *IOP Conf. Series: Earth and Environmental Science* 1442 (2025): 012002, <https://doi.org/10.1088/1755-1315/1442/1/012002>.

⁹⁷ Ana-Maria Boromisa, “Transition to Clean Energy Must Clear Economic and Geopolitical Hurdles,” *per Concordiam* 13, no. 2 (2025): 52-59, <https://perconcordiam.com/energy-challenges-in-the-western-balkans/>.

⁹⁸ Western Balkans Info Hub, “Declaration on Energy Security and Green Transition in the Western Balkans.”

integration of electricity and gas markets.⁹⁹ This energy juncture for regional sovereignty—besides the fatigued EU integration process—appears to have placed the region’s national governments on a path toward regional cyber sovereignty, a development that seems increasingly unavoidable. It may well serve as a starting point for other path-dependent processes, such as project learning and organizational integration.¹⁰⁰

This article views project learning as a means of building regional cyber capability by leveraging national cyber capabilities, while focusing on the need to enhance policy effectiveness for energy security. Organizational integration, in turn, can stimulate the transfer of best practices and resource allocation from partners to WB3C within the framework of the Joint Partnership for Strengthening Cyber Resilience in the Western Balkans, established under the Berlin Process in 2022.¹⁰¹ France, Italy, Germany, and the United Kingdom are among the pioneers of G7 cyber governance for energy systems because of their national cyber-power performance, trust, and strong record of working together on clustered cyber governance.¹⁰²

These Berlin Process partners, along with the European Union, UN, NATO, and OSCE, have supported regional cyber capability building through programs and initiatives within and beyond the WB3C,¹⁰³ such as the Cybersecurity Governance in the Western Balkans initiative (UK-led)¹⁰⁴; Protection of Public Spaces

⁹⁹ Engjellushe Morina, “Power of Need: Energy Security in the Western Balkans,” European Council on Foreign Relations, August 2, 2022, <https://ecfr.eu/article/power-of-need-energy-security-in-the-western-balkans/>.

¹⁰⁰ Giovanni Capoccia and R. Daniel Kelemen, “The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism,” *World Politics* 59, no. 3 (2007): 341–369, <https://doi.org/10.1017/S0043887100020852>.

¹⁰¹ “Berlin Process Summit 2024,” point 43.

¹⁰² “Agreement Establishing the Western Balkans Cyber Capacity Centre (WB3C),” signed by France, Slovenia, and Montenegro, Tirana, October 16, 2023, <https://wb3c.org/landing-page/WB3C%20AGREEMENT%20EN.pdf>. See also Pengili and Raszewski, “Transnational Cyber Governance for Risk Management in the Gas Sector”; ITU, *Global Cybersecurity Index 2024*.

¹⁰³ Fabio Barbero and Nils Berglund, “Cybersecurity Capacity Building and Donor Coordination in the Western Balkans,” Geneva Centre for Security Sector Governance, May 7, 2021, www.dcaf.ch/cybersecurity-capacity-building-and-donor-coordination-western-balkans; “Project: EU External Cyber Capacity Building Training for the Western Balkans, Eastern Partnership and Southern Neighbourhood,” *Cybil Portal*, 2022, <https://cybilportal.org/projects/eu-external-cyber-capacity-building-training-for-the-western-balkans-eastern-partnership-and-southern-neighbourhood/>; “Project: Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia,” *Cybil Portal*, 2023, <https://cybilportal.org/projects/cybersecurity-rapid-response-for-albania-montenegro-and-north-macedonia/>.

¹⁰⁴ Barbero and Berglund, “Cybersecurity Capacity Building and Donor Coordination.”

and Critical Infrastructures in the Western Balkans (France-led)¹⁰⁵; the Global Forum on Digital Security for Economic Prosperity (France-led)¹⁰⁶; the Cyber IPA Programmes (EU-led)¹⁰⁷; Cyber Incident Management and Critical Information Protection (EU-led)¹⁰⁸; and Confidence-Building Measures (OSCE-led).¹⁰⁹ Consequently, the approach to cyber capacity development in the region is shaped not only by the motivations of the actors involved but also by a broader geopolitical context that seeks to advance regional interests.

