DCAF Geneva Centre for Security Sector Governance

Legal and policy frameworks in Western Balkan economies

on PPPs in cybersecurity

Irina Rizmal

Legal and policy frameworks in Western Balkan economies on PPPs in cybersecurity

Albania

Albania adopted a Law on Cybersecurity in 2017.[1] In terms of cooperation, the Law directs the competent authority to coordinate with security institutions, sectorial CERTs and international authorities in the field of cybersecurity. No specific frameworks for public-private cooperation and multi-stakeholder engagement are outlined in the Law.

Bosnia and Herzegovina

At the state level, Bosnia and Herzegovina does not have an official cybersecurity framework. Currently, the only existing framework regulates cybersecurity matters in one of its entities, Republika Srpska. The entity has a Law on Information Security adopted in 2011,[2] which provides regulations on baseline cybersecurity measures and the institutional setup. There are no specific references to public-private cooperation (PPPs).

Kosovo

Kosovo has yet to adopt a specific law regulating the field of cybersecurity. In 2015, Kosovo adopted the National Cybersecurity Strategy, which covers the period 2016-2019 with a complementary action plan. The Strategy was developed in cooperation with the private sector, professional associations and civil society actors. PPPs are identified as one of the Strategy's "strategic principles" and establishing such a partnership is a "strategic objective."

PPP frameworks are primarily addressed in relation to critical information infrastructure protection. The Strategy envisions developing procedures for information exchange between competent authorities and privately-owned critical infrastructures. These include internet service providers, banks, electric power grids and supply, water supply, transport and academia.

The Strategy provides for a National Cybersecurity Council to be established to strengthen cooperation with the private sector. The Council has a mandate to coordinate the development of preventive tools and interdisciplinary cybersecurity approaches. Established in 2016, the Council consists of 16 public institutions and bodies.[3] According to the Strategy, the Council is to invite business representatives as associate members and involve academia to participate in its work at the technical level.

The Strategy envisions a role for non-governmental organizations in monitoring and assessment round tables organized by the National Cybersecurity Strategy Coordinator.[4]

---

1 Law no. 2/2017.

2 Official Gazette of Republika Srpska no. 70/11.

3 The Council is comprised of representatives from the following institutions: Ministry of the Internal Affairs, Kosovo Police, Kosovo Forensics Agency, Ministry of Kosovo Security Forces, Kosovo Intelligence Agency, Agency of Information Society, Kosovo Security Council, Ministry of Justice, Kosovo Prosecutorial Council, Kosovo Judicial Council, Ministry of Finance, Kosovo Customs, Ministry of Education, Science and Technology, Ministry of Foreign Affairs, Regulatory Authority of Electronic and Postal Communications, Central Bank of Kosovo. On specific occasions additional ministries and agencies are to be included.

4 The National Cybersecurity Coordinator is the Minister of Internal Affairs, or his authorized representative, and is responsible and mandated to coordinate, guide, monitor and report on the implementation of policies, activities and actions in connection with the National Cybersecurity Strategy.

On specific activities, the Action Plan refers to the lead role of the National Cybersecurity Council Coordinator. To this end, the National Coordinator is to oversee the designation of focal points for cooperation within the private sector; work on increased cooperation and information exchanges with Internet Service Providers; work jointly with the private sector to develop minimal mandatory criteria for the protection of critical information infrastructure; and host regular meetings with the private sector. None of the action points list steps to be taken and nor how they are to be achieved. There is no provision for a budget, rather these are referred to as administrative and budgeted costs. Performance indicators are purely quantitative, in the form of numbers of meetings or information exchanges.

Other than these specific activities, the Action Plan does not recognize any further possible roles for the private sector. There is a reference to NGOs being included in education and awareness raising on childrens' online safety.

Montenegro

Montenegro adopted its first Law on Information Security in 2010, amending it in 2016. The Law establishes the National Cybersecurity Council, as a multi-sector government body. Despite its primary design including only public institutions, the Council is tasked to work on strengthening cooperation with the private sector. As adopted in 2019, the current composition of the Council includes 12 members from 10 public institutions and bodies.[5]

In the Western Balkans, Montenegro stands out as the only economy to have already adopted its second National Cybersecurity Strategy. The current strategy, covering the period 2018-2021, assigns PPPs as one of its strategic goals; a goal that was also included in its previous strategy.

