**Good Governance in Cybersecurity in the Western Balkans**

1 June 2021 – 31 March 2024

**This project is implemented by the Geneva Centre for Security Sector Governance (DCAF) and funded by the UK Government’s Foreign, Commonwealth and Development Office (FCDO)**

DCAF - Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E

P.O. Box 1360

1

CH 1211 Geneva 1 [**www.dcaf.ch**](http://www.dcaf.ch/)

Switzerland

# PROJECT OVERVIEW

## Rationale:

**Beneficiaries:**

**Long-term goal: Outcomes:**

**Main Outputs:**

The project aims to contribute to a cybersecurity in the Western Balkan that not only protects the Western Balkan economies and its European neighbours but is also more responsive to the security needs of all its citizens. (Impact/Purpose)

To achieve this goal, the project will support cybersecurity policy making in Western Balkan economies that is more inclusive and collaborative. In regional and national exchanges, concrete opportunities for more cooperation amongst the six economies and multistakeholder collaboration at national level will be discussed. To contribute to informed national and regional cybersecurity policy discussions, a network of researchers will be established. Their research will in particular highlight issues around gender and cybersecurity and the cybersecurity needs of vulnerable groups and– topics so far absent from national discussions. (Outcome I)

Of equal importance are the capacity of public cybersecurity institutions in Western Balkan economies to mitigate cybersecurity threats. The project will contribute to this outcome by supporting national institutions in charge of training public sector staff and national CERTs in establishing strategic plans on increasing the cyber hygiene of general public, critical infrastructure and public sector staff. By developing capacity building plans for CERT-like structures working on securing these key ministries capacity of these structures to protect ministerial networks is improved. The development of capacity building plans and training of staff for selected national CERTs from Western Balkan economies will alow them to better protect their national networks. (Outcome II)

Western Balkan decision-makers of cybersecurity policies; national and governmental CERTs in Western Balkan countries; Civil society organizations.

To enhance cybersecurity governance in the Western Balkan region.

1. Cybersecurity policy making in Western Balkan economies is more inclusive and collaborative
2. The capacity of the public cybersecurity institutions in Western Balkan economies to mitigate cybersecurity threats is improved
3. Cybersecurity actors in the Western Balkan economies are aware of regional and national cybersecurity policy needs and collaborate at national and regional levels.
4. Quality gender sensitive research informs national cybersecurity policies in the Western Balkans economies.

DCAF - Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E

P.O. Box 1360

2

CH 1211 Geneva 1 [**www.dcaf.ch**](http://www.dcaf.ch/)

Switzerland

# PROJECT ACTIVITIES IN NUMBERS

3. Western Balkan national CERTs and ministry or sector specific cybersecurity incident response capacities have improved their ability to protect the ministerial and national networks.

4. Public sector institutions have a gender sensitive strategic plan on increasing cyber hygiene of public sector staff and national CERTs have strategic plans on increasing the cyber hygiene of general public, critical infrastructure and essential services

## National cybersecurity governance assessment reports for the six Western Balkan economies

At project start, project experts will undertake assessments of the level of cybersecurity governance in the six Western Balkan economies, based on DCAF’s methodology. The report will identify gaps and recommend actions, which will be discussed with the relevant stakeholders at the project start. This discussion will provide an opportunity for the stakeholders to clear goals that they would like to achieve through the project.

## Three Annual High-level Regional Conferences, 2021 – 2024

Once a year, high-level policy-makers from the six Western Balkan economies are gathered to discuss opportunities of regional cooperation in cybersecurity. The event aims to raise the policy-makers awareness of opportunities for cooperation (in the region and internationally) and provide a platform for discussion for countries to explore the feasibility of such opportunities. The topic of the conferences will be determined after consultations with the governments from the economies.

External experts will draft background policy papera for the annual high-level regional conferences which will discuss and provide recommendations on the topic of the conference. The policy paper will outline the issue and propose recommendations which can form the basis of discussion at the high-level regional conference.

## Organisation of National Multi-Stakeholder Meetings In 6 Western Balkan Economies

Twice a year over three years, a multi-stakeholder meeting is organised in each of the six Western Balkan economies. The meetings will be organised as workshops, round tables, table-top exercises or cyber drills. They will bring together cybersecurity actors from different stakeholder groups with the aim of: increasing stakeholder awareness; creating trust amongst stakeholders; providing an opportunity to identify and discuss national cybersecurity policy needs; test operational cybersecurity readiness; encouraging the setting up of more sustainable (formal or informal) national cybersecurity cooperation frameworks. The meetings aim at creating a more inclusive approach to national cybersecurity policy discussion and at contributing to more cybersecurity cooperation which will enhance the cybersecurity capacities of the country as a whole.

DCAF - Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E

* 1. Box 1360

3

CH 1211 Geneva 1 [**www.dcaf.ch**](http://www.dcaf.ch/)

Switzerland

## Regional Western Balkan Cybersecurity Research Network and Cybersecurity Summer School

At project start, 2 civil society researchers each from one of the 6 Western Balkan economies (12 researchers in total) will be selected to take part in a newly set- up Western Balkan cybersecurity research network. The researchers will have some general knowledge on researching cybersecurity policies. During three years they will meet up regularly (online and in person), guided by a project expert, who will train them on different aspects of cybersecurity governance and researching national cybersecurity policies. The research group will then draft and publish several research publications under the guidance of the project expert. The researchers will dedicate approximately 30% of their working time over three years to the network and receive a honorarium for this work. The policy research they conduct aims to also cover in particular aspects of cybersecurity policy which are so far underrepresented in national cybersecurity debates, such as the cybersecurity needs of vulnerable groups and gender and cybersecurity (the needs of women, men, girls and boys). The joint research also aims to:

* + - allow the researchers to increase their capacities through peer learning
		- increase trust amongst the researchers from the different economies, with the

aim of the research network continuing after project end

* + - allow for more comparative research and information on progress in cybersecurity governance in the Western Balkan region (the result of the research can then also be taken up in project activities 2 and 3 where national and regional cybersecurity policies are discussed.)