In conclusion, tackling cybersecurity threats requires collaboration that transcends national borders, as these threats are inherently cross-border and can significantly affect the region's economies and societies. The Western Balkan countries, through the Cyber Capacity Center in Montenegro, can lead efforts to promote collaborative frameworks, build cyber resilience, enhance governance, and tackle global cybersecurity challenges. Table 3 applies the key findings generated in the previous sections to the combined IAD-capability-building framework in order to evaluate the potential for a regional cyber governance framework formed by the Western Balkan countries and its effectiveness in reducing uncertainty and managing cyber threats.

Table 3. Institutional Design and Capability-Building Approach of WB3C as a Regional Cyber Governance Framework.

IAD Domain	WB Countries	Capability-Building Dimension
Policy Analysis Objective and Analytic Approach	Objective: Regional cyber governance in energy Approach: Cyber governance capabilities of each WB6 member Donor, national, and multistakeholder projects in cyber governance related to RES and energy security as domains of interest for WB6 members	

¹⁰⁵ "Project: Enhancing Protection of Public Spaces and Critical Infrastructures in the Western Balkans," *Cybil Portal*, 2023, <https://cybilportal.org/projects/enhancing-protection-of-public-spaces-and-critical-infrastructures-in-the-western-balkans/>.

¹⁰⁶ International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment* (London: IISS, 2021), 62, <https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power>.

¹⁰⁷ Barbero and Berglund, "Cybersecurity Capacity Building and Donor Coordination in the Western Balkans."

¹⁰⁸ "Western Balkans Projects," *Cybil Portal*, <https://cybilportal.org/?s=western+balkans>.

¹⁰⁹ Organization for Security and Co-operation in Europe, "10 Years of OSCE Cyber/ICT Security Confidence-Building Measures," October 2023, https://www.osce.org/files/f/documents/f/7/555999_1.pdf.

IAD Domain	WB Countries	Capability-Building Dimension
Physical and Material World	Synchronous liberalization of energy markets Maturity of cyber capabilities: Tier 1 – North Macedonia and Serbia; Tier 2 – Albania and Montenegro; and Tier 3 – Bosnia and Herzegovina, Kosovo The cyber culture of the state is limited to technical cooperation and capacity-building development National legislation has limited scope and impact in protecting energy infrastructure Missing discussion on cyber and energy sovereignty Top renewables: Albania, Montenegro Top importers: All WB transit hubs: Albania, Bosnia and Herzegovina, North Macedonia, Serbia, Montenegro, and Kosovo	Cyber Governance – Institutions
Community	Contractual Security Community, presence of mechanisms for non-violent conflict resolution; sustained efforts to ensure democratic legitimacy within and between states; and participatory decision-making Countries are bound by adherence to international community arrangements Shared strategic and economic interests	Institutions – Cyber Capabilities
Rules-in-use	National cyber strategies and regulatory frameworks Digital transformation strategies¹¹⁰ EU regulations adopted in order to fulfill strategic priorities¹¹¹	Cyber Capability – Cyber Governance

¹¹⁰ Mihkel Lauk and Juhani Lemmik, “Western Balkans Regional Study on Digitalisation in Government” (Podgorica, Montenegro: Regional School of Public Administration, 2023), www.respaweb.eu/download/doc/Western+Balkan+Regional+Study+on+Digitalization+in+Government.pdf/0aa384ee7971a2d8c6fdcf1187795f1a.pdf.

¹¹¹ Jovan Đurašković, Milena Konatar, and Milivoje Radović, “Renewable Energy in the Western Balkans: Policies, Developments and Perspectives,” *Energy Reports* 7, Supplement 5 (2021): 481-490, <https://doi.org/10.1016/j.egyr.2021.07.104>.

IAD Domain	WB Countries	Capability-Building Dimension
	Methodologies for cyber risk management in the public and private sectors are embryonic ¹¹² Decision-making rests with state-level institutions and high-level leadership	
Action Arena	Limited existence and integration of cyber units within government entities The Data Protection Academy for the Western Balkans and Eastern Partnership Region Public-private engagement Industry forums within regional frameworks	Cyber Capability – Cyber Governance
Patterns of Interaction	NATO structures EU structures OSCE Berlin Process and transfer of best practices in cyber-energy from France, Italy, Germany, and the UK Bilateral agreements Regional initiatives Informal and formal cyber coalitions Public-private platforms in France, the UK, Italy, and Germany ¹¹³	Institutions – Cyber Capabilities
Outcomes	Enhanced control over essential energy infrastructures Increased cyber resources and stronger expertise Governments establish a common language for cyber protection Increased clusters of regional expertise in cyber governance	

Source: Based on Polski and Ostrom, 1999, and Bass, Nicholson, and Subrahmanian, 2013.