According to the Strategy, the Cybersecurity Council is to serve as a framework for establishing permanent cooperation between the public and private sectors. Work on PPPs is focused on developing and strengthening cooperation with critical information infrastructure (i.e. internet service providers, the banking sector and electric companies). The National CIRT (CIRT.ME) is tasked with establishing partnerships with other CERTs and formalizing strategic partnerships with these CIIs.

The success in establishing PPPs is to be measured in terms of the number of established partnerships and development of procedures for coordination, communication and cooperation of the public and private sectors on cybersecurity incidents. There is no explanation as to what such institutionalization of PPPs would imply in practice, nor how this is to be measured.

Significantly, the strategy recognizes the specific risks of establishing cooperation among all relevant stakeholders. This relates to the reluctance of the private sector to share information on incidents due to reputational concerns. In response however, the strategy highlights that establishing trust is a process requiring comprehensive dialogue, time and effort, with roles of stakeholders needing to be clearly defined.

The Action Plan prescribes that to achieve the strategic developments, in 2018 several public bodies were to engage in establishing partnerships with the private sector and academia. Specifically, they were to define procedures for information exchanges and joint participa-

[5] Official Gazette of Montenegro no. 16/2019 and 52/2019. The Council comprises of representatives of the Ministry of Public Administration (competent ministry for cybersecurity), the Government of Montenegro, National Security Agency, Ministry of Interior, Ministry of Defence, National Security Authority, Ministry of Justice, Police Directorate, Ministry of Foreign Affairs, and Agency for Electronic Communications and Postal Services.

tion in various events. The same direction was provided in the 2019 Action Plan, with the exception that the Cybersecurity Council was to have the possibility of extending cooperation in the field to non-state actors. Other actors seen as relevant to this action include the Ministry of Public Administration (competent ministry), Ministry of Defence, Ministry of Interior, Ministry of Justice, Ministry of Education, Ministry of Foreign Affairs, National Security Agency, and National Security Authority. No further details on what such cooperation would imply, how specifically it is to be established, or what would be the objectives of such cooperation (other than establishing communication) are provided. Non-state actors are only allocated a passive role in the existing framework outline.

North Macedonia

In 2018, North Macedonia adopted its National Cybersecurity Strategy and Action Plan. The Strategy recognizes the need for establishing an integrated and multidisciplinary approach to ensure closer cooperation and coordination between the defence and security sector, private sector and CSOs.

Within its key principles, the Strategy recognizes the role of multi-stakeholder approaches in building efficient cybersecurity capacities in the field of research and development. A precondition for establishing cooperation and trust at the national level is the need to establish procedures for cooperation between the public, private and civil sectors. Cooperation with CII and important information systems (IIS) is recognized as being of vital importance.

In addition to the public and private sectors, the Strategy lists the private sector (especially CII), academic community and educational institutions as providers of cybersecurity expertise developing a strong body of knowledge in this field; and recognizes citizens and CSOs as its primary users.

The strategic goals recognize multi-stakeholder cooperation as being important to strengthening cyber capacities and a national cybersecurity-oriented culture. The strategy specifies that through the establishment of inter-organizational research teams, multi-stakeholder cooperation can take the form of knowledge exchanges. A special body with operational cybersecurity capacities is to be established, either as a separate entity or a new organizational unit within an existing state body, to operationalize activities envisioned by the Strategy.

Finally, the Strategy recognizes specific risks in establishing cooperation among all relevant stakeholders. These relate to cooperation in the field of cybersecurity being relatively novel and refer to it being a challenge to encourage stakeholders to change their accustomed behaviours. In addition, it is acknowledged that the lack of trust between the public and private sectors may be one of the main obstacles towards the Strategy's effective implementation.

On operationalizing the strategy, the complementary Action Plan recognizes the role of non-state actors in further developing the national cybersecurity framework. CII and IIS are recognized as having a role in identifying critical infrastructure, together with universities, and working on ensuring resilience of those identified sectors through the development of procedures and monitoring. CII and IIS, together with IT operators and companies, have a further role in defining national capacities on cyber defence.

