



REGIONAL AND TRANSNATIONAL COOPERATION





Introduction

In 2018, DCAF began a three-year project titled ‘Enhancing Cybersecurity Governance in the Western Balkans’ that emphasizes the importance of multi-stakeholder governance for cybersecurity and international coordination. Governments across the region are encouraged to work with each other and with relevant stakeholders to ensure a more effective and inclusive approach to cybersecurity challenges. DCAF organizes a variety of activities across the region to support the initiative and bring together national and international stakeholders from the public and private sector. The goal is to strengthen the capacity of Western Balkan countries to respond to the political and technical demands of cybersecurity.

While relevant policies and strategies are made at the national level, cybersecurity, by definition, exceeds the boundaries of national sovereignty. Threats and incidents in the cybersphere can instantly transcend borders with devastating effects to economic, political, and social spheres. Cybersecurity is thus an international issue that requires cooperation and trust between states to address the myriad of threats in cyberspace. As a result, DCAF focuses on enhancing regional cooperation in the Western Balkans and across Europe through a variety of interventions.

Enhancing Technical Cooperation and Contacts

Governmental and national Computer Emergency Response Teams (CERTs) are at the forefront of preventing and responding to cybersphere incidents. Each CERT must be able to coordinate with its national and regional counterparts quickly and efficiently to maintain a secure cyberspace. DCAF organizes regular joint training sessions that bring together governmental and national CERTs from Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia.

In addition to enhancing their technical and organizational capacities, the sessions serve as an opportunity for CERT staff to meet and strengthen contacts with their counterparts from across the Western Balkan region. Working together face to face helps to establish a foundation of trust that endures beyond the training’s completion. DCAF facilitates additional networking opportunities outside of training hours in more informal settings. In post-activity evaluations, participants said they found this particularly helpful for building trusted partnerships, exchanging information, and encouraging future cooperation.

Beyond the Western Balkans, CERT staff benefit enormously from establishing and strengthening connections with the wider international cybersecurity community. Consequently, DCAF also sponsors the participation of Western Balkan CERT staff in international conferences and forums.

This enables staff to exchange knowledge and experiences and to develop new channels of cooperation with peers from across Europe. Collaborating with their European counterparts also allows them to gain a wider understanding of developments in the field of cybersecurity, which is particularly important for many Western Balkans countries with nascent institutional mechanisms for enhancing cybersecurity.

Thanks to DCAF's support, Western Balkan CERT staff have attended high-level events in various locations including Cyprus, Estonia, the Netherlands, and Romania. The events allow CERTs to develop contacts and practices, and to further integration with the global cybersecurity community. Members of Serbia's national CERT (SRB CERT) attending an international conference in Tallinn, for example, met with representatives of the Forum of Incident Response and Security Teams (FIRST) to advance discussions on forthcoming plans for SRB CERT to apply for membership with the internationally renowned group. At another international cyber drill hosted by the International Telecommunications Union (ITU), DCAF-sponsored staff developed their network of contacts among other European CERT teams, members of the EU, ENISA, ITU, and other international organizations. Both interactions provided crucial opportunities to develop the capacity of Western Balkan CERTs and enable them to respond effectively to cyber incidents.

Highlighting the Importance of Cooperation for National Law-Makers

National decision-makers must be involved in efforts to enhance regional cooperation in order to develop policies and strategies that reflect the international nature of cybersecurity. DCAF's project aims to ensure that key senior Western Balkan decision-makers are able to assess cybersecurity challenges and understand the importance of regional and international cooperation. National awareness-raising roundtables are regularly organized across the region to achieve this goal. DCAF's wealth of experience and expertise in the Western Balkans means it excels in bringing together top cybersecurity stakeholders to tackle issues with an inclusive and holistic approach. The events offer an ideal forum for senior decision-makers to meet face to face with representatives of international organizations, civil society organizations, and other members of the public and private sector to see and hear first-hand the benefits of wider regional cooperation. In 2009, for example, DCAF organized a roundtable in North Macedonia that brought experts from NATO member states together with North Macedonian policy-makers to discuss matters pertaining to the expected national cyber defence strategy. The event helped policy-makers to develop strategic goals and attain specific documents from NATO as an aspiring member.

Tested Formula for Greater Regional Cooperation

DCAF's project reaches key members of governments and CERTs from six Western Balkan countries. It has significantly bolstered regional cooperation by creating opportunities for the region's key cybersecurity stakeholders to engage informally and to build trust between themselves, their organizations, and governments. At the global level, DCAF's activities have played a crucial role in helping Western Balkan CERTs to obtain accreditation in some of the world's most respected CERT networks. While this achievement is not down to DCAF alone, every activity to date has strongly supported this process and has been guided by the standards set for obtaining such membership and accreditation. The confidence and trust placed in DCAF's work demonstrates to political and technical cybersecurity actors the value of regional and international cooperation and the path toward strengthening it.



DCAF Geneva Centre
for Security Sector
Governance

DCAF Geneva
P.O. Box 1360
CH-1211 Geneva 1
Switzerland
Tel: +41 (22) 730 94 00
Email: info@dcaf.ch

DCAF Brussels
/ EU SSG Facility
24 Avenue des Arts (boîte 8)
1000 Brussels
Belgium

DCAF Ljubljana
Gospodinjska ulica 8
1000 Ljubljana
Slovenia

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

DCAF Beirut
Gefinor Bloc C
Office 604, Ras Beirut
Lebanon

DCAF Tunis
Rue Ibn Zohr 14
1082 Tunis
Tunisia