¹¹² Barbero and Berglund, “Cybersecurity Capacity Building and Donor Coordination in the Western Balkans.”

¹¹³ ENISA, “Public Private Partnerships (PPP): Cooperative Models.”

Conclusions

This is an introductory exploration of the potential of the Western Balkans Cyber Capacity Center (WB3C), established in 2024 in Montenegro, to serve as a regional cyber-governance mechanism for the renewables sector. It makes conceptual, empirical, and methodological contributions. *Conceptually*, it advances the notion of regional cyber governance through a regional organization, the WB3C. The Center suggests a governance model that is the result of the fusion of bottom-up pressures and top-down responses to build resilience through shared knowledge. *Empirically*, the work pioneers an analysis of the Western Balkans' journey into EU structures via the energy-cyber nexus, with institutionalized cooperation coordinated by the WB3C. As to the *methodological framework*, the article adopts an innovative approach to assessing the WB3C's capability for regional cyber governance, considering its wide range of activities and the countries' ambition to enter the EU Digital Market.¹¹⁴

Regional cyber governance for energy systems is a consequence of both cyber threats affecting the industry at national, regional, and global levels, and the countries' ambitions to integrate into the EU renewable energy framework. The Western Balkans' regional cyber governance appears to endorse norm subsidiarity and actorhood through project learning and organizational integration, conditioned by the European Union, NATO, the UN, the OSCE, and the Berlin Process partners. In other words, the required specialization in cybersecurity for the global energy transition underscores the need for regional governance, especially in light of initiatives involving transregional participation.

In January 2025, Albania, Italy, and the United Arab Emirates announced plans for cross-border green energy cooperation.¹¹⁵ While Italy and the UAE are ranked as cybersecurity role models according to the 2024 Global Cybersecurity Index,¹¹⁶ Albania is a regional leader in renewables.¹¹⁷ This alliance reflects the fact that the energy transition and its ambitious policy implications for the region's economies require a robust collective cybersecurity strategy to attract more investment within and beyond the EU. Implementing this policy demands regional governance capable of addressing challenges through mitigation and defense strategies.

To formulate these strategies, countries need to synchronize their cybersecurity approaches with one another and with states that share similar values.

¹¹⁴ Regional Cooperation Council, "High-level Cybersecurity Conference: Conference Summary Report," WB Conference "CyberPulse 2025: Tracking Progress, Building Resilience, Driving Change," Podgorica, July 2, 2025, www.rcc.int/docs/751/high-level-cybersecurity-conference-conference-summary-report.

¹¹⁵ Emiliano Bellini, "UAE, Italy, Albania Announce Cross-border Green Energy Cooperation Plans," *pv magazine*, January 16, 2025, www.pv-magazine.com/2025/01/16/uae-italy-albania-announce-cross-border-green-energy-cooperation-plans/.

¹¹⁶ ITU, *Global Cybersecurity Index 2024*.

¹¹⁷ Frey, "The Energy Transition in the Western Balkans."

This requires setting common standards, exchanging effective practices, and organizing joint actions against cyber threats. Cyberattacks targeting critical energy infrastructure are likely to continue affecting this economic sector predominantly; therefore, the WB3C should serve as a benchmark for demonstrating regional leadership in addressing cybersecurity challenges related to renewable energy.

This work has several limitations, which are related to: (a) the lack of literature in the native languages of the region; (b) the limited information available on the activities of the WB3C; and (c) the absence of primary sources, such as interviews with relevant stakeholders. Nonetheless, the article offers additional opportunities for both qualitative and quantitative work that are worth exploring. Future research could examine the drivers motivating states to adhere to regional cyber governance arrangements, develop joint strategies, and conduct joint operations to protect energy and renewables infrastructure. Furthermore, investigating stakeholders' ability to shape the nature of regional cyber governance is closely related to their capacity to influence the digital domain. In conclusion, future work can make an empirical contribution to understanding energy-cyber developments in the Western Balkans, while also advancing conceptual knowledge of cyber capability development in the countries of the region.