Universities and the academic community are recognized as contributing actors in developing the national cyber incident taxonomy, improving curricula focused on cybersecurity, and awareness raising efforts. Universities are expected to contribute to developing national cybersecurity and digital forensics capacities, research projects, and cybersecurity education for small and medium-sized enterprises.

In general, the private sector is expected to engage in establishing the exchange of information to enable civil-military cooperation and provide training for the public and private sectors. Chambers of Commerce are to contribute to the development of cybersecurity capabilities in CII and IIS operators and in the public sector. With the assistance of donors, the private sector is also to team-up with media actors in establishing a Centre for Internet Safety, a process to be led by civil society organizations.

Overall, the Action Plan recognizes the relevance of the multi-stakeholder approach in several activities which are envisioned in the Strategy. How this multi-stakeholder cooperation is to be operationalized is unclear. The only direction provided is that the Body with Operational Cybersecurity Capacities is the lead actor and that several activities are to be carried out with the inclusion of "all stakeholders."

Serbia

In 2016, Serbia adopted a Law on Information Security and since then two amendments have been passed.[6] The Law tasks the national CERT (SRB CERT) to cooperate with special CERTs (private CERTs registered with the SRB CERT in Serbia) and CERTs of independent operators of ICT systems.

The Law establishes a Government Body for Coordination of Information Security Affairs, as a multi-sector advisory body. The Body for Coordination consists of 14 members and 11 deputies, bringing together 12 public institutions and bodies.[7] According to the Law, the Body for Coordination can establish topic-based expert working groups, which will include other public-bodies, private sector, academic community and civil society.

The National Strategy for the Development of Information Security covering the period 2017-2020[8] recognizes multi-stakeholder cooperation as a precondition for the realisation of its objectives. Establishing public-private cooperation is one of the Strategy's principles and priority fields.

The Strategy recognizes the benefits of public-private cooperation, especially in preventing and responding to cybersecurity risks and incidents. It also refers to the possibility of establishing such cooperation through the framework of the Body for Coordination. Public-private cooperation is regarded as enabling effective communication and optimizing planned future activities. It is acknowledged that these different activities can foster the development of sustainable trust among all actors in cybersecurity.

The Strategy provides for the inclusion of academia in joint projects with the public and private sectors. Specifically, this community can contribute to development of new solutions and highlight international best practices.

Despite the prominent role of PPPs in the strategy, there is limited scope within the Action Plan for operationalizing such partnerships. Public-private cooperation is limited to facilitating training on cybersecurity, and such training is to be led the competent ministry and the agency hosting the national CERT.

---

6 Official Gazette of the Republic of Serbia no. 6/2016, 94/2017 and 77/2019

7 Official Gazette of the Republic of Serbia no. 24/2016, 53/2017, 79.2017 and 93/2018. The Body for Coordination of Information Security Affairs includes representatives of the Ministry of Trade, Tourism and Telecommunications (competent ministry for cybersecurity), Secretariat of the Government, Ministry of Defence, Ministry of Interior, Ministry of Foreign Affairs, Ministry of Justice, Security-Intelligence Agency, Military Security Agency, Military Intelligence Agency, Government Office for IT and eGovernment, Regulatory Agency for Electronic Communications and Postal Services and the Office for the National Security Council and Classified Information Protection.

8 Official Gazette of the Republic of Serbia no. 53/2017.

Public awareness raising campaigns, including those focused on private subjects and independent CERTs, are to be solely led by public bodies. Only in the case of awareness raising and education focused on the safety of children online does the Action Plan recognize a role for other actors such as Serbia's academic network.

Table 1: Overview of mapped formal and informal cybersecurity PPP practice in the Western Balkans

Albania Based on: Law	Declarative measures	Responsible authority to coordinate its activities with sectoral CERTs.
	Actionable measures	
	Coordinating entity	Authority responsible for electronic certification and cybersecurity
	Non-state actors mentioned	Sectoral CERTs
	Sectoral cooperation	Albanian Association of Banks[9]
	Informal frameworks	
Bosnia and Herzegovina	Declarative measures	
	Actionable measures	
	Coordinating entity	
	Non-state actors mentioned	
	Sectoral cooperation	Bank Association of Bosnia and Herzegovina (BABiH)[10] Independent System Operator in Bosnia and Herzegovina (NOSBiH)[11]
	Informal frameworks	OSCE-led multi-stakeholder working group

