DCAF Geneva Centre for Security Sector Governance

DCAF's CSIRT Capacity Building Methodology – Lessons learned from the Western Balkans

Milan Sekuloski

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

Computer emergency response teams (CSIRTs) are fundamentally important parts of any national cybersecurity governance framework. This report aims to support the international efforts for effective CSIRT capacity-building. The first part of the report captures some of the main features of CSIRT capacity building and provides an overview of some of the most well-known CSIRT capacity-building methodologies and approaches. The second part offers insight into DCAF's experience from engagement with CSIRT capacity building in the Western Balkans, extrapolating key lessons learned from its own approach, and offering it as 'DCAF's CSIRT capacity methodology'. This paper and proposed methodology aim at supplementing the existing approaches and methodologies, and by presenting some of the cases it draws from, offers additional material to the international body of knowledge in cybersecurity capacity building.

BACKGROUND

In July of 2018, The Geneva Centre for Security Sector Governance (DCAF) began the three-year project "Enhancing Cybersecurity Governance in the Western Balkans", which ran until March of 2021. The Project was funded by the UK Government Foreign Commonwealth and Development Office (FCDO), and aimed to contribute to more effective and accountable cybersecurity governance in the Western Balkans, as well as to increase regional cooperation on cybersecurity. One of project aims was to support Montenegrin and Serbian national and governmental CSIRT[1]s in improving their performance in detecting and preventing attacks on national systems by providing them with assessments of their mandate, internal structure and human resources needs. This work built on successful support provided to the Serbian Ministry of Interior's CSIRT (MUP CERT) - the first governmental CSIRT team in Serbia - in 2016 and 2017. By the end of 2020, the DCAF team has carried out five such assessments (in addition to MUP CERT, the Serbian national CSIRT (SRB CERT), including the Office for IT and E-government of the Republic of Serbia, the Montenegrin national CSIRT (CIRT.ME), and of the national CSIRT of North Macedonia (MKD-CIRT). In addition, similar methodology is being applied to an assessment of local administrative entity capacity for critical information infrastructure protection in Albania, in cooperation with the national CSIRT of Albania (AKCESK).

Many lessons have been learned from these assessments, and a methodology has emerged through these assessment reports. The purpose of this document is to capture that methodology and offer it to the wider cybersecurity community.

TARGET AUDIENCE AND OBJECTIVE

This document aims to support further cybersecurity capacity-building activities in the Western Balkan region, as well as to inform practitioners, researchers and the donor community interested in CSIRT capacity building. The following document will provide an overview of some of the main CSIRT capacity-building approaches (methodologies), and highlight the specific features of DCAF's approach, i.e. DCAF's assessment and capacity-building methodology for CSIRT development. More specifically, this paper will aim to do the following:

- Provide an overview of existing national and governmental CSIRT capacity development methodologies
- Define key advantages and disadvantages of methodologies identified above in the context of Western Balkans' national and governmental CSIRTs
- Provide a description of the methodology DCAF has applied in CSIRT capacity development assessments in the region during the period of 2016-2020
- Define key strengths and weaknesses of DCAF's approach
- Provide recommendations for future improvements of methodology and CSIRT capacity building in the region

[1] CSIRT stands for Computer Security Incident Response Team. Commonly used names for such teams are also CERT (Computer Emergency Response Team, copyrighted by Carnegie Mellon University) and CIRT (Computer Incident Response Team). In this text, CSIRT will be used consistently, but all acronyms are valid and used interchangeably across the region and in the literature.

These aims will be achieved using desk research, the experience of the DCAF team and experts involved in developing the previous CSIRT assessment reports, as well as the CSIRT teams themselves.

EXISTING CSIRT DEVELOPMENT METHODOLOGIES AND APPROACHES

Defining the targets: what is capacity development for a national CSIRT?

The United Nations[2] defines the key distinction of "capacity building" as supporting change process: "transformation that is generated and sustained over time from within; transformation of this kind goes beyond performing tasks to changing mindsets and attitudes". With this in mind, we should consider how the Norwegian Institute of International Affairs (NUPI) report from 2015 categorizes donor supports efforts for cybersecurity capacity building[3]:

1. Methodological support: "general concepts used for building local capacities, as well as basic research into how cyber capacity building works", i.e. advising on best approaches that are to bring about the desired capacity change;
2. Technical support: which they define foremost as training around the CERT/CSIRT structures, but also as help provided at law-enforcement level and "support for community-based instruments"; i.e. support to make the actual capacity change, not just by training but also by stakeholder management/community building;
3. Infrastructural support: supporting the change through infrastructure building projects;
4. Budgetary support: financial assistance, be it direct to beneficiary, through international organizations, or civil society.

When it comes to CERT/CSIRT capacity building, the abovementioned NUPI report highlights the evolution and complexities of understanding the role of CSIRT in national cybersecurity governance (citing OSCE and FIRST efforts towards defining them), while underlining the importance of national CSIRTs. The report concludes that "the only key component that all 'national' CERTs must have is the ability to serve as an authorized point of contact for technical issues – for major incidents, but much more likely for the day-to-day fight against cybercrime."[4] So although often seen as purely or predominantly a technical body, the technical capabilities of one national CSIRT are not the common denominator of national CSIRT: rather, it is its role as an international cybersecurity incident information exchange contact point (and consequently, as key national information exchange point). Even in cases when this may not be so clearly defined in the national normative documents, the very fact that international partners (most notably, but not limited to other national CSIRTs) will by default reach out to a national CSIRT (or a CSIRT acting as national CSIRT) puts these CSIRTs in the centre of national information exchange. Acknowledging this fact had a major impact on how DCAF approached CSIRT capacity-building efforts.

2 https://www.un.org/en/academic-impact/capacity-building , accessed 2 October 2020
3 https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf accessed 7 December 2020
4 https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf accessed 7 December 2020

Carnegie Mellon University's Software Engineering Institute (SEI) offers elaborate tools for assessing the incident management capabilities of a CSIRT[5]. Furthermore, SEI offers resources on advancing the technical cybersecurity capabilities of CERTs/CSIRTs using the elaborate CERT Resilience Management Model[6], offering operational metrics[7], and even advancing capability measurement by using the SEI-developed maturity indicator scale[8]. The SEI approach refers to three types of CSIRT maturity models[9] that can be used to map or track capacity building:

- Progression models: focusing on capturing the progression of key characteristics, indicators, attributes or patterns
- Capability maturity models (CMM): measuring capabilities, defined as "more than the ability to perform a task", adding the broader organizational capabilities that "reflect the maturity of the culture and the degree to which the capabilities are embedded (or institutionalized) in the culture"
- Hybrid models, measuring both maturity attributes and their evolution or progression. Consequently, SEI's guidance on best practice for national CSIRT capacity building[10] calls for a much wider approach, the one encompassing many external, non-technical factors and issues (which will be elaborated on more later in the text).

The NUPI report[11] also speaks of 'community-based instruments' as part of CSIRT's capacity building. It refers to the idea of one CSIRT's functions being augmented by the capacities of external actors (for example, other CSIRT teams, national or international, individually or through various organizations; law enforcement agencies; private companies or even civil society). However, the report focuses mostly on the area of 'threat intelligence', i.e. the exchange of technical information about existing and potential threats to cybersecurity of CSIRT's constituency. Repositories and platforms for sharing such information may be public, closed or commercial, but in "all cases they can be shared by multiple cyber security responders in a largely apolitical way (some may require 'some form of vetting of the recipient' of the feed, or a subscription fee)"[12]. The increase of (national and international) community information exchange, facilitated by a national CSIRT, would consequently be observed as that CSIRT's increased capacity, by all communities, regardless of that CSIRT's actual technical capacity to process/analyse the information it helps circulate.

In May 2020, the Global Forum on Cyber Expertise (GFCE) published a report titled "Lessons Learned: Cyber Incident Management Capacity Building"[13], which summarized key observations made by an international community of experts gathered under their auspices. This paper suggests that the CSIRT capacity-building efforts/project can be categorized based on their intended outcomes, which may be understanding the "current maturity of the CSIRT environment", upgrading the "CSIRT environment in capacity or

5 For example, "Incident Management Capability Metrics Version 0.1", available at https://apps.dtic.mil/sti/pdfs/ADA468688.pdf accessed 7 December 2020

6 2016_002_001_514462.pdf (cmu.edu) accessed 7 December 2020

7 https://apps.dtic.mil/sti/pdfs/ADA468688.pdf accessed 7 December 2020 accessed 7 December 2020

8 https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_69194.pdf

9 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187

10 https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15401.pdf accessed 8 December 2020

11 https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf accessed 7 December 2020

12 https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf accessed 7 December 2020

13 https://cybilportal.org/wp-content/uploads/2020/05/GFCE-Working-Group-B-Task-Force-CIM-Lessons-learned-in-Cyber-Incident-Management-Capacity-Building.pdf accessed 7 December 2020

capability", or building "relationships between the national CSIRT environment and partners". It also describes the key factors of successful CSIRT capacity-building projects:

The following factors were identified as contributing to the success of a capacity-building programme:

- Providing continuous support, rather than ad-hoc interventions
- Comprehensive understanding of wider cybersecurity context and stakeholders
- Fostering regional partnerships and regional approaches
- Remaining politically, technologically, and commercially neutral
- Thorough stakeholders' and their drivers' mapping
- Multi-stakeholder approach
- Coordination among various interventions
- Creating hands-on learning opportunities for beneficiaries

All of the listed resources suggest that building national CSIRT capacities goes well beyond providing additional technical resources or knowledge to these units. Rather, it could be considered as continuous support for CSIRT's change process, which should result in both its increased technical capabilities and its increased interaction with various national and international communities working on the prevention, detection and response to cybersecurity incidents.

Existing CSIRT capacity development approaches

The following section will describe some of the most established CSIRT capacity-building methodologies.

The first widely used CSIRT handbook was published in 1998 and revised in 2003: SEI's "Handbook for Computer Security Incident Response Teams (CSIRTs)"[14]. It was meant to be a comprehensive guide to those in charge of setting up and running different CSIRTs, and is still considered as a very valuable tool by many in the CSIRT/incident response community. The handbook calls for CSIRT projects to start by defining a core mandate, constituents and stakeholder relations; then based on those, define core services it will provide, governing operational principles, and services quality control. The handbook is indeed very comprehensive. However, though it acknowledges possible variations in CSIRT mandates and modalities, it puts technical incident handling capability in the centre of CSIRT capacity development. For example, links to national security governance structures are not sufficiently elaborated. Namely, these links were not as elaborate at the time of this Handbook's creation and revision. However, in the past several years these links are (globally) becoming increasingly important. And with the increased importance of cyber domain for national development, national cybersecurity authorities (and consequently the CSIRTs) are becoming more closely linked to traditional security and defence institutions.

The National Institute of Standards and Technology (NIST) from the United States offers its own recommendations for CSIRT development in its 'Computer Security Incident Handling Guide'[15]. First published in 2004 and revised in 2012, it is a US-centred guide,

14 https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf accessed 9 December 2020

15 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf accessed 14 December

but nonetheless, it offers some general guidelines for building an effective incident response programme. However, as stated in the guide, "the primary focus of the document is detecting, analysing, prioritizing, and handling incidents", i.e., the technical aspects of incident handling function of a CSIRT, not its establishment, defines its role in wider cybersecurity and security governance, and its role in the international and national cybersecurity communities.

In contrast, SEI's publication "Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0"[16] offers a very valuable framework for establishing a national CSIRT and thus supporting a national cybersecurity strategy and governance. It starts by elaborating on the importance of a strategic approach to national cybersecurity, calling for proper stakeholder identification and recognition of the role and importance of national CSIRT programmes. Further, it proposes four strategic goals that lead to establishing national cybersecurity incident response capability. For each of the goals, they define a number of 'enabling goals' or activities supporting the effective attainment of strategic goals. The strategic goals as defined in this document consist of planning and establishment of the national CSIRT, establishment of a shared situational awareness, management of cyber incidents, and support for the implementation of a national cybersecurity strategy.

The key challenge in applying this guidance in the Western Balkans is related to the implementation of public policy strategies, as they are rarely implemented as per best practice of strategic management. This is one of the conclusions of ITU's workshop on designing and implementing national cybersecurity strategies held in Skopje in 2019 for the representatives of national cybersecurity institutions from the Western Balkans[17].

The global Forum of Incident Responders and Security Teams (FIRST) is offering another source of advice and guidance for the CSIRT establishment. Namely, this organization has produced and published a CSIRT Services Framework[18]. FIRST built the list of CSIRT services, acknowledging that not all CSIRT teams will provide all of the listed services. However, FIRST's logic is that listing them should help the CSIRTs in 'choosing their services portfolio'. Similar services are grouped within service areas and each service is broken down to functions which are described with their purposes and outcomes.

The United Nation's International Telecommunication Union (ITU) offers national CSIRT establishment support to its member states[19]. Most notably, it provides National Computer Incident Response Teams (CIRT) assessments. The purpose of these assessments is to "define the readiness to implement a national CIRT". The most recent publicly available assessment (published in 2019) focuses on Albania and is in essence adapting the FIRST CSIRT Services Framework to Albanian national context[20]. This case demonstrates the usability of FIRST's services framework in the Western Balkans context. The weakness of this model might be that it depends heavily on the country's overall public administra-

---

2020

16 https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15401.pdf accessed 14 December 2020

17 https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/NCS_Outcome_Report.pdf accessed 14 December 2020

18 https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v1.1.pdf accessed 14 December 2020

19 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx accessed 14 December 2020

20 https://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjU7ZSm8-3tAhXJBRAIHajcC_MQFjAAegQIAhAC&url=https%3A%2F%2Fwww.itu.int%2Fmyitu%2F-%2Fmedia%2FPublications%2F2020-Publications%2FCIRT-in-Albania-2019.pdf&usg=AOvVaw2Y55VGFQ13yAmTq-ad_RYW accessed 28 December 2020

tion reform and prioritization of cybersecurity governance in the process. If insufficient resources and authority are not provisioned to the CSIRT by national government, they might find it difficult to implement the ambitious ITU's recommendations. This is particularly important in the context of Western Balkan , where most governments still struggle to achieve public administration performance levels of most developed countries (i.e. EU member states).

One of the most widely used models for CSIRT development is the Security Incident Management Maturity Model (SIM 3)[21]. This model is used by over 100 European CSIRTs and has been adopted by TF-CSIRT and their Trusted Introducer (TI) trust model in 2010, as well as used for CSIRT team capability certification[22]. The logic of the model is relatively simple, but its main strength is that it is conceived, developed and maintained by dedicated and experienced CSIRT and incident response professionals worldwide. SIM 3 model provides a framework for CSIRT maturity assessment based on over forty parameters, grouped in one of the four 'quadrants' (O – Organization, H – Human, T – Tools, P – Processes). The parameters are measured based on clearly a defined set of levels ranging from 0 to 4, with level 0 meaning that assessed CSIRT is not even aware of the importance of that parameter for incident response, while level 4 indicates the specific parameter is identified as important by the team, and formalized as a written rule in some way and vetted by an external authority. Results of measurement, through self-assessment or assessment, can easily be presented in several formats suggested by the methodology authors, depending on the intended use of the results, for team improvement, communication with other teams, management, or constituents.

The European Union's Network and Information Security Agency (ENISA) builds its own Maturity Evaluation Methodology[23] for CSIRTs based on the SIM 3 model, coupling it with its earlier reports (such as "Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity"[24]), EU NIS Directive, and GFCE recommendations. Instead of the five-level maturity scale, ENISA suggests using the "three-tier approach towards maturity", proposed in earlier ENISA's report "CERT community - Recognition mechanisms and schemes". In practice, this means ENISA's methodology is assessing SIM 3 parameters maturity only as either basic, intermediate or advanced. What is also specific to ENISA's approach is that it suggests using this methodology to define CSIRT's "growth path. They suggested that CSIRT can reach "the basic step within one year, intermediate two years later, and advanced another two years later for a total of five years maximum…". While ENISA says the basic step would already allow a minimum of successful cooperation between teams on incident handling, it still suggests higher steps are considered as they would facilitate much more capability of the entire CSIRT community (of the EU). In any case, EU CSIRTs are advised to start the process by conducting a self-assessment (using the modified SIM 3 with ENISA's scale), but then to also in engage in a peer-review process with other EU CSIRTs. The main purpose of this peer-review is to facilitate increased trust building with the EU CSIRTs in addition to offering the external verification of CSIRT's maturity - similar to the accreditation and certification processes already offered by the TF CSIRT-Trusted Introducer.

21 http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf accessed 14 December 2020

22 https://www.trusted-introducer.org/processes/certification.html accessed 14 Dec. 20

23 https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process accessed 15 December 2020

24 https://op.europa.eu/en/publication-detail/-/publication/eb2686fe-7663-11e7-b2f2-01aa75ed71a1 accessed 15 December 2020

Observed commonalities and trends

While most of the CSIRT capacity building approaches described above focus on measuring and developing teams operational capabilities for detecting and responding to incidents, it is observable, most notably in the more recent models (such as ENISA) that CSIRT capacity may and should be built through what the NUPI report calls "community-based instruments". This becomes even more relevant for national and governmental CSIRTs, for two key reasons:

- They usually have a wide and diverse base of constituents which may or may not depend on the national/governmental CSIRT for security incident detection and response (these services may be performed by constituents themselves, equipment vendors, consultants or similar), but they all depend on the central CSIRT for wider situational awareness and external communications (with other stakeholders in and out of the country).
- National (and in some cases governmental) CSIRTs are the main cybersecurity threat and incident communication hubs for all stakeholders outside of a given country. As rarely any cyber-attack targets and affects only one country, provision of this service becomes even more important for their constituents. Although, in principle, governmental or specific ministry of sectoral CSIRT should rely on national CSIRTs to perform this task, exceptions resulting from specific mandates (e.g. national defence) or technologies (e.g. specific industry controllers) may require governmental and sectoral CSIRTs to act as national information exchange contact points on occasions and complement or even substitute the role of national CSIRTs in those cases.

In conclusion, although ENISA focused its advice for CSIRT capacity building primarily on the EU CSIRT community, their approach in considering not only the technical, but involving more and more community-based approaches, seems like the best recipe for any CSIRT aspiring to become and remain effective in an increasingly interconnected world. In addition, the simplicity and adaptability of the SIM 3 model makes it the most likely baseline methodology for CSIRT capacity assessments in years to come. More elaborate technical capacity assessment and development models, like the ones developed by SEI and FIRST, will remain relevant as well, most likely focusing on specific aspects of security incident management or specific technologies (most notably the 'disruptive' technologies such as 5G, AI, quantum computing and the like).

DCAF's EXPERIENCE FROM CSIRT CAPACITY BUILDING IN THE WESTERN BALKANS

DCAF's engagement in the field of cybersecurity comes from the angle of security sector governance reforms, i.e., from the considerations related to democratic governance in the public sector, most notably related to security policies. Hence, building capacities of CSIRTs was not DCAF's goal in itself, but rather means to enhance good governance in the security institutions.

Consequently, DCAF did not a priori think of a specific technical capacity building methodology or approach when supporting CSIRT development. Rather, a wider context of socio-political circumstances and public administration reforms was both the starting point for intervention and field where success will be measured.

This proved to be a serious advantage compared to organizations focusing on CSIRT technical capacity building as their sole source of observation and action. However, over time and with growing number of interventions, DCAF has been able to formulate its own lessons learned and advice on some aspects of CSIRT capacity building methodology.

In spite of all said above, DCAF's approach acknowledges CSIRT and its capacity to deliver envisioned services as a pivotal element of national cybersecurity governance enhancement. However, for DCAF, the end state of CSIRT maturity was not as important as was setting in motion the process of capacity development in a way it is recognized by other cybersecurity governance stakeholders.

DCAF's CSIRT capacity development methodology

This report builds on DCAF's engagement with CSIRT capacity building in the Western Balkans in the period 2016-2020. In that period, DCAF supported capacity development of five teams (working with more at the time of writing, but not involved in this paper as they are still works in progress). The following chapter will describe these experiences, offering five case studies, with very diverse teams and different mandates, operating in different circumstances, but in the same historical and political moment in the Western Balkans. In that period, all of them made some progress, to varying degrees, in developing their capacities. DCAF has observed this capacity increase thanks to objectively verifiable indicators: admission or progression of these teams in the international CSIRT organizations through peer-reviewed processes (most notably in TF CSIRT's TI and FIRST; and through collecting anecdotal evidence of increased operational capacities of certain teams from their international and/or national interlocutors and partners (e.g. other CSIRT teams with whom they engaged in incident response). Certainly, this capacity increase is first and foremost to be attributed to the work and ambition of teams themselves, and as many of them confirmed, DCAF's support contributed as well. Hence, the purpose of the following chapter is to offer insight in DCAF's modus operandi and offer advice on applied system of practices, techniques, procedures that contributed to DCAF's CSIRT Capacity Building Methodology.

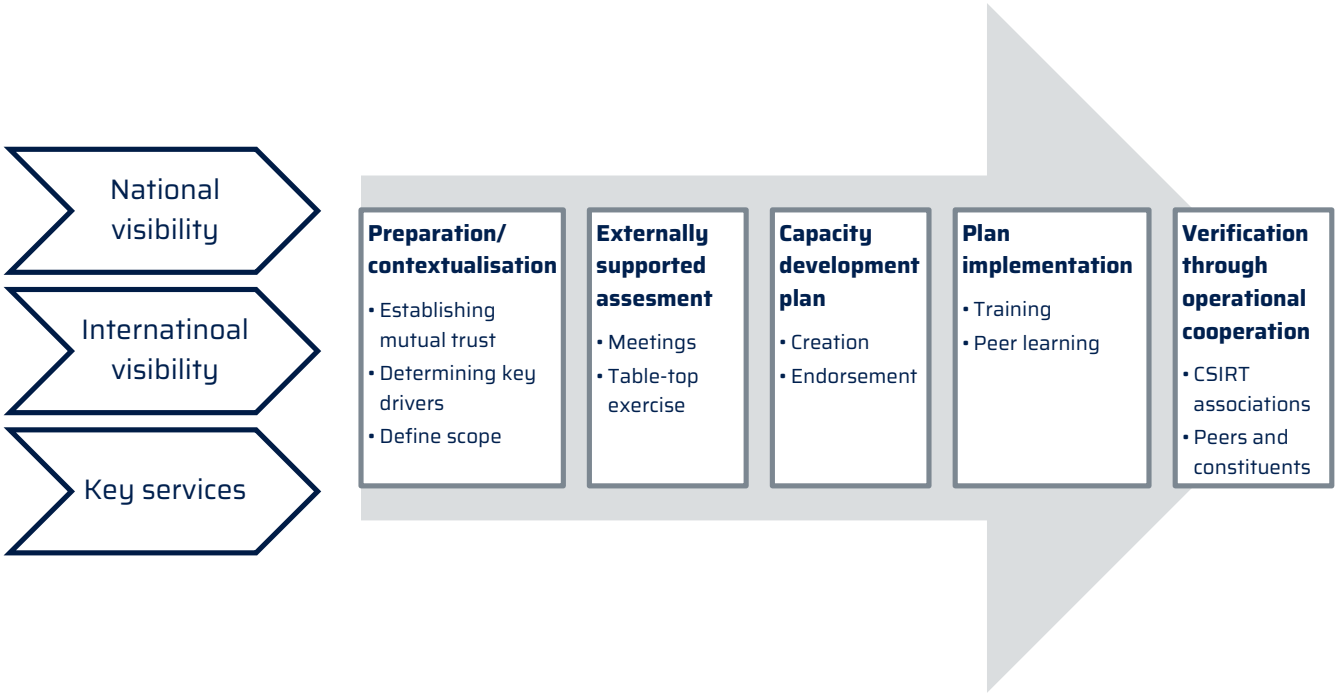
The three key parameters of CSIRT's increased capacity are the main focus in DCAF's approach:

1. CSIRT becomes more visible mong its constituents and national cybersecurity community/stakeholders
2. CSIRT becomes visible internationally (this is particularly valid for national CSIRTs and countries of the immediate region)

3. CSIRT starts providing or improves at least some of the key services for its constituents

DCAF supported CSIRT's in achieving these indicators by going through the following five stages:

1. Preparation/contextualisation
2. Externally supported assessment
3. Capacity development plan creation and endorsement
4. Plan implementation
5. Verification through operational cooperation



The first stage provides the basis for capacity building, as it seeks to identify the root problems and key drivers that may contribute to these problems being adequately addressed. This approach somewhat resembles the approach described by SEI in the best practice paper[25]. However, it relies more on acknowledging the CSIRT's policy environment status than attempting to change it (i.e. supporting bottom-up approach for desired systemic changes). Besides analysing the available legal and policy documents, capacity building support organization (in this case, DCAF) will devise strategies for gaining trust of beneficiary CSIRT. This trust is necessary to be able to establish an open and honest communication necessary for proper determination of the key internal and external capacity development drivers, factors that will shape CSIRT development approach and scope. And lastly, the support organization (DCAF) will make sure the scope of its assistance is well understood. The more capacity development processes will be in beneficiary's hands, the greater likelihood of sustainability – along with a greater risk of capacity development failure, as it is out of support organisation's (DCAF's) control. Most often, a capacity-building project support team would be faced with limited capacity de-

[25] https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15401.pdf accessed 14 December 2020

velopment assistance resources and would have to prioritize crucial CSIRT service(s) or capacity development areas.

The second stage is the externally supported assessment. Selection of external experts is a crucial success factor, as it should reflect the understanding of key capacity-building drivers and further project trustworthiness to the beneficiary. The key added value of DCAF in this stage was the ability to communicate well the context and expectations of beneficiaries to the experts, as well as experts' knowledge and abilities to the beneficiary. The assessment will have the form of meetings with beneficiary and external stakeholders (beneficiary's constituents and partners). In an ideal scenario, a table-top exercise will be conducted.

The third stage is the capacity development plan creation and endorsement by the beneficiary. This is a very delicate process, as it has to ensure a beneficiary's acceptance of described capacity deficiencies and proposed strategies for their overcoming. If trust is established and maintained through previous stages, obtaining an endorsement from the CSIRT should not be a problem. However, getting the right message to higher decision-making echelons may often be difficult due to simple human resistance to any proposed change, if for no other possible reasons.

The fourth stage is capacity building plan implementation. Two main avenues for increasing CSIRT capacity, as per intended plans and priorities, is through training and peer learning. Ideally, training plans would be owned by the CSIRT, which would decide on the pace and sequence of training implementation, so it best suits their absorption capacities. A team's willingness to dedicate their own time and resources to capacity building is a strong indicator of ownership. Peer learning, be it with colleagues from the country or region, is also a very effective way of increasing skills and knowledge - with a precondition being that a high level of trust exists among the peers. Although peer learning has its limitation, most notably due to different levels of knowledge and capability and different mandates, it also contributes towards 'community based' capacity building. Peer learning initiatives help build up trust networks among different stakeholders, which may complement one another's capabilities in cybersecurity incident prevention, detection, and response.

The final stage is the verification of CSIRT's increased capacity through increased operational cooperation. Once constituents, national or international peers confirm they have noticed a more active role of the CSIRT, it may be considered that the capacity building processes have successfully been initiated. When it comes to international partners' acknowledgement, a very reliable indicator may be the position of CSIRT in international organizations (TF CSIRT-TI accreditation, FIRST membership), as well as their reputation among constituents.

Unfortunately, increasing CSIRT capacity in any modern society is not an end-state, but rather a process which can go in both positive and negative directions. As long as the direction moves along the lines of any of the three key success indicators described above, it can be considered CSIRT capacity development according to DCAF's experience from the Western Balkans.

Case studies- DCAF's work on CSIRT capacity building in the Western Balkans

Case no.1

The first case relates to a governmental CSIRT, in charge of some of the most critical governmental systems and networks. The CSIRT was developed in the context of non-existing national legislation or strategy (both were adopted after DCAF's support intervention

started). The key driver for CSIRT establishment and development was a beneficiary's ICT professionals' understanding of the importance of information security and incident response capability for ICT systems development. Namely, in this case the key change advocates were the technical experts entrusted by senior management to implement a segment of wider ICT development strategy.

Thanks to its previous engagements with beneficiary institutions, DCAF had a general trust relation and was invited to provide support. Nonetheless, additional efforts had to be made by DCAF to ensure the technical experts' trust. This was achieved through careful selection of external technical consultants DCAF engaged. Their technical and change management experience, combined with DCAF's ability to thoroughly understand beneficiary's needs and organizational culture and specificities, were key enablers in the project design and implementation processes.

The capacity building process started with an assessment. A pre-agreed approach of separating human resources (HR, people capacities and organizational capabilities) from technical aspects (hardware and software needs) was applied. Establishing a trust environment with DCAF ensured that the beneficiary understood that honest assessments best serve their interests. This was not default thinking in the specific organizational culture in which the project took place, but it was a fundamental success factor. Exceptional leadership capabilities of a beneficiary's key management were instrumental in this stage. Most important of all was their readiness to take responsibility for 'leap of faith' assessment results that may have portrayed a grim situation, but with the understanding that this is the only way to get realistic, implementable and sustainable development advice from it. As it will be witnessed in many projects after this one, CSIRT leadership and personnel morale were crucial elements of success.

The HR assessment itself was implemented through a series of internal and external meetings, including a table-top exercise for immediate partners of the host institution. The tabletop was beneficiary facilitated, thanks to the fact that there was an overlap between the HR assessment and training phase (since the CSIRT was to be created from scratch, two team members were sent to a TRANSITS I course in parallel to assessment process).

The HR assessment was tailor-made by the experts, to reflect the key concerns and priorities of the beneficiary. It resembled the FIRST services framework to some extent but offered another layer of tailored advice related to team organization (existing vs. desired but realistic. It also had elements similar to those in the SIM 3 model, formatted in a 'heath map', identifying current maturity state of listed services, desired state as described by the beneficiary, and proposing which of them should be developed to what maturity level in 18 and 36 months. The 'heath map' was a basis for CSIRT's development plan, their internal document, which was developed with DCAF's facilitation of several "expert injects":

- First, CSIRT was advised by experts from some of the most developed European countries to encourage the acceptance of the need for continuous development even in the most resourceful environments.
- Second, advice was provided by an expert from a more advanced regional country with similar socio-political heritage to demonstrate that the 'interface' between legacy organizational cultures and legal systems with international best practice are possible.
- Finally, local expertise was employed to help the CSIRT identify what capacity-building opportunities exist locally that may suit the capacity development

plan. This element was fundamental for several reasons: cutting down expenses of needed training (presuming local training is cheaper than international); and building a base of local experts - CSIRT's national expert community - acquainting the CSIRT to local companies and experts with specific expertise they may need in operational work.

The HR assessment served as a basis for DCAF's training support to this beneficiary, but even more importantly-for the beneficiary's own training and staff development planning. Training plans were kept as live and open documents in terms of actual trainings but were focused on predefined staff capabilities that needed to be achieved-and maintained.

The technical assessment was implemented through an open and honest consultation process, and helped the beneficiary/CSIRT to better assess financial resources needed for CSIRT technical equipping. For example, the report proposed that the anticipated lack of finance for software provision may be compensated by the utilisation of free, open-source tools. Though not as comfortable and easy to implement as paid solutions, they offered learning and customization opportunities and helped to minimize risks of 'vendor locking'[26].

Although the actual plans were modified as circumstances changed, a structured approach to CSIRT development persisted with the beneficiary, offering clear and tangible results. Moreover, the fact that the plan was changed and adapted by the team itself exemplifies the high level of sustainability and ownership. The impact of the assessment reports was observed by DCAF over several years. The beneficiary managed to develop one of the most capable CSIRT teams in country and the region, actively contributing to national and international incident response, and supporting other national and regional teams' capacity development. In terms of outcomes DCAF aimed for, the implementation of these assessments and consequential CSIRT development plans was the security sector governance change desired: merit-based staff selection and progression, and efficient and accountable public administration.

Case no.2

The second case refers to a national CSIRT. The beneficiary CSIRT was formed a few months before the intervention, in a clear legal framework, but was struggling to start offering services to its constituents and to position itself in the national and international domains. DCAF's previous engagements with many of the key constituents of the CSIRT in this case enabled the necessary trust to be established quickly. In addition, DCAF decided to engage international experts familiar with the beneficiary and national context, with whom DCAF already worked in the beneficiary country. This was done in an effort to both enable easier trust building and minimize the need for providing contextual guidance to experts.

Having in mind that the mandate of this CSIRT, as prescribed by national legal and strategic documents in place, was more focused towards incident response stakeholder coordination and international communication, technical assessment as described in case no.1 was not requested from DCAF.

The initial capacity assessment took place soon after ENISA published its SIM 3-based CSIRT Maturity Self-Assessment Tool[27], and beneficiaries, experts and DCAF agreed the

[26] In this context, dependence from one software or hardware vendor for services delivery, i.e. a situation when migration to other solutions becomes more costly than the price difference in their favour.

[27] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturi-

capacity development plan provided would follow this model, i.e. that DCAF engaged experts would help the beneficiary CSIRT to conduct a guided self-assessment using the ENISA methodology.

The experts provided an overview of key competences prescribed by the legal framework (which was, in this case unlike some others, assessed as providing sound levels of mandate and constituency clarity), links of these competences to the appropriate ENISA/SIM 3 model maturity parameters, assessment of their current maturity, and recommendations for concrete actions that would enable the CSIRT to reach higher levels of maturity for those parameters. Given the support project's budgetary constraints, the experts were unable to provide a more detailed CSIRT staff training plan, whose development they strongly advocated. However, they did manage to provide advice for many easy-to-implement documenting activities. The purpose of these recommendations was to elaborate non-existing policies and practices, as well as to fortify and further elaborate those that existed but were not documented. In effect, development of this documentation enabled the beneficiary CSIRT to advance in the TF CSIRT community (and become an accredited team, advancing from a listed team), as well as to pass the criteria and become member of the FIRST CSIRT community. As mentioned earlier, both organizations assess the CSIRT maturity based on SIM 3 model, as does ENISA. And formal advancement in TF CSIRT and FIRST encouraged the beneficiary CSIRT to become more active in the international and regional CSIRT community. DCAF obtained anecdotal evidence that they successfully engaged in international incident response on several occasions since the assessment. Moreover, it was also observable that the increased confidence positively affected the CSIRT's attitude towards its constituents, making the CSIRT more active and more visible in the country as well. DCAF, along with some other actors working with the national cybersecurity governance reforms in that country, encouraged this development and cybersecurity governance practices relying and expecting an active role of the national CSIRT. Following the initial assessment and report production, DCAF provided some support for the CSIRT's personnel technical trainings, but always in the context of technical trainings for the whole community of governmental and national incident responders, in line with the principle of community-based capacity building described earlier.

Case no.3

In this case, the CSIRT supported by DCAF was a governmental CSIRT in development with a strong, legally defined, technical mandate to manage security incidents in governmental networks. Although the strategic importance of its security function for national security and good governance cannot be overstated, particularly in an environment in which governmental e-services become key governance tool (even more so after the COVID 19 pandemic), the perception of those in charge (by law) for establishing and running this CSIRT was to consider it as a primarily technical body. Admittedly, the technical capacities (ICT knowledge and equipment available) of staff designated for this CSIRT in development were probably among the highest DCAF has encountered while working in the region. This posed a new challenge to DCAF in terms of establishing trust: faced with such perceptions of CSIRT, one's perceived (not necessarily real) technical competence becomes the key parameter for establishing trust. A community-based capacity-building effort relying on the establishment of networks of trust among stakeholders with different competencies and role, which DCAF favoured in environments where this was possible, was hard to implement in this case.

ty-self-assessment-survey accessed 21 December 2020

Hence, a different approach was taken compared to other interventions. First, a team of experts selected to perform the capacity assessment and provide the capacity-building plan was comprised of an international seasoned technical expert, an academic expert with in-depth understanding of national legal framework, and a private sector technical expert. The connecting thread of these selected experts was their ICT expertise, which was to serve as a bridge between their diverse perspectives of CSIRT operation and the diverse communities that would rely on in its work.

The experts, in full cooperation with the beneficiary, conducted an initial desk review of legal documents and an assessment visit to the beneficiary, meeting with all key internal stakeholders (not just prospective incident responders and ICT security personnel). Following the assessment, DCAF and experts developed a five-step development plan for the CSIRT, first and foremost aimed at the positioning of CSIRT in the national governmental structure and beginning the provision of essential services to its constituency. The plan offered an analysis of the current legal status of the CSIRT and offered advice for its staffing, initial job descriptions, staff training, and retention. It also provided guidance for the second stage in which some of these services would become automatic, while others would be outsourced. All of the guidance and advice was tailored specifically to the beneficiary, taking into account the main concerns they expressed in the consultation process, as well as the main CSIRT development issues observed with similar CSIRTs by DCAF and external experts engaged for this task.

Unfortunately, the effects of DCAF's intervention were not as desired. At the time this paper was produced (December 2020), this CSIRT was not yet officially formed. Its creation is to be further assisted by a separate, much better resourced assistance project implemented by another organization (not by DCAF). Many factors contributed to this development. First, the resources made available to DCAF did not allow for a long-term investment solely in this CSIRT (DCAF's assistance project was designed around the idea of CSIRT community-based capacity building), i.e. it could not facilitate more one-on-one training and advising for the host institution and its key personnel. Second, the top management of the host institution did not see incident response and prevention as its key priority but was more focused on new e-government functions establishment and functionality. Fortunately, no major incidents affecting overall systems functionality occurred during DCAF's assistance period. And third, although overall well-staffed, the beneficiary institution was affected by staff fluctuation.

Case no.4

The fourth case study refers to a national CSIRT. The mandate and constituency of this CSIRT is well regulated by appropriate law and strategic documents. However, the scope of services envisioned to be provided by the CSIRT go far above the human and material resources made available to the CSIRT. As a result, the CSIRT provided very few of the services it was supposed to and was not well perceived among its constituents. The national cybersecurity governance structure in which the CSIRT operated was undergoing a transformation, resulting in uncertainties related to the prescribed national cybersecurity policy related function of the CSIRT. The CSIRT was not assessed as sufficiently active among both national and international stakeholders, but a national role was assessed by DCAF as stronger potential change driver.

Hence, a decision was made to focus on supporting the CSIRT's capacity to enhance one of its core national services, not easily replaceable by anyone from the national community - securing the governmental networks. This decision was made jointly by the CSIRT, external experts, and DCAF, and endorsed by the CSIRT's senior management. An external experts team selected for this task included one international and one local ex-

pert. The rationale for this decision was to ensure both the introduction of international best practice and to be able to contextualize CSIRT capacity-building advice to national legal, political, and organizational circumstances. Trust was ensured by engaging both the international and national experts with whom the beneficiary CSIRT already worked in the past, but also by the fact that DCAF already had longstanding good cooperation with the beneficiary and many of its most relevant stakeholders. As in other cases, an assessment visit and consultation took place, followed by the production of a detailed capacity building plan.

The capacity building report started with numbering the current challenges, highlighting those related to CSIRT's technical environment and personnel, and then offering practical ways of overcoming them. It offers very concrete advice on the technical environment for CSIRT (mostly optimization of existing ICT equipment usage) and human resources development, i.e., necessary job description revisions for the existing staff, necessary levels of technical knowledge, and trainings that could facilitate that. It also offers a detailed proposal for the timeline of technical and personnel improvement activities that would ensure increased CSIRT capacity in a 24-month timespan.

The capacity development plan was formally endorsed by CSIRT management, but never fully implemented, mostly due to ongoing national cybersecurity governance reforms and uncertainties around the exact place and role of a national CSIRT. However, DCAF tried to minimize the impact of such a situation on CSIRT capacity development through the capacity development plan implementation. Namely, DCAF provided some of the technical training envisioned by the plan, but in a way that involved all governmental stakeholders that would play a role in incident response involving critical governmental networks. Again, a community-based capacity-building approach was taken and has demonstrated potential to overcome structural challenges related to CSIRT development (uncertain mandate and constituency due to cybersecurity governance reforms). To what extent this will be a successful approach will need to be observed over time, after national governance structures are clarified and settled.

Case no.5

The last case that will be described here is related to a national CSIRT programme. The uniqueness of this team is that it was already a very active team at the moment it approached DCAF and requested assistance. However, the team had very scarce human resources (number of staff) and was operating in a changing policy and legal environment. Although the exact position and competences of the CSIRT in national cybersecurity governance structures may be subject to changes, its national and international visibility and established work practices make it very likely that CSIRT will play important national role in foreseeable future. In spite of its small staff numbers, it was a relatively well equipped and technically resourced team. Their biggest uncertainty, and the main reason for a support request to DCAF, was related to human capacity: future team size, composition and organization, and staff recruitment and retention. Hence, advising on these issues, in the context of planning the CSIRT's future capacity development, was the main request to DCAF.

The team of experts hired for this task consisted of one international and one local expert. The international expert was to provide advice related to best practices in comparable CSIRT operation, and the main tasks of national experts was to help seek innovative solutions to overcome identified HR challenges within the country's legal framework and organizational culture. The initial assessment involved various stakeholder interviews, but also drew from DCAF's previous engagements with the team and some of its constituents. Previous joint activities helped DCAF experts start their work in an environment

of trust. As with the CSIRT described in the first case study, management demonstrated superior leadership skills, remaining genuinely open to any kind of critical insights. This management attitude resulted in the creation of a report with very concrete and implementable suggestions aimed at overcoming critical challenges at a crucial moment in this CSIRT's development. However, it has to be noted that this capacity development report did not focus so much on the future delivery of the CSIRT's services, but rather at addressing what was assessed as a fundamental issue for the CSIRT's sustainability and development - human resources management. The impact of the report is yet to be observed. The beneficiary CSIRT has endorsed its recommendations, but it remains to be seen if they will be enacted in future national cybersecurity governance reforms.

CONCLUSIONS AND RECOMMENDATIONS

CSIRT capacity building will remain a crucial element of national cybersecurity governance development for the foreseeable future. Even as the cybersecurity rises higher on policy and political agendas, national and governmental CSIRTs continue to be central elements of both national and international governance structures. DCAF's experience from the Western Balkans in the period of 2015-2020 clearly demonstrates that these teams tend to play not just a technical, but very often decisive role in determining and implementing national policies, either by providing critical input for their development or through policy implementation. The role of CSIRTs in international cooperation is even more important: in the absence of clear and international cybersecurity regulation, the formal and informal international CSIRT networks become key elements for international incident response as well as international confidence building. This aspect of their significance is of particular importance in post-conflict regions such as Western Balkans.

This paper has described a number of well recognized CSIRT capacity-building methodologies and illustrated DCAF's experience in implementing some of them. It clearly shows that any capacity-building approach may give value to beneficiary CSIRT teams-if well contextualized. This is not unique to the Western Balkans, but rather it very much echoes the lessons learned, and recommendations offered by the GFCE community in 2020[28]. Drawing from those recommendations[29], DCAF proposes the following advice for future CSIRT capacity-building support to the Western Balkans:

Recommendation 1. CSIRT capacity-building efforts in the region should aim to be holistic in order to be trustworthy. This means they should focus on all three types of outcomes described by GFCE: understanding the "current maturity of the CSIRT environment"; upgrading the "CSIRT environment in capacity or capability"; and building "relationships between the national CSIRT environment and partner". These outcomes are logically connected, and engaging with either of them will raise expectations of beneficiaries that others will follow. These expectations are key motives for beneficiary cooperation, and consequently, the success of all CSIRT capacity-building efforts.

Recommendation 2. CSIRT capacity building should be coordinated based on CSIRT's capacity development plans. Having in mind that the holistic outcome approach described in recommendation 1 implies high complexity and high costs of project interventions, and donor coordination that facilitates this becomes of crucial importance. Ideally, the coordinating role should be owned by the beneficiaries themselves, as capacity development plans proposed by DCAF's methodology are an effort in this direction.

Recommendation 3. CSIRT capacity building should be supported continuously. Personnel and organizational changes and time-limited donor support are key challenges to this. Again, adherence to multi-year CSIRT capacity development plans proposed by DCAF may be a way forward.

---

28 DCAF was not part of GFCE at the time the recommendations were created, but can nonetheless reconfirm their validity

29 https://cybilportal.org/wp-content/uploads/2020/05/GFCE-Working-Group-B-Task-Force-CIM-Lessons-learned-in-Cyber-Incident-Management-Capacity-Building.pdf accessed 7 December 2020

Recommendation 4. Peer learning should be applied whenever possible, both at national, regional, and international levels. GFCE members highlighted the importance of the 'comprehensive understanding of wider cybersecurity context and stakeholders', as well as 'fostering regional partnerships and approaches'. DCAF's experience from the Western Balkans offers one possibility for this through national and regional peer learning: a capacity-building approach that includes the wider cybersecurity incident response community in CSIRT capacity building plan development (consultations, table-top exercise) and implementation (training). Involvement of regional and international peers encourages both more efficient capacity building as well as confidence building among stakeholders from different countries and regions.

Recommendation 5. Technical capacity building should be hands-on and technologically neutral. DCAF's approach in the Western Balkans demonstrated that providing practical training not linked to specific tools and technology providers, but rather widely accessible, open-source tools, provide an easier base for wider (national and regional) stakeholder engagement (peer learning), and help the beneficiaries mitigate 'vendor-locking' in the future. This doesn't mean specific support, linked to concrete technical solutions, should not be provided to certain teams, but just to acknowledge that although such support may lead to short-term capability increase, it may not be well suited for longer-term effective CSIRT capacity building.

Recommendation 6. Wider political and policy environments should be acknowledged in the CSIRT capacity-building efforts. While completely agreeing with GFCE's advice to make sure CSIRT capacity-building support remains politically neutral, DCAF's experience suggests that it cannot remain agnostic to political and policy developments. In a post-conflict region, such as the Western Balkans, political developments may significantly affect national and regional capacity-building efforts, even when their focus is purely technical. Hence, constant and in-depth observation of political risks and their mitigation remains a crucial success factor. According to DCAF's experience, looking for positive change drivers in linked policy processes (e.g. European integration, public administration reforms, security sector reforms) may make CSIRT capacity building more resilient to potential negative political developments. At the same time, remaining aware of the political environment may in some instances offer advantages: for example, efforts towards establishing common digital single markets, closer governmental relations ,and the like, may offer many new avenues for more efficient CSIRT capacity building through regional peer learning and exchanges. Strategically, DCAF acknowledges and builds on the fact that all Western Balkans economies declared EU membership as their strategic goals, meaning that they are all ultimately committed to working together and building joint institutions.

The following table offers an overview of these recommendations broken down by their targets, donors, WB governments/responsible governmental ministries and CSIRT teams:

	For donors	For WB governments	For CSIRTs
1	Ensure coordination with other donors taking into account past and future projects	Make sure to understand donors' intentions and communicate needs	Be open to government and donors about needs and expectations
2	Where existing, base support projects on CSIRT capacity building plans; where not existing, support their creation first	Ensure CSIRT capacity-building plans reflect national priorities and are complementary to other cybersecurity stakeholders' development and operational plans	Develop and own capacity-building plan: make sure it remains relevant and continuously revised and updated, even as an informal document
3	Ensure synergies with other interventions whenever possible	Ensure CSIRT needs are included in donor communication, particularly on digitalisation and security sector governance reform assistance	Make sure you have constant communication with responsible ministries on your development- achieved progress and future needs
4	Whenever possible, foster regional and international approach to capacity building	Ensure CSIRT's have travel budget for relevant CSIRT events	Communicate the benefits of regional and international cooperation and peer learning to the government regularly and continuously
5	Aim to offer practical and applicable training and solutions and remain vendor neutral as much as possible	Remain vendor neutral as much as possible	Remain vendor neutral as much as possible
6	Be aware of political developments and their impact on capacity development efforts; factor them in assistance plans	Enhance regional cooperation in cybersecurity capacity building for CSIRTs and policymakers whenever possible	Be active in all formal and informal regional and international CSIRT communities

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