Disclaimer

The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the Partnership for Peace Consortium, its participating institutions, or any governmental or international organizations affiliated with its governance structure.

About the Author

Megghi Pengili, Ph.D., is a Visiting Research Fellow at the University of Leeds. Her research area is defense innovation governance and Mediterranean studies. Megghi is an alumna of the George C. Marshall European Center for Security Studies and has twice been awarded a fellowship at the GCMC. Since 2022, she has served as Assistant Editor at *Civil Wars* journal.
<https://orcid.org/0000-0002-2491-1795>; *E-mail*: m.pengili@leeds.ac.uk

Bibliography

- "Agreement Establishing the Western Balkans Cyber Capacity Centre (WB3C)," signed by France, Slovenia, and Montenegro, Tirana, October 16, 2023, <https://wb3c.org/landing-page/WB3C%20AGREEMENT%20EN.pdf>.
- "Albania – Cybersecurity Policy," Cyber Policy Portal, <https://cyberpolicyportal.org/states/albania>.
- "Balkan Energy Strategies," Balkan Economic Forum, 2023, www.balkaneconomicforum.org/initiatives/events/balkan-economic-conference-2015/balkan-energy-strategies/.
- "Berlin Process Summit 2024, 10th Anniversary, Chair's Conclusions," *BerlinProcess.de*, October 14, 2024 https://www.berlinprocess.de/uploads/documents/chairs-conclusions-2024_1728992421.pdf.
- "Bosnia and Herzegovina – Cybersecurity Policy," Cyber Policy Portal, <https://cyberpolicyportal.org/states/bosnia-and-herzegovina>.
- "Cyber Budgets Increase, Executive Overview Improves, but Challenges Lurk under the Surface," Moody's, Special Report by Moody's Ratings, September 26, 2023, <https://www.moody.com/web/en/us/insights/data-stories/2023-cyber-survey-highlights.html>.
- "Cybersecurity Market (2026–2033)," Grand View Research, June 2025, <https://www.grandviewresearch.com/industry-analysis/cyber-security-market>.
- "CybilProject – WB6-EU Cooperation for Improving Cybersecurity in the Western Balkans," Cybil, 2024–2025, <https://cybilportal.org/projects/wb6-eu-cooperation-for-improving-cybersecurity-in-the-western-balkans/>.
- "First G7 Cyber Group Agrees on Info-sharing to Defend Democracies," *DeCode39 Geopolitical Insights from Italy*, May 17, 2024, <https://decode39.com/9058/first-g7-cyber-group-agrees-on-info-sharing-to-defend-democracies/>.
- "Government Adopted Training Needs Analysis for Civil Servants and State Employees at Central and Local Level," Government of Montenegro, August 25, 2021, <https://www.gov.me/en/article/244593--government-adopted-training-needs-analysis-for-civil-servants-and-state-employees-at-central-and-local-level>.
- "Navigating Cybersecurity Risks in Europe's Wind Energy Sector: The Challenge of Non-EU Infrastructure," Forvis Mazars, November 29, 2024, www.forvismazars.com/uk/en/insights/energy-infrastructure-and-environment-insights/the-challenge-of-non-eu-infrastructure.
- "Project: Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia," *Cybil Portal*, 2023, <https://cybilportal.org/projects/cybersecurity-rapid-response-for-albania-montenegro-and-north-macedonia/>.