9 More information available at: https://aab.al/en/.

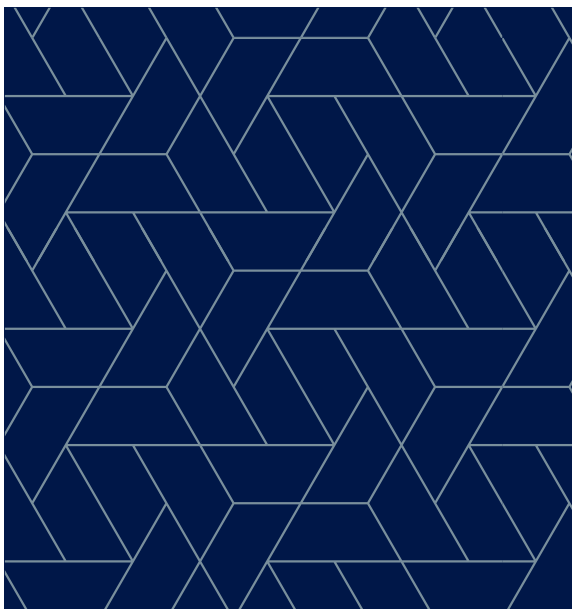
10 More information available at: https://ubbih.ba/en.

11 NOSBiH is a non-profit company in Bosnia and Herzegovina owned by the two entities; the Federation of BiH, and the Republika Srpska. It carries out its activities in the entire territory of BiH, managing the entire BiH transmission network with the aim of ensuring continuous electricity supply. The work of NOSBiH is regulated by the State Electricity Regulatory Commission (SERC). More information available at: https://www.nosbih.ba/en/pocetna.

Kosovo Based on: Strategy & Action Plan	Declarative measures	National Cybersecurity Council to invite business representatives, academia and non-governmental organizations.
	Actionable measures	Development of procedures for information exchange between competent authorities and privately-owned critical infrastructures. Development of minimal mandatory criteria for the protection of critical information infrastructure.
	Coordinating entity	National Cybersecurity Council
	Non-state actors mentioned	Academia; critical infrastructure (esp. ISPs, banks, electric power and supply, water supply, transport); non-governmental organizations; private sector in general
	Sectoral cooperation	
	Informal frameworks	
Montenegro Based on: Law Strategy & Action Plan(s)	Declarative measures	Cybersecurity Council can extend cooperation to non-state actors. National CERT tasked with establishing partnerships with other CERTs and formalizing strategic partnerships with critical information infrastructure.
	Actionable measures	Development of procedures for coordination, communication and cooperation of public and private sector.
	Coordinating entity	Cybersecurity Council
	Non-state actors mentioned	Academia; critical information infrastructures (esp. ISPs, banking sector, electric companies); private sector in general; telecommunication operators
	Sectoral cooperation	
	Informal frameworks	

North Macedonia Based on: Strategy & Action Plan	Declarative measures	Multi-stakeholder cooperation for raising cyber capacities and cybersecurity culture through knowledge exchange and establishment of inter-organizational research teams.
	Actionable measures	Development of procedures for cooperation with non-state actors. Critical information infrastructure/important information systems and universities to help identify critical infrastructure, develop procedures and monitor implementation. Universities and academia to help develop national cyber incident taxonomy, improve curricula and support awareness raising. Support for research capacities and business innovations through the establishment of a scientific research centre in the field of cybersecurity. Private sector, with civil society organizations and the media, to establish Centre for Internet Safety.
	Coordinating entity	Body with Operational Cybersecurity Capacities
	Non-state actors mentioned	Academic community and educational institutions; citizens and civil society organizations; critical information infrastructure/important information systems
	Sectoral cooperation	Macedonian Banking Association[12]
	Informal frameworks	Group of various stakeholders gathered by the national CIRT at technical level

NB: instances of sectoral cooperation are mapped based on DCAF's interaction with various sectoral associations as well as additional information obtained on sectoral engagement in the field of cybersecurity across Western Balkan economies.



