DCAF Geneva Centre for Security Sector Governance

Cybersecurity Capacity Building and Donor Coordination in the Western Balkans

Fabio Barbero, EUISS
Nils Berglund, EUISS

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

Contents

EXECUTIVE SUMMARY

Continued interest and investment in cybersecurity capacity building in the region clearly indicates that the Western Balkans remains a strategically important region for a number of international actors. Systematic, coordination-by-design methodologies and best practices among donors that utilise whole-of-society and multi-stakeholder approaches can improve the legitimacy, ownership and sustainability of outcomes in the context of persistent challenges to human capacity, political will, and resource scarcity. Furthermore, to better define the roles of different capacity building actors, help identify opportunities for strategic partnerships, and clarify donor-recipient relationships, donors should seek to strengthen the links between policy objectives and strategies for capacity building interventions. As the interwoven threats and opportunities of cybersecurity and digital development grow more complex, and geopolitical tensions rise, both donors and recipients should look towards a more holistic understanding of capacity building in the Western Balkans that also enables meaningful international engagement on the peace and security of cyberspace.

INTRODUCTION

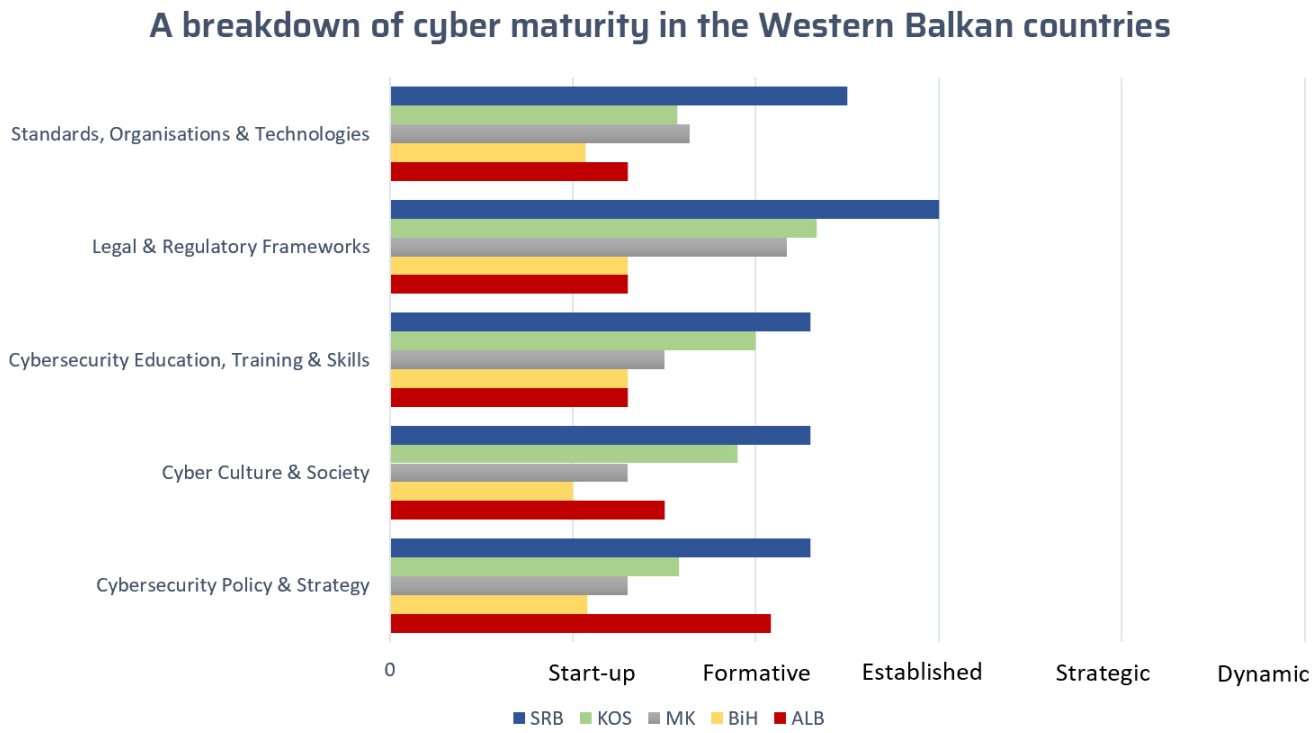
Cyberspace is a theatre where states cooperate and compete over their interests and values across all domains: security, diplomacy, criminal justice and development. Digital transformation – with ubiquitous access to the internet at its core – has become one of the key drivers for economic growth and societal changes. It is not surprising, therefore, that cybersecurity and resilience have become an important target for domestic reforms and an aspect for strengthening international cooperation. However, not all states have the resources and expertise required to pursue those objectives in a structured and sustainable manner.

