DCAF Geneva Centre for Security Sector Governance

Cybersecurity in the Western Balkans: a Guide to Public–Private Partnerships

Copyright page

Published in Switzerland by the Geneva Centre for Security Sector Governance (DCAF)

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

First published in March 2021

Cite as: Franziska Klopfer and Irina Rizmal, Cybersecurity in the Western Balkans: A Guide to Public–Private Partnerships (Geneva: DCAF, 2021)

Design by DTP studio
Copy-edited by Tania Inowlocki

About this Guide

This Guide was produced as part of a DCAF project entitled ‘Enhancing Cybersecurity Governance in the Western Balkans’ (2018–21) and funded by the United Kingdom’s Foreign, Commonwealth and Development Office. The views expressed are those of the authors alone.

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 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

Acknowledgements

The authors would like to acknowledge the important contribution made to this publication by several former DCAF colleagues. Adel Abusara and Nicholas Hudson both provided background research and written sections in earlier drafts of the Guide. Hine-Wai Loose edited earlier drafts.

Several other experts made significant contributions during the review of the text. Myriam Dunn Cavelty, ETH Zurich, supplied invaluable comments that helped shape the final version of the Guide. The authors are also grateful for insightful observations from Lea Kaspar, Global Partners Digital, and Ratko Mutavdzic, Microsoft Corporation.

Table of Contents

List of boxes and tables

List of abbreviations

DCAF	Geneva Centre for Security Sector Governance
ENISA	European Union Agency for Cybersecurity
ISAC	Information Sharing and Analysis Center
MKD-CIRT	North Macedonia National Center for Computer Incident Response
PPP	Public–private partnership
OSCE	Organization for Security and Co-operation in Europe

Introduction

In today's 'deeply cybered' world, technological developments are racing ahead of both military doctrine and international law (Demchak, 2012; Shackelford, 2013). As cybersecurity challenges conventional ideas of how security is delivered and governed, governments are struggling to adapt their models of cybersecurity cooperation. In many countries, it is not the state but rather the private sector that provides cyber services or that owns critical infrastructure, such as telecommunication networks and online platforms. Much of the cybersecurity expertise thus lies with non-state actors. In seeking to address cybersecurity challenges and build up resilience, governments are not able to go it alone (Dunn Cavelty, 2007; Reveron, 2012; Tropina and Callanan, 2015).

The legal and strategic frameworks of all Western Balkan economies recognize the need – and the opportunities – for public–private partnerships (PPPs) in cybersecurity. DCAF's analysis of relevant laws and strategies in the region shows that some present the concept of PPPs as an aspirational principle, while others refer to multi-stakeholder cooperation in certain areas of strategic importance. Indeed, certain policies set out specific actions to be taken to establish a cybersecurity PPP.[1] Overall, however, there is a lack of practical guidance on how to secure such cooperation and the region has seen few attempts to set up cybersecurity PPPs. Their presence is far more common in Western Europe and North America.

This Guide is designed to support Western Balkan governments and non-state actors that are planning to establish cybersecurity PPPs as part of their public–private cooperation. Drawing on international best practice, and referencing the region's distinctive cultural, economic, and social context, it highlights options for establishing suitable cooperation frameworks and methods for overcoming obstacles.

Chapter 1 defines the term 'cybersecurity PPP' and sets out the main concepts and principles that underpin the guidance on planning, establishing, and maintaining a cybersecurity PPP. It describes the critical role good governance plays in every stage of cybersecurity cooperation and underscores the benefits of assessing the maturity of a community of cybersecurity actors as part of the PPP planning process.

Chapter 2 provides practical, advice on how to plan, set up, and run a cybersecurity PPP in the specific context of the Western Balkans. It reviews key considerations that can inform various aspects of the process, including the selection and convening of stakeholders, communication among partners, the establishment of PPP objectives and rules, agreement on who leads and administers the PPP, and upskilling of stakeholders who may have limited experience in public–private cooperation.

Chapter 3 presents various types of cybersecurity PPPs and offers concrete examples from the Western Balkans and other parts of the world. It draws out useful lessons, noting what steps stakeholders can take to overcome challenges. The examples reveal the advantages of tailoring the modalities of planning, establishing, and maintaining a cybersecurity PPP to its specific objective.

[1] For details, see DCAF (2021).

Chapter 1 Concepts and principles

Useful general guidance on planning, establishing, and maintaining cybersecurity PPPs is readily available.[2] Much of it assumes that a state's cybersecurity actors already know one another and are ready to cooperate. In some countries, however, interaction between these actors may be in its early stages, and trust among them may still need to be established, particularly if cooperation between private and public entities is a relatively new concept.

This Guide differs from general manuals on cybersecurity PPPs in that it offers advice tailored specifically to policymakers and non-state actors from the Western Balkans. It takes into consideration that the countries in this region are undergoing democratic transitions, that their economies are developing, and that their communities of cybersecurity actors are only just emerging. Since these countries do not have a tradition of public–private cooperation, instituting a partnership can be particularly challenging.

The shared circumstances of Western Balkan economies help to determine how PPPs in the region can best be established and managed, and how their goals should be defined. In view of this regional context, Section 1.1 provides a broad definition of the term 'cybersecurity PPP', so as to include a variety of cooperation initiatives. It also distinguishes PPPs from public procurement and privatization, whose roles are often confused in states where the public sector usually engages with private actors only for commercial transactions.

In countries that are undergoing democratic transitions, the principles of good governance are key to successful public sector reform and security sector reform. Section 1.2 focuses on how these principles can be applied to cybersecurity PPPs. The good governance theme undergirds much of the advice in this Guide, including the detailed guidance in Chapter 2.

As discussed in Section 1.3, a country's community of cybersecurity actors may be categorized according to its stage of development: emerging, advanced, or mature. Recommendations on cybersecurity PPPs can usefully be brought in line with this status. The best practice guidance in Chapter 2 also considers a cybersecurity community's stage of development.