12 More information available at: https://mba.mk/w/mk/.

Serbia Based on: Law Strategy & Action Plan	Declarative measures	National CERT to cooperate with special CERTs and CERTs of independent operators of ICT systems, as well as public and private subjects. The Body for Coordination of Information Security Affairs can establish topic-based expert working groups to include representatives of the private sector, the academic community and civil society. Public-private cooperation for industrial research and innovation; academia to contribute to development of new solutions through joint projects with public and private sector.
	Actionable measures	National CERT hosts a database of special CERTs. Public bodies, public and private sector to organize public campaigns on the most common forms of cybercrime, such as unauthorized access, security compromises, internet fraud; as well as campaigns and workshops focused on children's inline safety.
	Coordinating entity	Government Body for Coordination of Information Security Affairs
	Non-state actors mentioned	Academia and specifically the academic CERT (AMRES); CERTs of independent operators of ICT systems and special CERTs; citizens organized in civil society; private sector in general
	Sectoral cooperation	Association of Serbian Banks[13]
	Informal frameworks	Standing multi-stakeholder public-private cooperation framework initially established by the OSCE Mission to Serbia and DCAF

Common traits in Western Balkan frameworks

Declaratively and on paper, Western Balkan economies recognize the need for adopting comprehensive approaches to national cybersecurity. These are referred to as both multi-stakeholder and PPP frameworks. All existing strategies list some form of cooperation frameworks as a strategic principle or a strategic objective/goal; or both.

In terms of how such frameworks are understood, based on the frequency of references in official legislation and strategic documents analysed, two common patterns are apparent across the Western Balkan frameworks. First, PPPs are regarded as being vital to protecting critical infrastructure and it is acknowledged that the private sector plays a key role in this work. To this end, cooperation is to be established with private sector actors holding CII to establish an understanding of what actually constitutes CII and how to increase its resilience. Second, the need for information exchange among all relevant stakeholders is recognized. As a result, cooperation is either to be established loosely for general coordination purposes or is to take the form of stricter formats with specific procedures to be

13 More information available at: https://www.ubs-asb.com/en.

developed on the exchange of information between state and non-state actors. References to non-state actors in Western Balkan economies' legislative and strategic frameworks are visualized in Figure 1 below.