- "Project: Enhancing Protection of Public Spaces and Critical Infrastructures in the Western Balkans," *Cybil Portal*, 2023, <https://cybilportal.org/projects/enhancing-protection-of-public-spaces-and-critical-infrastructures-in-the-western-balkans/>.
- "Project: EU External Cyber Capacity Building Training for the Western Balkans, Eastern Partnership and Southern Neighbourhood," *Cybil Portal*, 2022, <https://cybilportal.org/projects/eu-external-cyber-capacity-building-training-for-the-western-balkans-eastern-partnership-and-southern-neighbourhood/>.
- "Top 10 Emerging Technologies 2024," World Economic Forum, <https://intelligencce.weforum.org/collection/59bc981b-9585-4171-9573-4f78e0fbea51>.
- "Western Balkans Projects," *Cybil Portal*, <https://cybilportal.org/?s=western+balkans>.
- "What Is Cyber Risk Management?" *IBM*, 2023, <https://www.ibm.com/think/topics/cyber-risk-management>.
- Armed Conflict Location & Event Data Project, "Conflict Index Results: December 2024," <https://acleddata.com/report/conflict-index-results-december-2024>.
- Barbero, Fabio, and Nils Berglund, "Cybersecurity Capacity Building and Donor Coordination in the Western Balkans," Geneva Centre for Security Sector Governance, May 7, 2021, <https://www.dcaf.ch/cybersecurity-capacity-building-and-donor-coordination-western-balkans>.
- Bass, Julian M., Brian Nicholson, and Eswaran Subrahmanian, "A Framework Using Institutional Analysis and the Capability Approach in ICT4D," *Information Technologies and International Development* 9, no.1 (2013): 19-35, <https://itidjournal.org/index.php/itid/article/view/1028.html>.
- Bechev, Dimitar, "Energy in the Western Balkans," The Balkans in Europe Policy Advisory Group, May 24, 2023, <https://www.biepag.eu/publication/energy-in-the-western-balkans/>.
- Bellini, Emiliano, "UAE, Italy, Albania Announce Cross-border Green Energy Cooperation Plans," *pV magazine*, January 16, 2025, www.pv-magazine.com/2025/01/16/uae-italy-albania-announce-cross-border-green-energy-cooperation-plans/.
- Biresselioglu, Mehmet Efe, "Assessing the Energy Security in the Balkan Region: Existing Challenges," *Valahian Journal of Historical Studies*, no. 18 (2012): 17-42.
- Blueprint Energy Solutions, *Final Report – Study on Cyber Security in the Energy Sector of the Energy Community*, Energy Community, Document No. FINR-CS-EC-211019 (Vienna: Blueprint Energy Solutions GmbH, December 2019), https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf.

- Boromisa, Ana-Maria, "Transition to Clean Energy Must Clear Economic and Geopolitical Hurdles," *per Concordiam* 13, no. 2 (2025): 52-59, <https://perconcordiam.com/energy-challenges-in-the-western-balkans/>.
- Bryza, Matthew, "Western Balkans Must Pursue More Competitive Energy Sectors," Issue Brief, Atlantic Council, February 26, 2024, www.atlanticcouncil.org/in-depth-research-reports/issue-brief/western-balkans-must-pursue-more-competitive-energy-sectors/.
- Busch, Nathan E., and Austen D. Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," *Homeland Security Affairs* 8, Article 18 (2012), <https://www.hsaj.org/articles/233>.
- Calandro, Enrico, and Nils Berglund, "Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case," University of Cape Town, Graduate School of Business, 2019, https://researchictafrica.net/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf.
- Capoccia, Giovanni, and R. Daniel Kelemen, "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism," *World Politics* 59, no. 3 (2007): 341-369, <https://doi.org/10.1017/S0043887100020852>.
- Carr, Madeline, "Public-Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016): 43-62, <https://doi.org/10.1111/1468-2346.12504>.
- Castello, Pablo Ruiz, Hrvoje Medarac, Julian Somers, and Mandras Giovanni, "Recent Trends in Coal and Peat Regions in the Western Balkans and Ukraine," EUR 30837 EN (Luxembourg: Publications Office of the European Union, 2021), <https://doi.org/10.2760/81752>.
- Čermák, Petr, "New Gas Supplies for the Western Balkans Facilitates a Geopolitical Game Rather Than the Green Energy Transition," *Visegrad Insight*, February 14, 2024, <https://visegradinsight.eu/new-gas-supplies-for-the-western-balkans-facilitates-a-geopolitical-game-rather-than-the-green-energy-transition/>.
- Conway, Maura, and Sheelagh Brady, "A New Virtual Battlefield – How to Prevent Online Radicalisation in the Cyber Security Realm of the Western Balkans," Policy Report (Sarajevo: Regional Cooperation Council, 2018).
- Đurašković, Jovan, Milena Konatar, and Milivoje Radović, "Renewable Energy in the Western Balkans: Policies, Developments and Perspectives," *Energy Reports* 7, Supplement 5 (2021): 481-490, <https://doi.org/10.1016/j.egyr.2021.07.104>.
- ENISA, "2024 Report on the State of the Cybersecurity in the Union," December 3, 2024, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>.