To engage a wider group of actors from civil society and other stakeholder groups to start engaging in cybersecurity policies in the Western Balkan region, the project will also organise 3 annual cybersecurity summer schools for young leaders from the region(one per project year). Young leaders (from the public and private sector) at the start of their career will raise their awareness on important cybersecurity governance challenges and have an opportunity to meet and share experiences with their peers from the region.

## Development of Capacity Development Plans for Three National CERTs (Bosnia- Herzegovina, Kosovo, Albania)

Using DCAF’s tested methodological approach for supporting CERTs in self- assessment, experts will support CERTs in analysing their capacity. An assessment report will then form the basis of a development plan. This will allow the CERTs to take practical steps to improve areas such as: their practices of attracting and retaining expert staff; planning training to increase expertise of their staff; cooperation with other relevant cybersecurity stakeholders; the strategic standing of the CERT.

DCAF - Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E

P.O. Box 1360

4

CH 1211 Geneva 1 [**www.dcaf.ch**](http://www.dcaf.ch/)

Switzerland

## Tailored Training for National CERTs of Albania, Kosovo and Bosnia-Herzegovina

Based on the capacity development plan (Activity 5), the staff of the national CERTs receives a series of targeted trainings that aim to increase the skills and knowledge of staff and achieve an increased level of professionalism of the CERT.

## Six Technical Colloquia for Western Balkan CERTs

Two meetings per year are organised for the network of Western Balkan national CERTs that was established by the DCAF project “Enhancing Cybersecurity Governance in the Western Balkans” (2018-2021), funded by the UK FCDO. In the meetings, the CERTs will discuss: common technical questions and challenges; enhancing joint cooperation amongst Western Balkan CERTs; practical exercises and trainings to test cooperation and technical skills. The aim of the colloquia is to deepen the trust amongst the national CERTs, encourage them to further cooperate (information exchange, operational cooperation) and allow them to discuss possible formal or information cooperation frameworks (based on a study established in the project “Enhancing Cybersecurity Governance in the Western Balkans“).

## Participation of Western Balkan National CERTs in International Trainings and Conferences

Members of national CERTs from the Western Balkan economies take part in international meetings and conferences on cybersecurity. At the events they increase their knowledge and skills and increase their professional network. It is expected that this this will help them to build trust with other CERTs (and lead them towards joining international CERT associations), thereby leading to more exchanges of information and operational cooperation regional and internationally.

## Development of Capacity Development Plans for Ministry or Sector Specific

**Cybersecurity Incident Response Capacities**

Using DCAF’s methodological approach for supporting CERTs in self-assessment, experts will support ministry or sector specific cybersecurity incident response capacities of key security sector ministries, such as ministries of interior and ministries of defence. The report on the self-assessment will form the basis of a development plan. This will allow the teams to take practical steps to improve areas such as: their practices of attracting and retaining expert staff; planning training to increase expertise of their staff; cooperation with other relevant cybersecurity stakeholders.

## Development of Action Plans on Public Sector Staff Cyber Hygiene for Civil

**Servants in Western Balkan Economies**

The six Western Balkan economies will receive policy advice on public sector staff cyber hygiene. Based on the advice an expert team will draw up an action plan, taking into account efforts that have already been made and providing advice on international best practices in strategically training public sector staff of cyber

DCAF - Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E

P.O. Box 1360

5

CH 1211 Geneva 1 [**www.dcaf.ch**](http://www.dcaf.ch/)

Switzerland

hygiene. The plan is supposed to allow the institution in charge of the training of public sector officials to educate them appropriately set in place internal policies (if appropriate) that allow for a greater resilience against external cyber attacks.

## Support to National Institutions in the Western Balkans on Public Awareness Raising Campaigns on Cybersecurity

The project will provide support to those state institutions in Western Balkan economies, which are in charge of raising the awareness of the public on cybersecurity (in general, national CERTs). The project will support them in producing targeted awareness raising material (videos, audio clips, etc) that they will distribute through social media and other appropriate channels. The institutions will also receive tailored advice and training on how to strategically plan and implement awareness raising campaigns and manage communication with the public. Through this support, the relevant state institutions are expected to be able to independently plan and carry out campaigns and design/commission the design of awareness raising materials.

To support the institutions in implementing the communication action plans, the project will support them in hiring young communication experts to work with them for 12 months on a part-time basis. These young communication experts will support their leadership in planning and developing proactive and sustainable outreach to specific target groups. The approach will provide the national institutions with a strategic communications framework and human capacities to implement large scale public campaigns that will lead to development of in-house knowledge, skill and practical experience needed for sustainable communication management. The expectation is that the national institutions, if they are satisfied with the performance of the young communications expert, will continue their employment after the project support ends.

DCAF - Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E

P.O. Box 1360

6

CH 1211 Geneva 1 [**www.dcaf.ch**](http://www.dcaf.ch/)

Switzerland