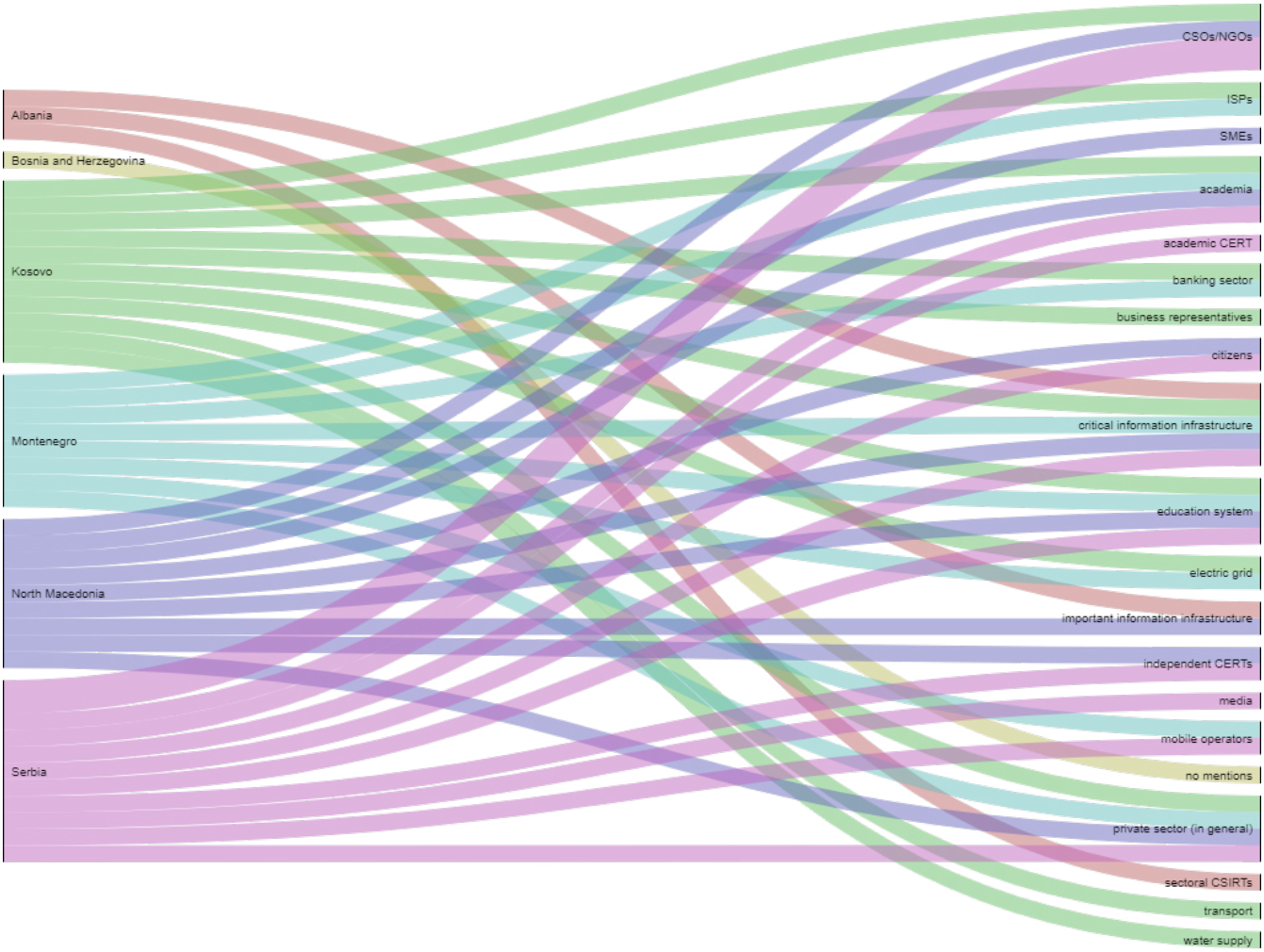


Figure 1: References to non-state actors in Western Balkan economies' legislative and strategic frameworks

Apart from these roles, non-state actors are recognized as potential contributors to only a limited set of activities. These predominantly focus on, for example, the roles of academia in developing new curricula and the private sector in research and development. The potential benefit of public– private cooperative frameworks and what these can deliver, in terms of the efficient and inclusive identification of policy needs and directions, is rarely recognized. Nor is there recognition of the value of involving those who will ultimately be impacted by the laws and policies involved in any way in their formulation. In the Western Balkans, public consultations processes are frequently conducted with limited transparency and in short timeframes. Such an approach does not encourage the engagement of the private sector, CSOs and academia in the formulation of laws and policies. In the often-small administrations of the Western Balkans, this approach does not take advantage of the knowledge and expertise found in the local cybersecurity community.

The specific roles attributed to non-state actors in Western Balkan economies' cybersecurity laws and strategic frameworks are visualized in Figure 2 below.