- Esquith, Stephen L., and Fred Gifford, eds., *Capabilities, Power, and Institutions: Toward a More Critical Development Ethics* (Pennsylvania: The Pennsylvania State University Press, 2010).
- European Commission, "Key Findings on the 2020 Report on Bosnia and Herzegovina," Press Corner, October 6, 2020, https://ec.europa.eu/commission/presscorner/detail/en/country_20_1793.
- European Commission, "NIS2 Directive: Securing Network and Information Systems," Directive 2022/2555, European Commission – Shaping Europe's Digital Future, 2022, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
- European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Bosnia and Herzegovina Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/bosnia-and-herzegovina-report-2020_en.
- European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Kosovo Report 2024," https://enlargement.ec.europa.eu/kosovo-report-2024_en.
- European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Montenegro Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/montenegro-report-2020_en.
- European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "North Macedonia Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/north-macedonia-report-2020_en.
- European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, "Serbia Report 2020," October 6, 2020, https://enlargement.ec.europa.eu/serbia-report-2020_en.
- European Parliament and the Council, "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)," *Official Journal of the European Union*, December 27, 2022, <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.
- European Union Agency for Network and Information Security (ENISA), "Public Private Partnerships (PPP): Cooperative Models," November 2017, www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-3%203%20Public%20Private%20Partnerships%20%28PPP%29%20Cooperative%20models.pdf.
- Eurostat, "Statistics Explained: Renewable Energy Statistics," December 2024, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.

- Freeman, Sarah G., et al., "Attack Surface of Wind Energy Technologies in the United States," Idaho National Laboratory, January 2024, <https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf>.
- Frey, Barbara, "The Energy Transition in the Western Balkans: The Status Quo, Major Challenges and How to Overcome Them," *Policy Notes and Reports* 76, Vienna Institute for International Economic Studies, May 2024, <https://wiiw.ac.at/the-energy-transition-in-the-western-balkans-the-status-quo-major-challenges-and-how-to-overcome-them-dlp-6896.pdf>.
- Geneva Centre for Security Sector Governance, "National Cybersecurity Strategies in Western Balkan Economies" (Geneva: DCAF, 2021), www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf.
- International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment* (London: IISS, 2021), 62, <https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power>.
- ITU, *Global Cybersecurity Index 2024* (Geneva: International Telecommunication Union, 2024), <https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024/en>.
- Jasper, Scott, "Cyberspace," in *Handbook of Governance and Security*, ed. James Sperling (Cheltenham: Edward Elgar Publishing, 2014), 343-360.
- Kefalas, Panos, "The Future of Energy in the Western Balkans: A Renewables Revolution," Aurora Energy Research, October 7, 2024, <https://auroraer.com/in-sight/the-future-of-energy-in-the-western-balkans-a-renewables-revolution/>.
- Kosovo Ministry of Internal Affairs, "National Cyber Security Strategy 2023–2027," September 2023, <https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2692/Strategjia%20p%C3%ABr%20Siguri%20Kibernetike%20-%20ENG..pdf>.
- LaBelle, Michael Carnegie, "Breaking the Era of Energy Interdependence in Europe: A Multidimensional Reframing of Energy Security, Sovereignty, and Solidarity," *Energy Strategy Reviews*, no. 52 (2024): 101314, <https://doi.org/10.1016/j.esr.2024.101314>.
- Lauk, Mihkel, and Juhani Lemmik, "Western Balkans Regional Study on Digitalisation in Government" (Podgorica, Montenegro: Regional School of Public Administration, 2023), www.respaweb.eu/download/doc/Western+Balkan+Regional+Study+on+Digitalization+in+Government.pdf/0aa384ee7971a2d8c6fdcf1187795f1a.pdf.
- Lindstrom, Nicole, "Power Trips: Europeanization, Market-governance, and Energy Policy in the Western Balkans," *Policy and Society* 30, no. 3 (2011): 197-207, <https://doi.org/10.1016/j.polsoc.2011.07.004>.

