DCAF Geneva Centre for Security Sector Governance

CYBERSECURITY GOVERNANCE ASSESSMENTS

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.

A roadmap for strengthening cybersecurity governance

Network systems have faced an increasing number of risks in recent years, which have, in turn, threatened the safe and efficient use of cybersphere services. Regardless of whether this is the result of unintentional or deliberate actions, the consequences can instantly transcend borders and societal sectors with devasting effects on economic, political, and social spheres. In the Western Balkans, certain countries must act quickly to consolidate and improve their cybersecurity governance systems. With an emphasis on short- to mid-term action, DCAF implements governance assessments that highlight gaps and provide Western Balkan governments with a clear foundation and roadmap for enhancing their cybersecurity capacities over time.

Each country faces its own unique set of cybersecurity challenges; its capacity to respond to these challenges varies, as do the tools at its disposal. DCAF's assessments begin with multiple expert visits to the country in focus to determine the effectiveness, efficiency, and accountability of the current governance system. Thanks to nearly two decades of experience in the region, DCAF's expertise and background knowledge provides a deep understanding of the limitations of, and potential opportunities for, improving existing systems. DCAF experts also carry out thorough desk research, interviews with key national stakeholders, field research, meetings, and interactive activities.

A holistic approach to cybersecurity

Widespread participation and efficient coordination between relevant actors serve as the cornerstones of cybersecurity. DCAF strives for a holistic view of the cybersecurity governance landscape by examining the capacities of actors across the entire security system, rather than simply security actors. DCAF reviews actors in charge of planning, managing, and coordinating cybersecurity; actors in charge of delivering specific cybersecurity services (either for specific government networks or all national networks); and actors responsible for overseeing the delivery of cybersecurity. By considering elements such as control and oversight, DCAF's recommendations seek to improve the overall governance system while sticking to our broader mission of enhancing human and state security within a framework of democratic governance, the rule of law, and respect for human rights.

Constant national involvement

Once DCAF has collected data from numerous expert visits, we produce an assessment report that evaluates the country's cybersecurity capacities and offers actionable recommendations for key national stakeholders. Feedback from national actors is critical for the project's ultimate success – it ensures that the process remains locally accountable and relevant for each country. In addition to sharing early drafts of the report, DCAF organizes a series of cross-sectoral focus group meetings and tabletop exercises that enable stakeholders to discuss the report's findings and to test the suggested models of cooperation and coordination. The process also helps DCAF to improve the report and its recommendations by considering input from stakeholders and triangulating data better.

As highlighted above, cyber incidents affect nearly all sectors of society. Effective cybersecurity governance requires active participation from all relevant stakeholders, as well as timely and clear communication. Practical exercises enable stakeholders to gather together to test findings and respond to gaps in the cybersecurity governance structure. For many participants, the events serve as their first opportunity to meet and exchange with other cybersecurity actors in the country. They form a valuable foundation for continued coordination and contact between all actors, which endures long after DCAF's experts provide the final assessment.

Ensuring local ownership and long-term success

The primary goal of DCAF's assessment projects is to lay the groundwork for establishing a national dialogue on how stakeholders can improve their current cybersecurity governance system. Thanks to its recognized regional expertise and a methodology that encompasses all levels of the governance and security system, DCAF's projects often go beyond this goal with recommendations that can be implemented immediately, and that offer a pathway towards sustainable and inclusive cybersecurity governance.

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