As the Cybersecurity Capacity Maturity Model (CMM) Review Reports for the Western Balkans countries show[1], cyber maturity in the region ranges from start-up to formative levels, scoring differently depending on countries and across dimensions (Fig.1). Despite remarkable exceptions, several states still lack official cybersecurity documents detailing how to establish coordination between key cybersecurity governmental and non-governmental actors or lack an overarching national cybersecurity strategy. Several emergency response teams exist in the region, however the degree of government-led coordination at the national level varies from country to country, together with CERT's affiliation to international consortiums such as FIRST[2]. Relevant difference exists with regards to the existence of formal categorisation of critical infrastructure and related legislation. National cybercrime legislation exists in most countries in the region, but challenges in the effective prosecution of cyber criminals and in the alignment of laws with regional legal instruments such as the Council of Europe's Convention on Cybercrime remain. Different levels of awareness exist around the protection of personal information and the security of personal data, with a growing – but still insufficient – cybersecurity culture among citizens, which varies greatly depending on internet penetration, the uptake of e-commerce and e-government in the national economy, and the availability of cybersecurity education in national curricula.

---

1 CMM reviews have been conducted for all WB countries. All except Montenegro published their CMM reviews, which are accessible here: https://gcscc.ox.ac.uk/cmm-reviews
The graphic below was compiled by the authors based on publicly available CMM reviews: Each of the CMM stages of cyber maturity, i.e. start-up, formative, established, strategic, and dynamic was assigned a score from 1 (start-up) to 5 (dynamic). A score for each dimension was calculated based on the average score of each factor within said dimension.

2 At time of writing, only Serbia and Montenegro are members of Forum of Incident Response and Security Teams (FIRST). https://www.first.org/members/map



The need to close the gap between those most and least advanced as well as to continue advancing the global levels of 'cyber readiness' against the background of evolving cyber threats and digital risks is what has attracted everybody's attention to the existing mechanisms such as technical cooperation and capacity building/development.

Cyber capacity building (CCB) can be broadly defined as the development and reinforcement of processes, competences, resources and agreements aimed at strengthening national capabilities, at developing collective capabilities and at facilitating international cooperation and partnerships in order to respond effectively to the cyber-related challenges of the digital age. These CCB activities can contribute to preventing cyber-related risks, to protecting citizens, infrastructures and processes, to the pursuit of criminal acts in cyberspace and to the response to malicious cyber events.[3]

Amid an evolving threat landscape and an upsurge in investment, the Western Balkans have seen a proliferation in cyber CCB activities carried out by both national and international actors. Despite the existing gaps, progress in the understanding of the importance of building adequate capacities has increased in the region, allowing Western Balkans nations to become players and partners as opposed to mere recipients.

Given the increasing number of stakeholders involved in the field globally, the 2018 'Council Conclusions on EU External Cyber Capacity Building Guidelines'[4] recognised that such a proliferation, "creates opportunities for synergies and burden-sharing but also poses challenges in terms of coordination and coherence." As such, it called upon the EU and its Member States "to continuously engage with key international and regional partners and

3 Pawlak P. (2018) (ed.), "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building". Available at: https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building. See also the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building (2017) at: https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf

4 Council of the European Union (2018), EU External Cyber Capacity Building Guidelines, Council Conclusions (26 June 2018). Available at: https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

organisations as well as with civil society, academia and the private sector in this field with the aim of avoiding duplication of effort given the limited resources."

The COVID-19 pandemic has brought new challenges to CCB activities in the region. As policymakers face the health crises and its social and economic impacts, more competing priorities limit the financial, human and time capacities that can be devoted to cyber capacity building. For donors and implementors, shifting political priorities may make the reception of CCB activities more challenging, while the broadening of the surface attack due to COVID-19 - comprising for example hospitals and the health supply chain - brings forward new areas for capacity building. On the other hand, the pandemic makes coordination even more important as it allows for more efficient allocation of resources. Yet, in the absence of venues for physical meetings and venues for networking, coordination between donors and implementors has been disrupted to a great extent.

In this context, our discussion paper explores how cyber capacity building actors and initiatives in the Western Balkans could be better coordinated, while considering the barriers to reaching cyber maturity in the region. Firstly, we offer a non-exhaustive overview of projects, donors, and implementors active in the Western Balkans, based on desk research and a series of interviews with relevant stakeholders. Secondly, the paper will explore best practices on coordination through the framework of the Operational Guidance for the EU's International Cooperation on Cyber Capacity Building[5]. Lastly, based on the above, some conclusions and broad recommendations are proposed, with an eye to future CCB investment.

PARALLEL CAPACITY UNIVERSES IN THE WESTERN BALKANS

Cyber capacity building is inexorably linked to ongoing international debates about the peace and stability of cyberspace.[6] As a process focused on human resources development, organisational arrangements and legal and institutional frameworks, CCB activities can generally be understood as promoting an implicit or explicit set of political and social arrangements that reflect the values and priorities of a given donor. While such projects build capacity by strengthening infrastructure and skills, they function as diplomatic mechanisms for aligning positions on cyber-related issues.[7] Rather than purely technocratic endeavours for socioeconomic development, then, capacity building initiatives implemented by international actors are also a form of political instrument, oriented around the advancement of foreign policy interests. As such, different actors engage in the Western Balkans with particular strategic priorities and policy objectives, that tend to shape the nature of their cyber capacity building interventions.

THE EUROPEAN UNION

The EU cybersecurity strategy published in December 2020 expressly stated that "EU cyber capacity building should continue to focus on the Western Balkans and in the EU's neighbourhood [...] The EU efforts should support the development of legislation and policies of partner countries in line with relevant EU cyber diplomacy policies and standards[8]". The doc-

5 Pawlak P. (2018) (ed.), "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building". Available at: https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

6 See for example A/RES/74/173 in the United Nations General Assembly, adopted in December 2019.

7 Pawlak, P. (2016). Capacity Building in Cyberspace as an Instrument of Foreign Policy. Global Policy, 7(1), 83–92. Available at: https://doi.org/10.1111/1758-5899.12298

8 European Commission (2020), "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade". Available here: https://ec.europa.eu/digital-sin-

ument calls upon the EU to develop a training programme dedicated to EU staff in charge of the implementation of the union's digital and cyber external capacity building efforts. A clear nexus is also drawn between malicious cyber activities and the integrity and security of democratic systems and societies.[9] Moreover, the EU's economic and investment plan for the Western Balkans from October 2020[10] stressed that the EU should support cybersecurity capacities with particular regard to infrastructure and the digital transition, "developed based on a needs assessment to be conducted in 2021."[11] As a self-described enabler of that transition, the EU called for the Western Balkans to focus on reform priorities, including "cybersecurity capacity and the fight against cybercrime, especially by implementing the EU toolbox regarding cybersecurity risks to 5G networks."

With the Council of Europe, the European Union has been funding joint regional projects on cooperation against cybercrime under the Instrument of Pre-Accession (IPA). The Cyber@IPA programme[12] (2010-2013) was utilised to further align legislation to the Budapest Convention, support the set up and specialisation of high-tech crime units in police and prosecution services, and foster a regional network of cooperation. From January 2016, the 48-month project iPROCEEDS[13] – funded under the IPA II Multi-country Action Programme 2014 – focused on strengthening the capacity of authorities to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet in Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Turkey and Kosovo*. From January 2020, a second iteration of the project was launched, targeting Albania, Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia, Turkey and Kosovo* for an additional 42 months. Based on the previous capacity building efforts, iPROCEEDS 2 focuses on the alignment of personal data protection with EU and CoE's standards, on interagency and public-private cooperation in investigations, public reporting systems on online fraud and other cybercrime offences, judicial training and international cooperation and information sharing for investigation of cybercrime and online crime proceeds.[14] Among the detailed actions foreseen by the programme, one can find workshops and training courses on cybercrime and electronic evidence for judges and prosecutors, case simulation exercises and mock trials, first responder training courses, tabletop exercises and simulations with service providers, etc. The project also refers to the development of guidelines and templates for international cooperation, to the support of partnership building, of the preparation of beneficiary reports on cybercrime and cybersecurity trends and criminal justice statistics and the support in setting-up online reporting platforms for cybercrime in North Macedonia and Kosovo*. Notably, this project dovetails with other Council of Europe cybercrime initiatives

gle-market/en/news/eus-cybersecurity-strategy-digital-decade

9 See also the "European Democracy Action Plan". Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

10 European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An Economic and Investment Plan for the Western Balkans". p. 12. Available at :https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/communication_on_wb_economic_and_investment_plan_october_2020_en.pdf

11

12 CyberCrime@IPA Project Page. Available at : https://www.coe.int/en/web/cybercrime/cybercrime-ipa

13 iPROCEEDS – Targeting crime proceeds on the internet in South Eastern Europe and Turkey website. Available at: https://www.coe.int/en/web/cybercrime/iproceeds
* This designation is without prejudice to positions on status and is in line with UNSCR 1244(1999) and the ICJ Opinion on the Kosovo declaration of independence.

14 iPROCEEDS-2 Project Summary, v. 6 December 2019. Available at : https://rm.coe.int/0000-iproceeds2-summary-v2/16809942df

in the region, including the End Online Child Sexual Exploitation and Abuse (EndOCSEA) project funded by the EVAC fund[15].

Another intervention, the "Enhancing Cybersecurity, Protecting Information and Communication networks" (ENSYSEC) project, was carried out from 2014 to 2016 under the Instrument contributing to Stability and Peace managed by the Directorate General for International Cooperation and Development (DG DEVCO) of the European Commission. The project, implemented by Expertise Française[16] in partnership with Civipol, aimed to increase the security and resilience of ICT networks in the beneficiary countries by "building and training local capacities to adequately prevent, respond to and prosecute cyber attacks and/or accidental failures".[17] In particular, it supported North Macedonia, Moldova and Kosovo* to build capacities for national CERTs, to provide advice on policy, financial and legal implications of national cyber security strategies and to enhance public-private partnerships and cooperation internationally.

In January 2020, the EU announced, within its Instrument for Pre-Accession Assistance (IPA II), an 8-million-euro intervention in support of cybersecurity capacity building in the region, starting in 2021. The EU support to cybersecurity capacity building in the Western Balkans intervention aimed to "build up functioning and accountable institutions in the Western Balkans to strengthen the region's cyber resilience in order to respond effectively to challenges and risks such as cyber attacks."[18] Despite the magnitude of the intervention, which was supposed to target all the six Western Balkans economies for six years, in August 2020 the procurement procedure was cancelled "due to a re-assessment of the implementation modality and scope of the project". While it is at present unclear if and when these or other EU funds will be available for the region, several EU documents gesture to the strategic importance that the Western Balkans should have for the EU when it comes to CCB.

Certain EU member-states are also engaged in bi-lateral capacity building projects, notably, the Netherlands funded project on Supporting good governance and public-private partnership in cybersecurity in Serbia, implemented by DCAF from September 2019 to September 2020. The project supported the public-private partnership initiative 'Petnica Group', a group of representatives from institutions, regulators, oversight bodies, regulators, the private sector and academia. The project aimed to formalise the group's objectives and operations through meetings, workshops and exercises, therefore ultimately giving a structure to public-private partnership in Serbia.

THE UNITED KINGDOM

According to the 2016-2021 Cybersecurity strategy, the UK's international engagement is intended to "exert our influence by investing in partnerships that shape the global evolution of cyberspace in a manner that advances our wider economic and security interests."[19] In the Western Balkans in particular, the strategy of the Foreign, and Commonwealth & Devel-

15 EndOCSEA project page. Available at: https://www.coe.int/en/web/cybercrime/endocsea-europe

16 'L'Assistance au Développement des Échanges en Technologies Économiques et Financières' (ADETEF) aided the implementation but was later integrated into Expertise France.

17 ENCYSEC project website. Available at: http://www.encysec.eu/web/

18 "EU support to cybersecurity capacity building in the Western Balkans" programme information at: https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1580863587704&do=publi.detPUB&orderby=upd&page=1&orderbyad=Desc&searchtype=QS&aoref=140655&nbPubliList=50&userlanguage=en

19 National Cyber Security Strategy 2016 to 2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

opment Office (FCDO) after Brexit is focused primarily on security cooperation and tackling corruption and organised crime.[20]

The Cybersecurity Governance in the Western Balkans project, started in July 2018 and implemented by DCAF, involves to different extents all Western Balkans countries and is expected to run until March 2021. The project, aimed to support eighteen national governance reforms processes and actors, comprises three main pillars: i) supporting cybersecurity governance policy-making dialogue in Bosnia and Herzegovina, Montenegro, North Macedonia and Serbia; ii) building capacity of national and governmental CERTs in Montenegro and Serbia[21]; iii) enhancing regional and international CERT cooperation across the six beneficiary countries.

The FCDO also sponsors the Chevening Cyber Security Fellowships, delivered by Cranfield University and allowing mid-career professionals from the Western Balkans to attend a 10-week program focusing on cybersecurity policy and its implications for national security, commercial opportunity, crime prevention, and the right to privacy, as well as on trust building and sharing of best practices.

THE UNITED STATES

The US National Defence Strategy (NDS) has called for strengthening alliances and attracting new partners in the context of strategic competition with China and Russia. As such, engagements in the region are centred around a defence-forward strategy that emphasises the strengthening of NATO alliances and cyber defence.[22] In the context of cybersecurity, this has translated primarily through technical expertise and hardware, but also human capacity. As the US Bureau of Global Public Affairs mentions, following their NATO accession in 2017, U.S. cyber experts worked alongside government officials from Montenegro in 2018 and 2019 to counter malicious cyberattacks on critical networks and platforms. As one of the primary implementors of cyber capacity building for the U.S. Department of State, Carnegie Mellon University's Software Engineering Institute (SEI) has also supported national CERTs in the region, as well as tabletop exercises. Back in 2011 for example, their project "Albanian Cyber-Security Program", aimed to "build the Government of Albania's capacity to prevent and respond to cyber-security incidents," and ran a series of workshops and trainings that supported the establishment of the Albanian Cyber Incident Response Agency (ALCIRT). Notably, SEI support and cooperation has also extended beyond NATO members, including to the National CERT of the Republic of Serbia (SRB-CERT).[23] Another implementor operating as part of the US Department of State Cyber Capacity Building program is the George C. Marshall European Center for Security Studies, which has implemented training courses, and inter alia, runs the Program on Cyber Security Studies (PCSS) where national officials, including those from the Western Balkans, have been sponsored.[24]

---

20 Hoxhaj, A. (2019). "The UK's Policy on the Western Balkans Post-Brexit". Globe Centre Policy Brief #6, University of Warwick https://warwick.ac.uk/fac/soc/law/research/centres/globe/policybriefs/web_pb6_a_hoxhaj_by_research_retold_-_19_nov_2019.pdf

21 From March to August 2017, the UK Good Governance Fund and DCAF supported – through the MUP CERT project – the cyber emergency response team of the Serbian Ministry of Interior, which acted at the time as the Serbian CERT of last resort.

22 National Defense Strategy (NDS). Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

23 SRB-CERT Proceedings (2019) Regional Cybersecurity Conference, 05-06 June 2019, Ohrid. Available at: https://mkd-cirt.mk/wp-content/uploads/2019/04/2019Ohrid_6.1.-Jelica-Vujadinovic-SRB-CERT-Nacional-ni-CERT-Ohrid-2019-v1.pdf

24 Program on Cyber Security Studies (PCSS) Courses. Available at: https://www.marshallcenter.org/en/academics/college-courses/program-cyber-security-studies-pcss

THE OSCE

The mandate for the Organisation for Security Co-operation in Europe spans across 'politico-military', environmental, economic, and human aspects. Through a number of institutions and structures, their activities encourage participating states to commit to "full respect for human rights and fundamental freedoms; to abide by the rule of law; to promote principles of democracy."[25] As a member-state organisation of which all Western Balkan states are a part, their capacity building initiatives in the region are internally focused, coordinated through the national OSCE mission offices. The OSCE has intervened in the region primarily in relation to supporting national cybersecurity governance reforms and confidence-building measures. From October 2017 to December 2020, the OSCE was involved in supporting the implementation of Confidence-Building Measures through an initiative funded by Germany and the United States. According to the project's entry in the Cybil portal[26], the project worked with Western Balkans states (except Kosovo*) "to identify and prioritize national implementation challenges", as well as "creating national CBM implementation roadmaps and a customized capacity building assistance plan in cooperation with international partners."[27] Pending additional funding, the OSCE also hopes to carry out a national table-top exercise on "Preventing and Countering the Use of the Internet for Terrorist Purposes" in the region[28]. With regards to Serbia, the local OSCE Mission supported the national public-private dialogue, facilitating the creation and maintenance of the Petnica Group[29]. In Bosnia and Herzegovina, the local OSCE Mission supports the work on developing national cybersecurity strategic frameworks.

THE WORLD BANK

The World bank has historically supported the Western Balkan countries on economic transition, early reforms, as well as post-conflict reconstruction in Bosnia and Herzegovina, and Kosovo*. Today, the World Bank Group's Western Balkans program is centred around economic transformation opportunities in conjunction with their support of European Union Ascension.[30] Between 2016 and 2019, the World Bank, with the funding of the Korea-World Bank Group Partnership (KWPF), has undertaken a Global Cybersecurity Capacity Program. As part of the programme, the Global Cyber Security Capacity Centre (GCSCC) of the Oxford University conducted a series of Cybersecurity Maturity Model for Nations (CMM) assessments of Albania, Bosnia and Herzegovina and North Macedonia. Following this exercise, several CMM Review reports were published and currently five countries out of six in the region have made those assessments public. The Global Cybersecurity Center for Development (GCCD) within the Korea Internet & Security Agency (KISA) also delivered a series of cybersecurity capacity-building workshops and trainings[31]. Building on this ex-

25 OSCE Office for Democratic Insitutions and Human Rights Mandate. Available at: https://www.osce.org/odihr/mandate#:~:text=ODIHR%20is%20tasked%20with%20assisting,promote%20tolerance%20throughout%20their%20societies.

26 The Cybil portal is a knowledge database for Cyber Capacity Build programmes operated by the Global Forum on Cyber Expertise. Available at: https://cybilportal.org/

27 Confidence-Building Measure Customized Implementation Support" Cybil entry at: "https://cybilportal.org/projects/confidence-building-measure-customized-implementation-support/

28 From January 2019 to December 2020, the OSCE carried out three national table-top exercises in Central Asia, with ambitions of expanding to South-Eastern Europe.

29 Rizmal, I. (2018), "Guide through Information Security in the Republic of Serbia 2.0." OSCE Mission to Serbia. Available at: https://www.osce.org/mission-to-serbia/404255?download=true

30 Western Balkans Program Overview, Brief, 16 October 2019. Available at: https://www.worldbank.org/en/region/eca/brief/vienna-see-program-overview

31 Global Cybersecurity Center for Development (GCCD) project webpage. Available at: https://www.kisa.or.kr/eng/mainactivities/internationalCooperation_01.jsp

perience, the Global Cybersecurity Capacity Program II was launched in 2019, expanding the list of target countries in the Western Balkans to Kosovo*, Montenegro and Serbia[32]. The program is expected to run until June 2021, providing policy dialogue on cybersecurity, tailored knowledge products and cybersecurity assessments, technical assistance and capacity-building mainly targeted to cybersecurity policymakers. In 2019, a Report containing "Lessons Learned and Recommendations towards strengthening the Global Cybersecurity Capacity Program" was published[33]. The Cybersecurity Alliance for Mutual Progress (CAMP), initiated by the Korean government, also involves the Ministry of Economic Development (MED) in Kosovo* and the Ministry for Information Society and Telecommunications (MIST) in Montenegro as members. Within the 3rd CAMP Regional Forum, seminars and forums to enhance cybersecurity capabilities were held in Belgrade and Skopje.

THE UNITED NATIONS

The United Nations has supported cybersecurity projects in the Western Balkans through a number of agencies. Most notably, the UN International Telecommunications Union's (ITU) capacity building initiatives support and inform on the use of ICTs for sustainable development, and "promote the availability of infrastructure and foster an enabling environment for telecommunication/ICT infrastructure development and its use in a safe and secure manner"[34] through assistance to developing countries. In the Western Balkans, they have encouraged the integration of ICTs into the broader economy and society through the support of an annual digital summit.[35] They also provide technical assistance in the region, upon the request of UN member states. As such, the ITU also engaged with several Western Balkans countries in defining national CERT development plans, mainly through ad-hoc technical support in Montenegro (Jan-Dec 2010), Serbia (Jan-Dec 2010), North Macedonia (Jan-Dec 2014), Bosnia and Herzegovina (Jan 2017-Dec 2018) and Albania (Jan-Dec 2018). These ITU interventions aimed to study institutional and organizational requirements and arrangements for setting-up National CIRTs.[36]

The United Nations Development Programme (UNDP) has also supported cybersecurity capacity building initiatives, notably in Kosovo*, through the Kosovo Safety and Security Programme (KSSP) ongoing from 2017-2021. The project has supported the National Council on Cyber Security as well as a stakeholder working group in "developing legal and policy frameworks in line with the EU norms and standards to improve cyber security".[37] As part of a wider project running from 2018-2021 funded by the Norwegian Embassy in Belgrade,[38]

---

32 World Bank project web entry. Available at: https://www.worldbank.org/en/news/feature/2020/06/01/kwp-fgscp

33 World Bank (2019), "Global Cybersecurity Capacity Program. Lessons Learned and Recommendations Towards Strengthening the Program". Available at: http://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf

34 ITU-D Mandate, Mission and Strategy. Available at: https://www.itu.int/en/ITU-D/Capacity-Building/Pages/MandateStrategy.aspx

35 Western Balkans Digital Summit. Tirana 2020, ITU event entry at: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2020/DigSumWB/Tirana.aspx

36 For example, the ITU organised a workshop in Skopje with the Government of North Macedonia and DCAF, aiming to support national cybersecurity strategies development and implementation in the regional economies. In 2019, the ITU, together with the Geneva Centre for Security Sector Governance (DCAF) and the Regional Cooperation Council (RCC) organised regional to develop capacities on national cybersecurity strategies.

37 Kosovo Safety and Security Programme (KSSP) Project Summary. Available at: https://www.ks.undp.org/content/kosovo/en/home/projects/kosovo-safety-and-security-project.html

38 Norway for You—Serbia Press Release. Available at: https://www.norveskazavas.org.rs/en/vtext/norveska-nastavlja-podrsku-razvoju-srbije-kroz-novi-projekat-norveska-za-vas-srbija-1

the United Nations Office for Project Services (UNOPS) is also implementing an initiative that aims to strengthen the Serbian Government's information security. The project aims to develop a methodology for identifying critical information infrastructure and enhance resilience through the procurement of a cybersecurity platform for national cyber drills and accompanying trainings.[39]

ENHANCING COORDINATION THROUGH CAPACITY BUILDING PRACTICES[40]

The European experience with the cyber capacity building demonstrates that grounding project development in the existing project management instruments and mechanisms might offer at least partial response to the challenge of coordination. While being particularly relevant in the initial stages of the CCB process, good coordination permeates the broader architecture of an intervention (i.e., coordination-by-design). As observed in the Operational Guidance in relation to the EU's action, "different intervention logics, if not addressed from the outset, may undermine the coherence of EU action and result in sub-optimal outcomes in terms of economic opportunities created, competitiveness or sustainability."[41] The following paragraphs aim to provide an overview of the role of coordination throughout the stages of the cycle.

A thorough mapping of stakeholders is crucial to understand who is active in a specific policy context, which actors can share up-to-date information that may be useful for the project's set-up, and who may be affected by the change that the project intends to bring. Tools such as the Cybil Portal by the Global Forum on Cyber Expertise represent an invaluable one-stop shop to conduct a first stakeholders mapping.

The mapping of stakeholders should analyse the coordination mechanisms in place, both within the national context (e.g. cross-sectoral consultations) and within international donors' or implementors' structures. The aim of this activity should be to understand the most used mechanisms in a specific environment and draw lessons on their applicability in the specific project that is being set up. Coordination is essential to increase situational awareness and allows to learn if some of the needs identified in a country – or that will be identified by the project – have already been addressed by other CCB projects. Ultimately, it averts the risk of duplication of efforts. For example, the Council of Europe coordinates all of their cyber activities in the Western Balkans through the same cybercrime office in Bucharest, and harmonizes their work on online harms, technical assistance, legal support and law enforcement cooperation through joint-objectives, standard procedures and internal consultations, ensuring that their work is unified despite several funding streams. The OSCE has hosted consistent stakeholder meetings and informal working groups focusing on building links between implementers in the region. This practice can lead to the creation of a contact network including updated persons of contact within governments and ministries. Similarly, DCAF, the ITU, and the Regional Cooperation Council (RCC) have engaged tri-laterally on the regional coordination of national CERTs and their human capacities.

---

39 Based on interview data.

40 This specific section draws from the Cyber Capacity Building Framework (CCBF) proposed in the "Operational Guidance for the EU's international cooperation on cyber capacity building" and is based on the analysis of several general capacity-building and development frameworks adopted by donor agencies, as well as best practices put forth by cyber policy organisations. As the CCBF is grounded in methodologies of the development community, it exhibits overlaps with other dominant approaches like the EU's Project and Programme Management Cycle (PPMC), based on the Logical Framework Approach (LFA) and the Theory of Change (ToC).

41 Pawlak P. (2018) (ed.), Operational Guidance, op. cit., p. 66.

Any project must be informed by a thorough analysis of the policy context, allowing for the identification of priority areas and issues to be addressed. Coordination in this sense is two-fold: with the national stakeholders to make sure that donors and implementors are aware of the country's priorities and how their actions fit into the partner's goals; among donors to build synergies and division of labour, to share good practices and to pool resources in the view of minimizing costs, increasing the coherence of actions and their effectiveness, as well as of sharing risks. This is particularly important as some actors may approach particular cyber-related issues through the lenses of building government's capacities, while other may look more at impact of state actions on civil liberties and citizens' privacy. Coordination in the analysis of the policy context helps to grasp the interlinkages between policy areas, on which each actor may focus specifically and have specific expertise. Furthermore, dialogue among donors avoids that differences in policy objectives lead to 'forum shopping', whereby potential partners look for the most sympathetic or least demanding intervention towards the partner's positions, views or policies[42].

Once the public policy and context are better understood, the next step is to define specific objectives of a possible intervention and assess the capacities required to achieve them. Since capacities evolve and depend on a multitude of environmental factors, the assessment cannot be a one-off exercise but needs to be a continuous process that needs to be designed and carried out in collaboration with the partner countries and organisations. Capacity assessments should be participatory in nature, and when possible, make use of available home-grown expertise. While building on existing capacities, donors can also help develop home-grown expertise: the UK-funded Chevening fellowships has for example built local competences in the short term while creating a well-coordinated network of experts to draw upon and contact in future engagements.[43] In this sense, participatory self-assessments do not only contribute to capacity development on their own, but also bring forward the acceptance of ownership for the required change process.[44] Capacity assessments can improve donor coordination by providing an overview of the cybersecurity landscape, considering capabilities of both implementers and recipients. This includes determining where an implementing organisation fits within that broader architecture, and if mandates and rules match their role and its intended outcomes. Because CCB is built on building local capacities and external actors play a secondary role, this also ensures that interventions are within the realm of the possible. Essentially, capacity assessments and needs analyses also reduce duplication by shaping a suitable goal and strategy for intervention, hence determining what mechanisms, institutions and capacities exist, and what is necessary to create or reinforce those capacities. As such, rather than an analysis of a static moment in time, assessments provide a foundation and roadmap for follow-up action, thus enabling CCB actors to better determine their priorities.

Following assessments, adopting appropriate monitoring and evaluation is key not only to ensure performance management for a specific project, but also to allow future interventions to build on the positive and negative lessons learnt by other actions. Indicators should be clear, significative for the progress to be measured and comparable for external donors and implementors. In addition, performance and results monitoring should take place throughout the intervention. Consistently with a cyclic view of project management, the evaluation phase represents both the last stage of the Project and Programme Management Cycle and part of stage one, i.e. problem and context analysis, of a future action. As a matter of fact, the lack of publicly available projects' evaluations and end-of-project assessments, but also of reports describing the activities carried out, constitutes a significant hurdle. In this

42 Ibid.

43 Based on interview data.

44 K. Schulz, I. Gustafsson, & E. Illes (2005), "Manual for Capacity Development", SIDA, Stockholm.

respect, the monitoring, reporting and transparency efforts by the Council of Europe are a remarkable exception.

Incentives of coordination	most relevant in:	with national stakeholders	among donors
Increase situational awareness	Stakeholders mapping Policy analysis Capacity assessment	✓	✓
Avoid duplication	Stakeholders mapping Policy analysis Capacity assessment Formulation of logic of intervention	✓	✓
Allow coherence of actions	Formulation of logic of intervention	✓	✓
Share external risks	All		✓
Avoid forum shopping	Stakeholders mapping Analysis of the policy context		✓
Build sustainable actions	All	✓	✓
Ensure feasibility	Capacity assessment Formulation of logic of intervention	✓	✓
Ensure clarity and usability of lessons learnt	Monitoring and evaluation		✓

LOOKING AHEAD

Despite the concerted efforts of a number of donors and implementers, and notable strides in cooperation and capacity building, a great deal of work remains. Rather than a duplication of efforts, we observe that the persistent challenges of human capacity, political will, and resource scarcity remain some of the largest hurdles for states in the Western Balkans. As threats and emerging technologies grow more complex, countries in the Western Balkans will need to develop a holistic understanding on the intersections between cybersecurity and digital issues. On everything from 5G and supply chain security to platforms and artificial intelligence, the challenge will be to meaningfully engage with these issues without succumbing to hype, while managing limited resources and maintaining political stability. The longer this takes, the more challenging it will become. Regionally, this will require overcoming barriers to political cooperation, grappling with a lack of homogeneity in ICT maturity and public administration, and the differing political relationships and stages of EU ascension observed across countries in the Western Balkans.

Currently, coordination mechanisms and information-sharing on technical matters have been strongest, and yielded noticeable results in Cybercrime and CIRT cooperation[45], Yet the success of technical cooperation and interventions can be isolated from political impact, with bottom-up implementation strategies and knowledge communities that do not trickle-up to political levels. As cyber maturity increases in the region, there is a need and desire for Capacity building in the Western Balkans to continue moving away from focusing solely on technical capabilities and awareness-raising, to interventions that aim to build institutions, policy, and sustainable cybersecurity mechanisms with meaningful political influence. Such outcomes require not only the holistic visions of donors and implementers, but also top-down leadership at the national level. Best practices among donors and a project lifecycle anchored in coordination-by-design can yield meaningful impact and improve uptake by building a community of intervention whose benefits span well beyond the duration of a single project. Furthermore, as some of the interviewees mentioned, the long-standing presence of some international organisations in a specific country – as well as their involvement throughout the region – can provide means and venues for assisting new CCB actors, notably by building and nurturing personal relationships, sharing situational awareness and mentoring.

With specific reference to coordination, governmental stakeholders play an essential role, in determining and communicating capacities or needs, as well as by providing the political buy-in required for meaningful results. However, a whole-of-society approach to cyber capacity building and to cybersecurity governance is indispensable to ensure legitimacy, ownership and sustainable outcomes that are compliant with the donors' values in the region. Future CCB interventions in the region can foster the multi-stakeholder components of cybersecurity governance in the Western Balkans. This can be done at different stages. First, a multi-stakeholder approach should play a key role in the stakeholder and policy analysis, and should aim at improving awareness about the actors, the interplay between governments and non-governmental entities, as well as the possible objects of contention between the two. Secondly, CCB actions can promote and support multi-stakeholderism as an approach within the national modes of governance, therefore amplifying the voices of non-governmental organisations in the region. This, in general, allows for more legitimacy for the adopted policies, for increased public scrutiny and increased ownership, while at the same time improving linkages between policy areas and cross-cutting issues (e.g., gender equality, respect for human rights online, accountability, etc.). Engaging with civil society and private actors also ensure that local expertise is being mobilised in the region, facilitating long term impact and the sustainability of interventions.

While coordination can go to great lengths to build cyber capacities in the region, it is important for international donors and implementers to acknowledge that there is no one-size-fits-all approach. As for every region, within the Western Balkans differences in levels of ICT development, socio-political culture and institutional arrangements call for a tailored approach to cyber capacity building, drawing on local capacity and ultimately aiming to create home-grown expertise.

Ultimately, improving donor coordination in the Western Balkans will also benefit from an acknowledgement of both the political source, and the potential political implications of cyber capacity building. For the donor community, this means strengthening the link between policy objectives and strategies for capacity building interventions. Strengthening those links will better illuminate the role of different CCB actors, help identify opportunities for strategic partnerships, and clarify donor-recipient relationships. Whether this involves conditionality or not will be a strategic decision and based on a donor's mandate and policy objectives.

---

45 Based on interview data and CMM assessments of Albania, Montenegro, Bosnia and Herzegovina, Kosovo* and Serbia.

Acknowledging the political implications of cyber capacity building means placing interventions within the big picture of opportunities and consequences in cybersecurity and digital development. A strategic framing that also targets the political level can clarify what is at stake and contribute to building the political will necessary for improved coordination and sustainable impact. As the involvement of international partners in the Western Balkans increases, discussions arise around the responsibilities of states as they progress in their cyber maturity. In addition to building resilience internally, capacity building should highlight the necessity for states in the region to meaningfully engage in international debates that determine the future of cyberspace. There exist multiple venues for global action around the issue of security in the use of ICTs, such as the Open-ended Working Group or the UN Group of Governmental Experts. More recently, the establishment of an Open-ended Ad Hoc Intergovernmental Committee of Experts[46] to elaborate an international convention against cybercrime and the proposal for a Programme of Action[47] (PoA) for advancing responsible state behaviour in cyberspace opened new perspectives for further engagement, particularly for those states that were not part of previous UN GGEs. When it comes to cybercrime, it will be crucial for all states – including the Western Balkans countries – to ensure that the negotiations are consistent with current international frameworks and with the related reforms already undertaken by governments around the world and in the region. This is all the more important given that the international frameworks that will be discussed are likely to impact on how capacity building is conceived of and how it is carried out. Along the same lines, the proposal for a PoA explicitly mentions the necessity to step up cooperation and capacity building. As a long-term goal of building cyber capacity, facilitating an atmosphere of international cooperation, exchange and responsible behaviour will depend upon the engagement and contributions of not only donors, but all partners involved in building capacities.

46 UN General Assembly Resolution 74/247 'Countering the use of information and communications technologies for criminal purposes', 27 December 2019. Available at: https://undocs.org/en/A/RES/74/247

47 'Programme of Action (PoA) for advancing responsible state behaviour in cyberspace', 10 August 2020. Available at : https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

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