- Luijff, Eric, Kim Besseling, and Patrick de Graaf, "Nineteen National Cyber Security Strategies," *International Journal of Critical Infrastructures* 9, no. 1-2 (2013): 3-31, <https://doi.org/10.1504/IJCIS.2013.051608>.
- Manley, Max, "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership," *Journal of Strategic Security* 8, no. 3 Suppl. (2015): 85-98, <http://dx.doi.org/10.5038/1944-0472.8.3S.1478>.
- Manolkidis, Sotirios, "Geopolitical Challenges and Cooperation in the European Energy Sector: The Case of SE Europe and the Western Balkans Six Initiative," in *Aspects of the Energy Union: Application and Effects of European Energy Policies*, 101-114, https://doi.org/10.1007/978-3-030-55981-6_5.
- Maravić, Dražen, "Cybersecurity Policy Development and Capacity Building – Increasing Regional Cooperation in the Western Balkans" (Geneva: Geneva Centre for Security Sector Governance, 2021), www.dcaf.ch/sites/default/files/publications/documents/CybersecurityPolicyDevelopment_CapacityBuilding_in_WB_mar2021.pdf.
- Martin, Marilen, "More Than Just Money? EU Investments for Green Western Balkans," *OBC Transeuropa*, August 16, 2023, www.balcanicaucaso.org/eng/Areas/Balkans/More-than-just-money-EU-investments-for-green-Western-Balkans-226134.
- Mathioulakis, Michalis, "Strategic Elements of the Energy Union and the Role of Regulation in Energy Security," in *Aspects of the Energy Union: Application and Effects of European Energy Policies in SE Europe and Eastern Mediterranean*, ed. Michalis Mathioulakis (London: Springer, 2021), 73-101, https://doi.org/10.1007/978-3-030-55981-6_4.
- Mihalčatinová, Chiara, "Is Albania a New Regional Champion in the Energy Transition?" *Strategic Analysis*, 2024, <https://www.strategicanalysis.sk/is-albania-a-new-regional-champion-in-the-energy-transition/>.
- Mitrescu, Sergiu, "Energy Diplomacy in the Western Balkans," *Foreign Policy Review* 16, no. 1 (2023): 78-90, <http://doi.org/10.47706/KKIFPR.2023.1.78-90>.
- Morina, Engjellushe, "Power of Need: Energy Security in the Western Balkans," European Council on Foreign Relations, August 2, 2022, <https://ecfr.eu/article/power-of-need-energy-security-in-the-western-balkans/>.
- Nakamura, Hidetoshi, "Regional Security Communities," in *Globalisation, Multilateralism, Europe: Towards a Better Global Governance?* ed. Mario Telò (London: Routledge, 2014), 333-345.
- National Cybersecurity Agency of Italy, "National Cybersecurity Strategy 2022–2026," 2022, www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6. – in Italian

- Organization for Security and Co-operation in Europe, "10 Years of OSCE Cyber/ICT Security Confidence-Building Measures," October 2023, https://www.osce.org/files/f/documents/f/7/555999_1.pdf.
- Pengili, Megghi, and Slawomir Raszewski, "Transnational Cyber Governance for Risk Management in the Gas Sector: Exploring the Potential of G7 Cooperation," *Gases* 4, no. 4 (2024): 327-350, <https://doi.org/10.3390/gases4040019>.
- Polski, Margaret M., and Elinor Ostrom, "An Institutional Framework for Policy Analysis," in *Elinor Ostrom and the Bloomington School of Political Economy: Volume 3, A Framework for Policy Analysis*, ed. Daniel H. Cole and Michael D. McGinnis (Lexington Books, 2017), 13-47, <https://doi.org/10.5040/9781666993875.ch-002>.
- Popovski, Vasko, et al., "Crisis Prevention and Critical Infrastructure in the Western Balkans," IDSCS Policy Brief (Skopje: Institute for Democracy "Societas Civilis," 2023), <https://idscs.org.mk/wp-content/uploads/2023/05/Second-Paper-Online.pdf>.
- Prelec, Tena, Nikolaos Tzifakis, and Dimitar Bechev, "Green Power Politics: External Actors and Energy Transition in the Western Balkans," HAL Open Science, March 2024, <https://hal.science/hal-04526114v1>.
- Rajić, Milena, Emanuele Quaranta, Alban Kuriqi, and Egidijus Kasiulis, "Renewable Energy in the Western Balkans and EU Policy: Pathway to Regional Net-Zero," in *IOP Conf. Series: Earth and Environmental Science* 1442 (2025): 012002, <https://doi.org/10.1088/1755-1315/1442/1/012002>.
- Regional Cooperation Council, "High-level Cybersecurity Conference: Conference Summary Report," WB Conference "CyberPulse 2025: Tracking Progress, Building Resilience, Driving Change," Podgorica, July 2, 2025, <https://www.rcc.int/docs/751/high-level-cybersecurity-conference-conference-summary-report>.
- RFE/RL's Bulgarian Service, "Bulgaria Defends Decision to Impose Tax on Russian Gas Transit as Hungary, Serbia Vow to Respond," *Radio Free Europe/ Radio Liberty*, October 18, 2023, <https://www.rferl.org/a/bulgaria-defends-tax-russian-gas-hungary-serbia/32643100.html>.
- Rosenzweig, Paul, "The International Governance Framework for Cybersecurity," *Canada-United States Law Journal* 37, no. 2 (2012): 405-432, 407, <https://scholarlycommons.law.case.edu/cuslj/vol37/iss2/10>.
- Scazzieri, Luigi, "Reviving European Policy towards the Western Balkans," Policy Brief, Centre for European Reform, December 15, 2021, www.cer.eu/publications/archive/policy-brief/2021/reviving-european-policy-towards-western-balkans.
- Sen, Amartya, *Development as Freedom* (Oxford University Press, 1999).

- Siccardi, Francesco, "Understanding the Energy Drivers of Turkey's Foreign Policy," Carnegie Europe Papers, February 28, 2024, <https://carnegieendowment.org/russia-eurasia/research/2024/02/understanding-the-energy-drivers-of-turkeys-foreign-policy>.
- Smeets, Max, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford: Oxford University Press, 2022).
- Smith, Don C., "Cybersecurity in the Energy Sector: Are We Really Prepared?" *Journal of Energy & Natural Resources Law* 39, no. 3 (2021): 265-270, <https://doi.org/10.1080/02646811.2021.1943935>.
- Spasić, Vladimir, "Alcazar Secures USD 50 Million from US DFC for Investments in Western Balkans, Other Markets," *Balkan Green Energy News*, April 26, 2024, <https://balkangreenenergynews.com/alcazar-secures-usd-50-million-from-u-s-dfc-for-investments-in-western-balkans-other-markets/>.
- Taylor, Adam, "Data Shows Global Conflict Surged in 2024," *The Washington Post*, December 12, 2024, www.washingtonpost.com/world/2024/12/12/conflict-war-2024-israel-gaza-ukraine/.
- United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, June 24, 2013.
- United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, July 22, 2015.
- United Nations Institute for Disarmament Research & the Center for Strategic and International Studies, "The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities," Report of the 2nd International Security Cyber Workshop Series, Geneva, Switzerland, January 24, 2019, <https://undir.org/publication/the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability/>.
- Van Popering-Verkerk, Jitske, et al., "A Framework for Governance Capacity: A Broad Perspective on Steering Efforts in Society," *Administration & Society* 54, no. 9 (2022): 1767-1794, <https://doi.org/10.1177/00953997211069932>.
- Vanhoonacker-Kormoss, Sophie, and Karolina Pomorska, "The Institutional Framework," in *International Relations and the European Union*, ed. Christopher Hill, Michael Smith, and Sophie Vanhoonacker (Oxford University Press, 2011), 76-100.
- Voo, Julia, Irfan Hemani, and Daniel Cassidy, "National Cyber Power Index 2022," Report (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022), <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.

Western Balkans Cyber Capacity Centre (WB3C), “Operational Technology, Cyber Resilient Ecosystems, and Critical Information Infrastructure Protection: Enhancing Cybersecurity Proficiency for Western Balkans Administrations,” September 6, 2024, <https://wb3c.org/event/7/operational-technology-cyber-resilient-ecosystems-and-critical-information-infrastructure-protection-enhancing-cybersecurity-proficiency-for-western-balkans-administrations>.

Western Balkans Info Hub, “Declaration on Energy Security and Green Transition in the Western Balkans,” Berlin Process Summit, Berlin, November 3, 2022, https://www.berlinprocess.de/uploads/documents/energy-declaration-bp-2022_1678468873.pdf.

Western Balkans Investment Framework, “€1 Billion Energy Support Package for the Western Balkans,” December 14, 2022, <https://www.wbif.eu/news-details/1-billion-energy-support-package-western-balkans-approved-5-december>.