[2] In particular, see ENISA (2011).

1.1 Defining cybersecurity PPPs

Definitions of the term 'public–private partnership' abound and agreement on the meaning and goals of a 'cybersecurity PPP' remains elusive.[3] In Europe, one commonly used definition is that of the European Union Agency for Cybersecurity (ENISA), which defines a PPP as 'an organised relationship between public and private organisations, which establishes common scope and objectives, and uses defined roles and work methodology to achieve shared goals' (ENISA, 2011, p. 12). Building on the ENISA definition, this Guide defines cybersecurity PPPs as:

> **All organized relationships (formal and informal) between public and private actors that cooperate to achieve a goal related to the improvement of cybersecurity.**

This definition may be unpacked to shed light on its component parts:

- Organized relationships, in contrast to one-off meetings or discussions, involve the pursuit of agreed common goals by stakeholders that have set up and cooperate within a dedicated framework, be it formal or informal (see the next point).
- By including formal and informal cooperation, this Guide promotes an inclusive approach to cybersecurity PPPs. Formal PPPs may be registered entities to which all partners have (legally) committed themselves; such advanced partnerships may be difficult to achieve in many Western Balkan economies, which are not able to rely on traditions of PPPs the way developed states can. Informal PPPs have an agreed objective and a well-defined group of partners, but the partnership itself is not registered and membership commitments are not (legally) binding.
- In the phrase public and private actors, 'public' relates to state actors, while 'private' denotes the private sector and all other non-state actors that have a stake in cybersecurity, including private businesses, civil society, the technical community, and academia. Inclusive PPPs stand to benefit from the knowledge, research, and experience of civil society organizations and academia, as these groups can provide invaluable insight into issues such as freedom of information and data privacy matters.

Also of note is what the definition does not specify:

- The definition does not restrict PPPs to any particular institutional framework, thereby indicating that a partnership is free to select the most appropriate model of cooperation.
- This Guide does not define a PPP as a commercial relationship between the public and private sector,[4] but rather as a framework within which all partners cooperate to achieve a common goal for the common good. In that sense, a PPP is distinct from commercial activities such as public procurement and privatization, both of which can potentially deliver cybersecurity, typically once the state outsources its responsibility to the private sector. As noted above, this distinction is useful to make in the context of transitioning economies, in which PPPs are often mistaken for public procurement processes. What sets a PPP apart from commercial frameworks is that all of its participants have a stake in attaining the same cybersecurity outcome. Such unity of purpose

---

3 See, for example, the PPP definitions in different language editions of Wikipedia.

4 Other definitions describe PPPs as essentially commercial in nature. The World Bank, for example, defines a PPP as 'a long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance' (World Bank, 2018).

requires clearly defined objectives, especially in terms of what activities a partnership aims and declines to undertake.

In practice, a cybersecurity PPP that corresponds to the above definition is a partnership that brings together all the actors that can help to solve a country's cybersecurity governance challenge for the common good. As part of this whole-of-nation approach to cybersecurity, all stakeholders have a duty to collaborate and contribute to the extent that they are needed.

1.2 The principles of good governance

The principles of good governance include accountability, effectiveness, efficiency, participation and inclusion, responsiveness, and transparency (DCAF, 2015). These principles are critical to successful public sector reform and security sector reform in democracies. Accordingly, this Guide supports their application to cybersecurity PPPs, as described in Table 1. The principles are also a recurring theme in the guidance presented in Chapter 2.

Table 1 Applying principles of good governance to cybersecurity PPPs

Principle	Application to cybersecurity PPPs
Accountability	By acting responsibly, being accountable for their behaviour, demonstrating that they work to advance the objective of the PPP, and preventing the misuse of the PPP for other purposes, its members can help to safeguard the partnership's legitimacy, particularly if it is publicly funded.
Effectiveness	PPP members can maximize the impact of their work by selecting the most suitable organizational structure, means of communication, and approach to cooperation.
Efficiency	An efficient PPP is one that seeks to limit the waste of resources, minimize diversions of funds from other essential services, and avoid unnecessary debt, while simultaneously securing the maximum cybersecurity gains.
Participation and inclusion	By involving a variety of stakeholders that can contribute to achieving its objectives – including academics and civil society organizations – a PPP can help to promote democratic values and build resilience.
Responsiveness	Flexible structures can allow PPPs to respond swiftly to new cybersecurity threats while remaining receptive to evolving public, institutional, and social needs and demands.
Transparency	Transparency is essential to ensure accountability. Given the relative novelty of cybersecurity PPPs in the Western Balkans, their establishment might raise questions relating to the selection of members or a state's rationale for cooperating with particular businesses. By being transparent about such processes, a PPP can help to secure a good reputation and acceptance.

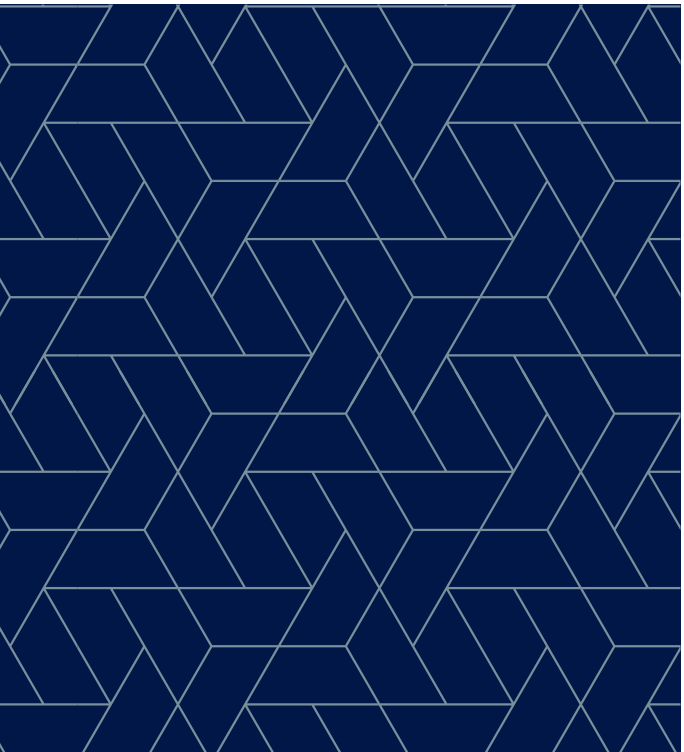
1.3 Assessing the maturity of cybersecurity communities

A strong cybersecurity community – one in which actors from different stakeholder groups work together well and with ease – is among the keys to a successful cybersecurity PPP. A strong cybersecurity community is not created overnight, however; it may take many years to develop. In countries where such communities are nascent or evolving, an understanding of their stage of development helps to inform and adjust the processes of planning, establishing, and maintaining a cybersecurity PPP.

As detailed in Table 2, a country's cybersecurity community may be described as emerging, advanced, or mature. Chapter 2 provides specific guidance on planning, setting up, and running a cybersecurity PPP based on the maturity of a country's cybersecurity community.

Table 2 Stages of cybersecurity communities

Stage	Characteristics of cybersecurity communities
Emerging	Cybersecurity actors have limited experience in communicating or cooperating with each other. Key development strategies at this stage include building trust among stakeholders and expanding the network of cooperating partners.
Advanced	Cybersecurity actors are aware of each other and have a general understanding of the advantages of cooperation. They recognize one or several actors as conveners of a cybersecurity PPP. For communities at this stage, two critical components of establishing a successful PPP are an appropriate process for selecting members and well-defined terms and conditions of cooperation.
Mature	A cybersecurity PPP or other cooperation structure has already been established. Cybersecurity actors are committed to this network and understand their roles and responsibilities. To consolidate their PPP and ensure that the partnership can work effectively and sustainably, the members may introduce work procedures and adopt planning and management tools.



Chapter 2 Planning, setting up, and running a cybersecurity PPP

This chapter presents a number of good practices that should be followed by those planning, setting up, and running a cybersecurity PPP. The advice is addressed primarily at state bodies, given that in laws and strategies in the Western Balkan economies, usually a state body is identified as taking the lead in establishing and running a cybersecurity PPP. However, it is equally relevant for non-state actors, as they might also find themselves in position of initiating or leading a cybersecurity PPP or in supporting the state actor in such endevours.

Each subsection begins with the key takeaways of its contents. The key takeaways also refer to the maturity of cybersecurity communities wherever relevant, to underline the fact that some of the steps might be more or less important, depending on how mature the cybersecurity community is. The subsections then list a number of important steps related to the topic of the subsection that government actors (and their partners in a cybersecurity PPP) should take in planning, setting up and running a cybersecurity PPP. Neither the subsections nor the steps of a subsection appear in any specific chronological order.

2.1 Planning a cybersecurity PPP

Key takeaways

- Commitment of all actors to multi-stakeholder cooperation is a precondition for the success of a cybersecurity PPP. This is especially true in the case of an emerging cybersecurity community, which requires particular efforts to build cooperation and trust among stakeholders.
- A stakeholder map can support the PPP planning process, including tasks such as identifying, selecting, and assigning roles to various cybersecurity actors. Even for PPPs whose membership is already established, a stakeholder map can provide useful information on the wider cybersecurity community.
- Some relevant stakeholders may not be equipped to make meaningful contributions to a cybersecurity PPP, especially in emerging cybersecurity communities. Capacity building can empower stakeholders by allowing them to acquire the skills and experience they need to become active participants in a PPP.
- By focusing on finding common ground in initial meetings, PPP conveners can foster trust and confidence among stakeholders. This step may be especially valuable if the objective of the PPP remains to be defined or if stakeholders are not sufficiently familiar with one another, as in an emerging cybersecurity community.
- Following initial discussions and the start of trust building among stakeholders – yet before the establishment of a PPP – organizers are well placed to define the objective of the PPP and to inform prospective PPP members of the benefits of participation.

Commit to multi-stakeholder cooperation in cybersecurity

Planning, setting up, and running a cybersecurity PPP can be a lengthy, costly process. It requires adequate financial and human resources as well as political support. In this context, a the commitment of all actors to multi-stakeholder cooperation in cybersecurity matters is critical.

Throughout the Western Balkans, laws and policies explicitly refer to the importance of engaging with non-state actors in cybersecurity-related activities; however, few provide concrete instructions on setting up corresponding bodies. The dearth of guidance may be limiting the establishment cybersecurity PPPs.

Once a government tasks a public sector actor with setting up a cybersecurity PPP, it can signal its support by empowering that actor to engage in multi-stakeholder cooperation, notably by providing the necessary resources. A PPP is more likely to be inclusive if the government allows civil servants to network outside government circles, both formally and informally. If a government assigns cybersecurity responsibilities to a powerful and well-resourced ministry, funding for a PPP may be more easily available and ministry representatives may find it easier to gather and lead multi-stakeholder initiatives.

If political commitment does not exist yet, then it needs to be created. Awareness raising among top decision-makers can help to call attention to cybersecurity concerns and the benefits of multi-stakeholder cooperation in that area.

Create a stakeholder map

Stakeholder mapping can facilitate the planning of a PPP. The exercise can be used to reveal which cybersecurity stakeholders are active in a country and what roles they play in the sector. This information can help PPP planners determine whether and how stakeholders might contribute to a partnership, either as PPP members or as external contacts.

Stakeholder mapping is particularly relevant in countries where cybersecurity actors have limited interaction, including in Western Balkan economies. In these settings, cybersecurity actors in the public sector may not be aware of their non-state counterparts. In some cases, stakeholders within the same sector may not even know one another.

A mapping exercise is useful in identifying the widest set of relevant stakeholders. Individuals involved in setting up a PPP may then contact them to ascertain their key interests and whether they should become a member of the partnership. As part of this process, PPP planners may wish to organize conferences or other events to allow stakeholders to meet and explore how they relate to other actors in the cybersecurity community.

Empower stakeholders to make a meaningful contribution

Some stakeholder groups in the Western Balkans are only beginning to show an interest and demonstrating expertise in cybersecurity. Generally, academic programmes in the region are limited to contributing technical capacity building to the development of a talent pool of IT specialists, but not cybersecurity experts. Civil society organizations tend to be focused on traditional security matters; few are specialized in cybersecurity.

While these stakeholders are relevant actors in the cybersecurity community, they may not be able to contribute to a cybersecurity PPP or related policy discussions. They may lack knowledge about the PPP or have little experience working with other stakeholders. Unless they receive targeted assistance, these actors risk staying on the margins of a PPP or finding themselves excluded from the process altogether.

Sustained, long-term support can help these actors develop the expertise they need to make meaningful contributions to national cybersecurity discussions. The public sector, private companies, and international capacity building organizations could provide relevant training, for example in cybersecurity policy or multi-stakeholder processes.

Focus on finding common ground in initial discussions

By focusing on finding common ground, initial PPP meetings can help to build confidence among stakeholders. In discussing legislative frameworks, strategies, or operational solutions, for example, actors are able to get to know one another, build trust, and foster cooperation through dialogue. During these meetings, they can be encouraged to share their experiences in dealing with certain cybersecurity challenges and to identify perceived gaps in the policy response.

In Western Balkan economies, some state and non-state actors may not have any experience working together. As a result, they may initially be reluctant to speak openly during multi-stakeholder discussions. One way to make everybody around the table feel comfortable is to establish clear goals and rules at the outset, so that all actors know exactly what to expect from one another. If the rules instruct actors to keep any and all information shared within the group confidential, for instance, participation is likely to grow and the work environment may become more relaxed.

PPP organizers can identify common interests among stakeholders by developing an understanding of their individual motivations. These commonalities can serve as starting points for discussions, workshops, and other forms of dialogue. Organizers can elect to engage experienced facilitators to moderate such meetings, so as to ensure that stakeholders offer constructive input and concentrate on what unites participants rather than what divides them. To gain a better understanding of how each actor could contribute to solving policy challenges, the organizers can invite stakeholders to speak about their individual capacities and capabilities.

Clearly define the PPP's objective(s)

A cybersecurity PPP requires a well-defined objective or objectives that can serve as the basis for rules and a framework, which, in turn, will allow the partners to reach the objective. A gap analysis can identify areas for improvement, allowing organizers to define the broad terms of a PPP's services and activities.

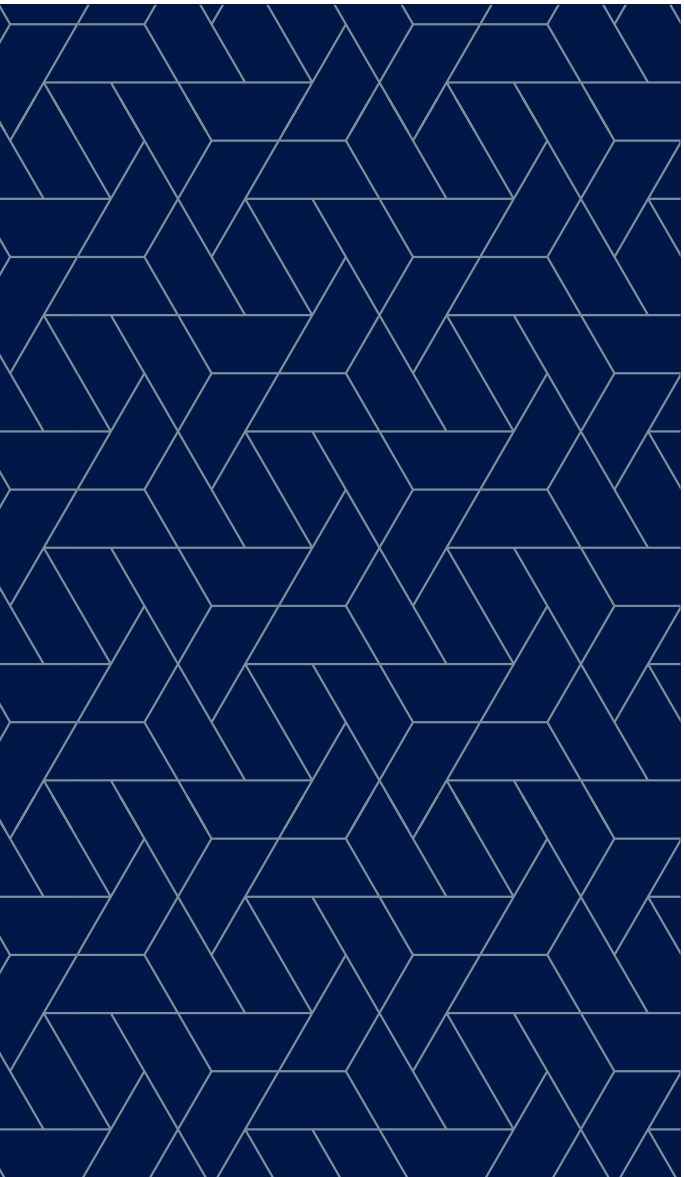
In the case of an established cybersecurity PPP, a broad objective may already be stipulated in a law or decree that established the partnership. Such a PPP may benefit from additional clarity in its mandate, based on what it can realistically be expected to achieve.

Inform prospective PPP members of the benefits of participation

Multi-stakeholder cooperation is most likely to achieve its goals and operate sustainably when all participants understand their roles and the benefits of fulfilling their responsibilities. PPP organizers can ensure that is the case by specifying to prospective members precisely what they would need to invest in the partnership and what they would gain from it. Table 3 lists some of the benefits that state and non-state actors may be able to expect from membership in a cybersecurity PPP.

Table 3 Selected benefits of membership in a cybersecurity PPP, per stakeholder sector

Sector	Benefits
State sector (government, public institutions)	Access to the advanced resources of the non-state sector, especially in terms of expertise and technical capabilities. A better understanding of non-state cybersecurity actors. Exposure to new policy ideas through policy discussions with a wider range of stakeholders. Collaboration with cybersecurity stakeholders that will be involved in the implementation of policies. Overview of cybersecurity actors and capabilities in the country.
Non-state sector (businesses, civil society, technical community, academia)	Pooling and sharing of public and private resources. Participation in cybersecurity policy processes. Opportunity to demonstrate social responsibility. Option to share resources and improve cybersecurity capabilities.



2.2 Setting up a cybersecurity PPP

Key takeaways

- After the objective of the PPP is clarified, roles and responsibilities of all members need to be clearly defined.
- In selecting the appropriate level of formality for the PPP's structure, it is useful to consider its objective, its maturity, and the degree of trust and cooperation among its partners.
- If the PPP's leadership is not yet in place, then its hierarchical structure needs to be established.
- A PPP can only be viable if a financial plan is established at the planning stage and it is clear that the PPP can be financed in the long term.

Define the roles and responsibilities of all members

Once a cybersecurity PPP's objective is defined, the next steps are identifying tasks that need to be carried out to meet the objective and assigning corresponding roles and responsibilities to different partners. Regardless of whether the PPP is formal or informal, such as a discussion forum, assigning roles and responsibilities helps partners to work towards the same goal and prevents misunderstandings that could lead to conflict, oversights, or the duplication of efforts.

In some cases, the roles and responsibilities of different partners are already defined, typically in the law or strategy that established the PPP. If they are unclear or vague, they can be amended to be more precise or detailed.

Assigning roles and responsibilities tends to be a straightforward process, as partners in a cybersecurity PPP generally have specific expertise or play a particular role in the national cybersecurity framework, such that it may be obvious which tasks they are best suited to undertake.

If the objective of the PPP is to deliver a part of national cybersecurity, then the definition of roles and responsibilities must be in line with the national constitutional order.

Determine the appropriate level of formality

In highly formal PPPs, actors officially register as members, legally commit to delivering certain services, and agree to abide by established rules. This degree of formality may dissuade some actors from joining a PPP. Moreover, such strict procedures are not necessary for all forms of cooperation; policy discussion forums, for example, can easily operate in an informal manner.

In an informal cooperation structure, members do not have to commit themselves financially or legally. This lack of requirements may be perceived as a key benefit, particularly among public sector representatives, who may need approval from their management to participate in formal PPP activities. In the absence of a lead institution or actor, however, informal initiatives are at risk of remaining at the level of a discussion forum, unable to build momentum towards long-term results.

The following considerations can help organizers select the appropriate degree of formality for a cybersecurity PPP:

- the PPP objective, which can indicate whether a formal arrangement that binds members to specific activities and rules is necessary;
- the maturity of the PPP, which can be nurtured through an informal format, especially in the case of new or growing partnerships;
- the level of trust among PPP stakeholders, which can be fostered through formal arrangements that clarify positions and roles of different partners; and
- the degree of cooperation between state and non-state actors, which can be promoted through light measures, such as non-disclosure agreements and the Traffic Light Protocol.[5]

Define the hierarchical structure

A cybersecurity PPP can be organised in various ways. It can be run by one main actor, who decides on the partnership's objectives, rules, and membership and who also convenes and manages the PPP. Another option is for all partners to set up the PPP together, non-hierarchically, so that all members have an equal say. The PPP can then be run either by all members or by an administrative body, such as a secretariat.

In countries where mistrust continues to characterize the relationship between the public and private sectors, a state-lead PPP may be the only type of PPP that state representatives would be permitted to join. Indeed, in their laws and strategies, Western Balkan economies tend to reserve a quasi-PPP leadership role for a state body, such as a ministry or national cybersecurity council, which would cooperate and communicate with all cybersecurity stakeholders.

It is also possible for a third party – an external, independent actor, such as an international organization or a state body that is considered neutral – to support stakeholders in establishing a PPP. Once the PPP is set up, it can be run by the partners or by an independent secretariat, for which funding would need to be secured.

Establish a financial plan

A cybersecurity PPP's budget will depend on its objective and planned activities. A PPP with a modest objective and a straightforward plan to hold thematic workshops, for example, may be able to run on a relatively limited budget, as facilitation and meeting expenses may be the largest costs. More ambitious or formal PPPs may require greater financial resources, particularly if they involve an official permanent representative, contact points, a secretariat, or long-term initiatives.

In drawing up a budget, PPP organizers itemize the funds required to set up the partnership, manage its activities, and carry out related tasks. In-kind contributions from the state budget or other sources may be available to cover some of these costs; for others, funds may need to be raised.

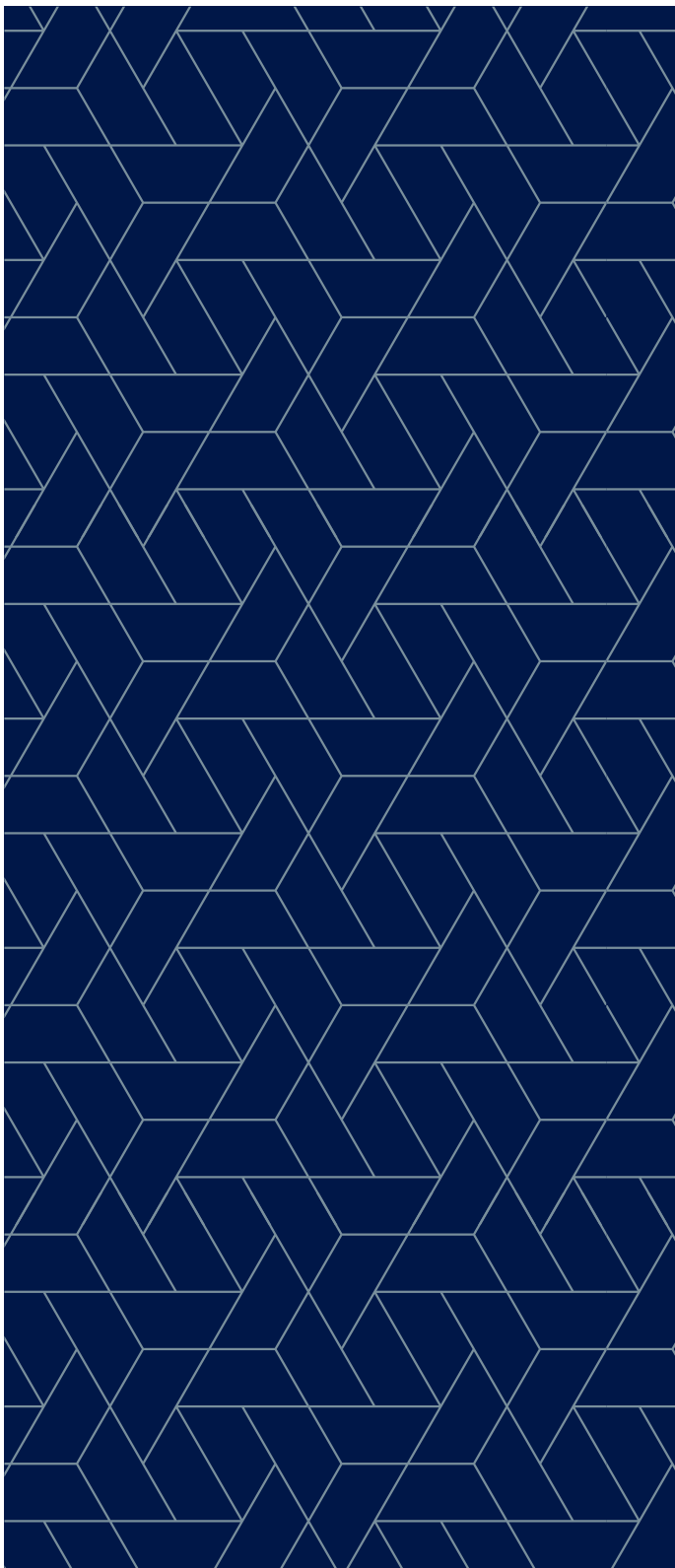
In the Western Balkans, national budgets allocate limited or no financial resources to establishing PPPs as part of cybersecurity action plans. Independent PPPs may be eligible to apply for funding from sources such as public bodies, diplomatic missions and embassies, and international organizations. As such funds tend to be project-based, however, they may

---

5 The Traffic Light Protocol is a system for classifying and encouraging greater sharing of sensitive information. The level of sensitivity is classified through the use of four colours (based on traffic lights): red means information is meant for named recipients only; amber is for limited distribution; green is for a whole community; and white is unlimited. For details, see ENISA (n.d.).

not support activities of the PPP in the long run. An alternative is membership-based funding, which can sustain basic operations indefinitely; this approach works only if all actors, including public bodies, agree to contribute.

If funds need to be raised, the PPP organizers may wish to set up a fundraising function within the partnership's structure. Partners can be encouraged to think about which resources they may be able to offer in kind, such as venues or relevant expertise.



2.3 Running a cybersecurity PPP

Key takeaways

- By planning activities strategically and evaluating results, a cybersecurity PPP can enhance its accountability and efficiency.
- The long-term sustainability and efficiency of a PPP depends on the stability of its financial and human resources.
- Good working relationships among PPP members are necessary for ensuring the partnership's long-term success. Accordingly, a PPP benefits from fostering trust among partners, promoting cohesion and communication, and developing its membership base.

Employ strategic planning and evaluate results

Strategic management methods can help to improve a PPP's effectiveness and accountability. They allow members to become more aware of their roles and how best to fulfil them. In particular, both formal and informal cybersecurity PPPs can benefit from:

- developing a clear action plan that describes how the PPP will meet objectives and how its members will contribute;
- monitoring and evaluating results;
- learning and sharing lessons;
- adopting rules and tools for ensuring transparency, including with respect to action plans, annual reports, lists of partners, and financial information, especially for PPPs that are financed by public money or that work for the public good; and
- establishing a communication strategy and securing resources for effective communication with the public (such as through a public relations point of contact).

Secure the required financial and human resources

As mentioned in Section 2.2, establishing a PPP involves planning for human, financial, and other resources. Ongoing efforts to manage a PPP's budget and raise new funds are best undertaken by specialized staff. A PPP also require funds to recruit and manage its staff members.

Foster trust continuously

Building trust among different PPP actors with diverging interests is an ongoing process – one that requires time and effort. Developing trust-based relationships is far from straightforward; years may be invested in creating a safe and supportive environment, while one single event can significantly destabilise the good relations amongst its members.

If some members feel they cannot speak freely within a PPP structure, tensions may develop and trust may be lost. Actors from the private sector or academia may react negatively to institutional limitations such as security clearance procedures and protocols, which also hamper the public sector's ability to foster open dialogue with non-state actors (Bechkoum et al., 2017). Transparency about such limitations, sensitive issues, and non-negotiable rules can help to prevent unease and conflict by ensuring that partners understand and respect one another's constraints.

Promote cohesion and communication

One way to foster trust and strengthen commitment to the PPP's objective is to promote cohesion and communication among members. Doing so is also likely to enhance the quality of each partners' work and of the partnership's overall results.

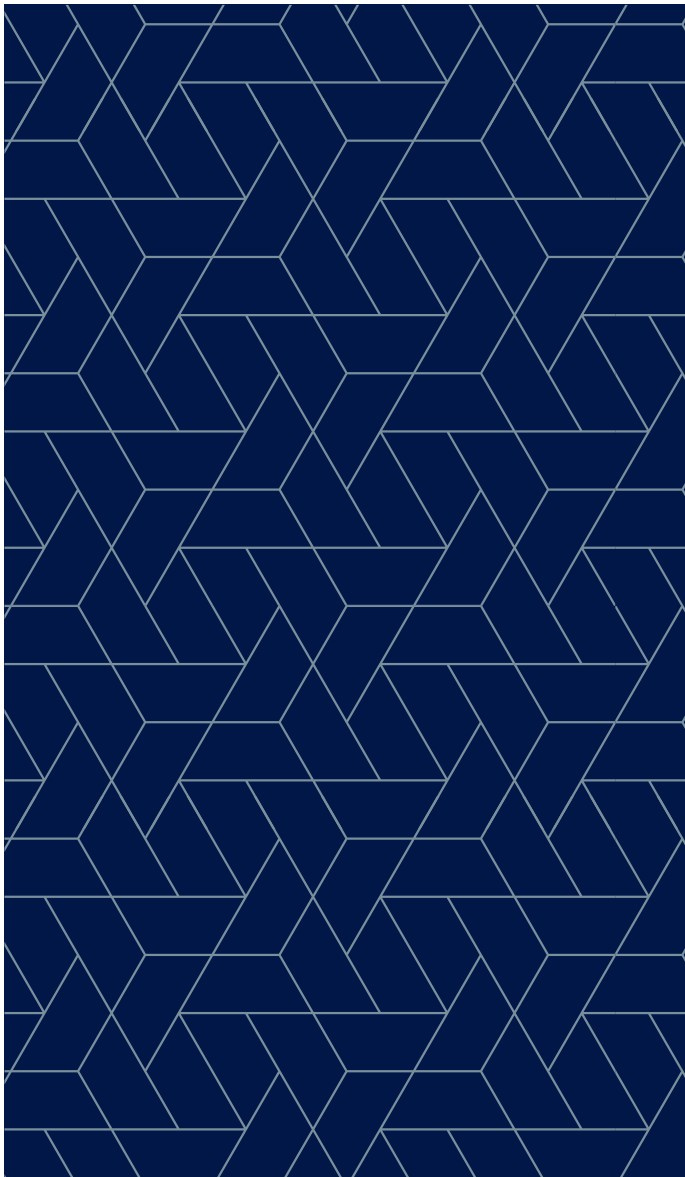
A PPP can appoint an official contact person (or institution) to facilitate communication among all actors and to disseminate relevant information. Regular face-to-face meetings, social events, conferences, trainings, and joint exercises also help to strengthen partnerships (ENISA, 2017).

Develop the PPP's membership

A PPP's membership does not remain static; it changes over time. In some cases, member turnover is expected and maybe even welcome. Less formal PPPs such as discussion forums, for instance, can profit from new members, who may introduce new skills and ideas. Even PPPs with a clearly defined membership list may lose individual members.

Every PPP needs procedures for integrating new actors. Prospective members may be asked to apply through a standardized process, or to be sponsored by existing partners, as is frequently the case in community emergency response team (CERT) communities.

Changes in membership can affect trust levels among members, as good personal relationships between partners can take a long time to establish. If turnover is high, a PPP may wish to dedicate more time to integrating new members and fostering bonds between old and new members.



Chapter 3 Examples of cybersecurity PPPs

This chapter presents five types of cybersecurity PPPs and illustrates them with selected examples from around the world, including the Western Balkans. The aim is to highlight differences and similarities across the PPP types, while also demonstrating that various forms of cooperation among cybersecurity actors have given rise to cybersecurity PPPs or may yet do so.

The examples show that the most important early step in planning a cybersecurity PPP is to determine its objective. Once the objective is clear, other details fall into place. Steps such as selecting relevant partners and a suitable organizational structure – be it formal or informal, open or confidential – follow on from the objective.

3.1 Cooperating to protect critical infrastructure

In cybersecurity PPPs that aim to protect critical infrastructure, the objective usually cannot be met unless the work is fully coordinated between the state and the private sector. While the state has the overall responsibility to protect critical infrastructure, private-sector actors typically own the various assets, including power plants, main highways, and telecommunication networks. As a result, state and business actors must collaborate to protect these assets.

Given that the protection of critical infrastructure is a national security imperative, these partnerships are highly formal, restricted structures with a clear distribution of tasks and responsibilities. Membership is limited to actors that are in charge of critical infrastructure or involved in protecting it. To prevent sensitive or classified information from being leaked and trust among the partners from being lost, such PPPs use strict security protocols.

3.2 Enhancing situational awareness through information sharing

A PPP that is focused on sharing cybersecurity information to improve situational awareness can usefully include all stakeholders that have relevant information to share (see Boxes 1 and 2). Since information about cybersecurity threats is likely to be sensitive or classified, these PPPs typically use formal structures and clear rules about the confidentiality of shared information.

Box 1 Information sharing in the United States

The United States has several Information Sharing and Analysis Centers (ISACs) and forums for information sharing. Requiring minimal organization and resources, ISACs focus on mitigating imminent cyber threats and exchanging information on the root causes of incidents and threats.

Box 2 Information sharing in North Macedonia

In North Macedonia, the National Center for Computer Incident Response (MKD-CIRT) has begun to convene relevant national actors for regular policy discussions, in line with its mandate. In addition to issuing specific guidelines for various sectors, the MKD-CIRT has established contact with community actors, including representatives of the public sector, universities, banks, and telecommunication companies. The stakeholder community engages in information sharing and has discussed draft procedures for incident classification and reporting, as well as coordination and communication in case of a national cybersecurity incident.

3.3 Improving national cybersecurity culture

PPPs that focus on enhancing a country's cybersecurity culture aim to improve the delivery of cybersecurity services for the whole nation or for certain groups, so as to boost their ability to contribute to national cybersecurity. Such a PPP might lead national cooperation on the cybersecurity education of children, for example.

Given their broad and 'soft' goals, PPPs of this type benefit from an open, inclusive, and informal approach. All stakeholders that can contribute to a topic can be included. Since confidentiality is not likely to be an issue, these PPPs can be flexible in integrating new members.

3.4 Sharing cybersecurity resources and expertise

A lack of financial and human resources among cybersecurity actors can provide a strong incentive for capacity sharing. If the public sector lacks resources, for example, non-state actors – such as experts from private businesses, academia, or the technical community – may offer their expertise.

Unlike contractors in an outsourcing arrangement, non-state actors in a partnership provide such services on a complimentary basis – in kind or as an act of social responsibility – although they may charge for related expenses.

In capacity-sharing PPPs, the need for expertise may vary over time, as may partners' ability to share their resources. Member turnover is then to be expected. Being open and maintaining good connections to all cybersecurity stakeholders can help such PPPs find new partners.

If state actors support non-state partners, a capacity-sharing PPP may require relatively formal frameworks to be able to account for the use of public money. Such frameworks can also help PPPs avoid accusations of corruption and nepotism.

3.5 Engaging in policy discussions

By being open and inclusive, policy discussion PPPs can encourage broad participation of cybersecurity actors (see Boxes 3 and 4). At the same time, formal rules can help to define the roles and responsibilities of each actor and to ensure transparency.

In particular, rules can clarify that while all stakeholders are invited to share their thoughts and expertise, policies can be adopted and implemented only by actors that are mandated to do so by law.

Rules on reporting can contribute to transparency, which, in turn, can prevent a policy discussion PPP from being perceived as a private members club with undue access to policy circles.

Formal rules can also serve to clarify a PPP's format, such as by specifying that a partnership is an established forum with regular meetings for all stakeholders, rather than one-off gatherings. Over time, such transparency can foster trust among partners and allow cooperation to flourish.

Box 3 Cybersecurity policy discussions in Bosnia and Herzegovina

In 2018, Bosnia and Herzegovina, the local mission of the Organization for Security and Co-operation in Europe (OSCE) set up an unofficial working group of leading state and entity actors, with the aim of discussing strategic directions in the cybersecurity field at the state level. The OSCE Mission has been hosting the group's regular meetings.

Comprising mainly public-sector actors from the state and entity levels, the group aspires to widen its membership to include more stakeholders from the private sector. Some small companies already started attending meetings. The group has worked on guidelines for developing strategic cybersecurity frameworks and plans to produce guidance on drafting complementary action plans.

Box 4 Serbia's Cybersecurity Network Foundation

In partnership with DCAF and DiploFoundation, the OSCE Mission to Serbia first brought together public-sector cybersecurity stakeholders in 2015. By the following year, this informal group included representatives of the private sector, civil society, and academia.

The group has discussed the first law on information security and the first national strategy on information security, as well as draft coordination and communication procedures for responding to national cybersecurity incidents. It also debated the development of public awareness raising campaigns and the latest amendments to the information security law.

In addition to all relevant public-sector stakeholders, the group comprises representatives of large, medium, and small enterprises, telecommunication companies, internet service providers, banks, vendors, companies that control critical infrastructure (including energy companies), academia, and civil society organizations. With DCAF support, the group formalised its framework and in 2019, the Cybersecurity Network was set up as a legal foundation.

Bibliography

Bechkoum, Kamal et al., Towards Stronger Cyber Security Public Private Partnerships in Developing Countries (Gloucestershire, UK: University of Gloucestershire, 2017).

CrowdStrike, 'CrowdStrike's Work with the Democratic National Committee: Setting the Record Straight', Blog (updated 5 June 2020).

DCAF (Geneva Centre for Security Sector Governance), Legal and policy frameworks in Western Balkan economies on PPPs in cybersecurity (Geneva: DCAF 2021).

DCAF, Security Sector Governance: Applying the Principles of Good Governance to the Security Sector, SSR Backgrounder (Geneva: DCAF, 2015).

Demchak, Chris, 'Cybered Conflict, Cyber Power and Security Resilience as Strategy', in Derek S. Reveron. ed., Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World (Washington, DC: Georgetown University Press, 2012).

Dunn Cavelty, Myriam, 'Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory', in Johan Eriksson and Giampiero Giacomello. eds., International Relations and Security in the Digital Age (Abingdon, UK: Routledge, 2007).

ENISA (European Union Agency for Network and Information Security), Corporative Models for Effective Public Private Partnership: Good Practice Guide (Heraklion, Greece: ENISA, 2011).

ENISA, Public Private Partnerships (PPP): Cooperative Models (Heraklion, Greece: ENISA, 2017).

ENISA, 'Considerations on the Traffic Light Protocol', CSIRTs in Europe (n.d.).

Mandiant, APT1: Exposing One of China's Cyber Espionage Units (Mandiant, 2013).

Reveron, Derek S., 'An Introduction to National Security and Cyberspace', in Derek S. Reveron. ed., Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World (Washington, DC: Georgetown University Press, 2012).

Shackelford, Scott J, 'Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance', American University Law Review, Vol. 62: No. 5 (2013), pp. 1273–1364.

Tropina, Tatiana and Cormac Callanan, Self- and Co-regulation in Cybercrime, Cybersecurity and National Security (Cham, Switzerland: Springer International Publishing, 2015).

World Bank, 'What Are Public Private Partnerships?', PPPLRC (Public-Private-Partnership Legal Resource Center) (last updated 6 February 2018).

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