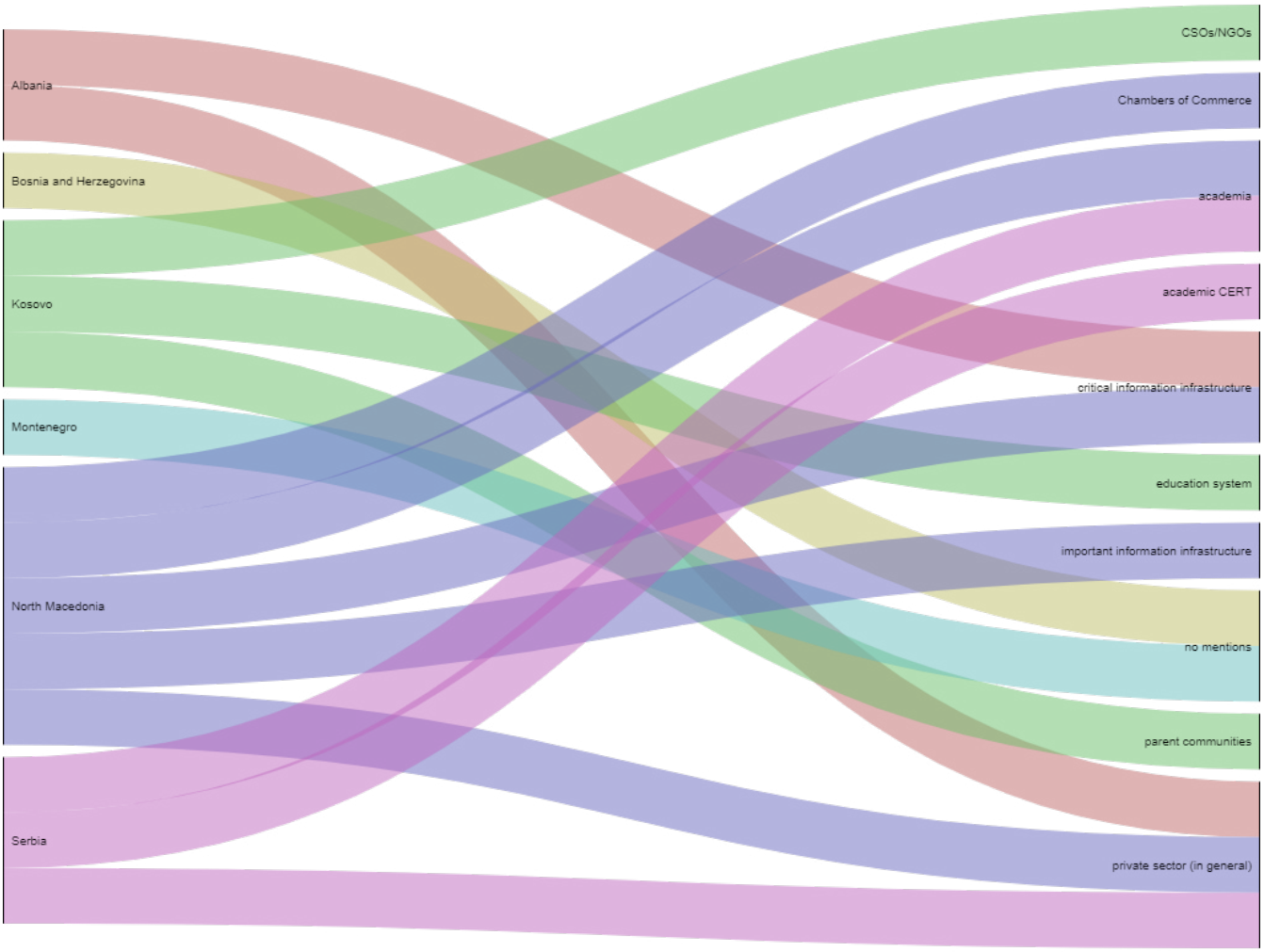


Figure 2: Non-state actors attributed with specific roles in Western Balkan economies' legislative and strategic frameworks[14]

Cooperation with non-state actors is predominantly to be state-led and issue-focused, based on existing legislative and strategic frameworks. It is unclear how this cooperation is to be operationalized. In several Western Balkan economies, the legislative framework envisions establishment of specific bodies or councils aimed at coordination of the relevant public cybersecurity actors. Such bodies are to engage non-state actors. However, this engagement is not envisioned as a permanent framework, but rather as an ad-hoc mechanism.

Overall, despite recognizing the benefits of multi-stakeholder approaches, Western Balkan economies appear to lack an understanding of the benefits of cooperating with all actors and at best are paying lip service to the notion. This is reflected in strategic measures related to multi-stakeholder cooperation that are mainly declarative and the evident lack of resources and actionable measures in the complementary Action Plans. Arguably, it remains unclear how the PPPs referred to in strategic documents are to be established, by whom, and for what purpose.

[14] It is important to note for both Figure 1 and Figure 2 is that the graphs are simplistic visualizations for easier understanding of existing circumstances. For the purpose of simplicity, actors are presented in clusters as they appear in the examined documents, with no further elaboration. For example, some documents refer only to CII, while others list what sectors they refer to as 'critical', or 'ICT systems of special importance'. Similarly, when it comes to non-state CERTs, the term 'independent CERT' is employed, which refers to various references to this concept – private CERTs in North Macedonia and special CERTs in Serbia, for example. A detailed breakdown of mapped actors is provided in Annex I.

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

DCAF's Foundation Council is comprised of representatives of about 60 member states and the Canton of Geneva. Active in over 80 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF - Geneva Centre for Security Sector Governance

Maison de la Paix Chemin Eugène-Rigot 2E

CH-1202 Geneva, Switzerland

Tel: +41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

Twitter @DCAF_Geneva

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva