DCAF Geneva Centre for Security Sector Governance

Western Balkan CERT Cooperation

Written on the request of DCAF
by the Open CSIRT Foundation

Editors:
Prof. Dr. Klaus-Peter Kossakowski
Mirosław Maj
Don Stikvoort MSc

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

Table of Contents

1. Introduction

In July 2018, DCAF started the three-year project "Enhancing Cybersecurity Governance in the Western Balkans" (July 2018-March 2021). This Project is funded by the UK Government`s Foreign and Commonwealth Office (FCO) and aims to contribute to more effective and accountable cybersecurity governance in the Western Balkans, as well as to increase the regional cooperation in cybersecurity. It primarily addresses the following economies and their national CSIRTs[1] (in alphabetical order of official name):

- Republic of Albania (AKCESK/NAECCS)
- Bosnia and Herzegovina (CERT RS)
- Kosovo * (KOS-CERT)
- Montenegro (CIRT.ME)
- Republic of North Macedonia (MKD-CIRT)
- Republic of Serbia (SRB-CERT and MUP CERT[2])

One of the most significant outcomes of the project focuses on the capacities of national CSIRTs (short: nCSIRTs) in the Western Balkans and the communication and cooperation among them. In the course of the first two project years, members of Western Balkans nCSIRTs were brought together in many events (conferences, drills, training, online discussions) and as a result improved communication and trust. For example, they set up joint Viber groups, supported each other with professional advice and also worked together on incidents. On several occasions, the CSIRTs discussed possibilities of improving their communication, for example by setting up a joint MISP[3]. Another idea was to set up more formal cooperation frameworks.

1.1 Target Audience

The target audience of this report is as follows:

Western Balkans policy makers (responsible for policies on cybersecurity and cybersecurity incident management)

Western Balkans national CSIRT teams (responsible for handling cybersecurity incidents and vulnerabilities on the operational level)

The international community in Western Balkans economies (supporting regional cooperation in cybersecurity)

---

1 * 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. We use the free, unlicensed term "CSIRT" throughout, and the original term CERT (trademarked by the Carnegie-Mellon University or CMU) only in the title: content wise, there is no difference between both terms. We did not review the state of affairs on this matter in the region, but it was brought to our attention that both teams from Serbia signed agreements with CMU for the use of the name "CERT".

2 MUP CERT acted originally as Serbian CSIRT of last resort, until SRB-CERT took up the nCSIRT role. However, given MUP CERT's significant role, we have approached both SRB-CERT and them.

3 MISP: Open Source Threat Intelligence Platform. See https://www.misp-project.org/

1.2 Objective

The objective of this report is to provide concrete proposals for the target audience on possible approaches and models for enhanced cooperation among Western Balkans national CSIRTs based on the following main research questions:

- In which areas can national CSIRTs from the Western Balkans region cooperate with other nCSIRTs, but also other types of CSIRTs, from other economies, to increase their capabilities (to detect, analyse and mitigate attacks; to analyse and communicate warnings and alerts to prevent such attacks; to raise public awareness; etc.)?
    - What successful CSIRT cooperation networks (in Europe and other parts of the world) exist?
    - Which of these are relevant for the national CSIRTs from Western Balkans economies?
    - How and to what extent can models of international best practice be applied?
- How can the national CSIRTs from Western Balkans improve their multilateral cooperation and communication by building on their achievements of the past?
    - What successful CSIRT collaboration tools and processes exist?
    - Which of these are relevant for the nCSIRTs from Western Balkans economies?
- How and to what extent is the cooperation among the national CSIRTs from Western Balkans affected by the individual capacities and capabilities as well the maturity of each individual nCSIRT?
    - What successful approaches and best practices exist to evaluate and plan for the improving of maturity, including the appropriate capacities and capabilities?
    - Which of these are relevant and should be applied within the Western Balkans economies?

1.3 Report Structure

Before we address the three areas identified by the main research questions listed above, we will briefly review the background of the status quo of CSIRTs in the Western Balkans in chapter 2.

In chapter 3 we will address how the national CSIRTs benefit from European and international communities by engaging with these communities as valued, contributing members.

Chapter 4 will focus on multilateral collaboration within the Western Balkans, before we will turn to focus on the national situation of the teams in chapter 5. The main concern we found is the need for further increasing maturity that in turn will enable improvements in all other areas we outlined in the preceding chapters 3 and 4. The concluding chapter 6 will present key recommendations based on our research.

2. Background on CSIRT Development in the Western Balkans

CSIRTs have been active in the Western Balkans since 2011, but the majority have been established after 2015. More recently, the Western Balkans national CSIRTs have adopted best practices and most of them have become TI Accredited.

Of course, DCAF has organized extensive support in the region in the past three or more years, through assessments, training, advice and regional meetings. Also, the ITU has supported regulatory bodies in some economies and applied best practices from their National CIRT program, while others have benefitted from training provided by FIRST and/or TF-CSIRT/TRANSITS volunteers. CERT/CC and KISA were also mentioned as contributors.

Economy	National team	Established since	TI Listed	TI Accredited	Other TI Listed teams
Republic of Albania	AKCESK/ NAECCS	2017	2013[4]	May 2020	---
Bosnia and Herzegovina	CERT RS [5]	2011	2019	April 2020	---
Kosovo*	KOS-CERT	2013	2013	July 2017	5
Montenegro	CIRT.ME	2011	2016	July 2017	---
Republic of North Macedonia	MKD-CIRT	2016	2016	Dec. 2017	---
Republic of Serbia	SRB-CERT	2017	2017	Aug. 2019	4[6]

All teams referred to in the table, plus MUP CERT, participated in our expert interviews and were very helpful in answering additional questions. Based on their experiences, insights and willingness to discuss the ideas raised in the interviews, we were able to deliver this report both quickly and with sufficient depth.

4 An older team with the same name has existed since 2013. In 2017 the current team was established with a new mandate, taking over the previous TI Listing.

5 CERT RS is the coordinating team for the Republika Srpska, one of the entities of Bosnia and Herzegovina, but it is the only active CSIRT team in Bosnia and Herzegovina.

6 This includes MUP CERT, which was established in 2015, and became TI Listed in 2016 and TI accredited in November 2018. The oldest CSIRT in Serbia is AMRES-CSIRT, which was established in 2011 and became TI Listed in the same year.

3. Benefitting from European and International Communities

In all interviews, we found in all teams a strong drive to participate in extra-regional and international CSIRT cooperation. TF-CSIRT and FIRST were unanimously mentioned, as was ENISA. This section will examine this in more detail.

3.1 International CSIRT Cooperation

The three most relevant forms of supra-national CSIRT cooperation are briefly treated below.

3.1.1 Sectoral Cooperation

For any given economy, it is useful to assess what supra-national cooperations exist on the CSIRT-level in critical sectors (government, finance, energy, healthcare, etc.). For example, EU national/government CSIRTs cooperate in the CSIRTs Network, administered by ENISA[7].

Where relevant cooperation platforms exist, it is useful to find out the benefits and responsibilities that come along with joining them. Joining the CSIRTs Network would certainly be very useful and beneficial, but this is currently only open to EU Member States national teams – neither teams from the EEA nor from economies who are candidates for EU membership are currently involved in the CSIRTs Network. However as becoming a member of the EU will also involve the cybersecurity aspect, it is useful to work with the higher political levels in Western Balkans economies to see what kind of cooperative approach could be taken towards ENISA and the CSIRTs Network.

In this sectoral light, ISACs (Information Sharing and Analysis Centres) are also worth considering as a model.[8]

And relevant ISACs are for instance:

- EE-ISAC (European energy sector)[9]
- European FI-ISAC (European financial sector)[10]

3.1.2 Transnational cooperation

To join a transnational CSIRT cooperation platform that is relevant for your team, is very strongly recommended, and for nCSIRTs it can be classified as indispensable. Such transnational cooperation platforms have been essential in the development of the CSIRT community ever since 1993. Most of them also provide some form of CSIRT training. The most prominent examples of such cooperations:

- Africa: AfricaCERT11

---

7 https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network.

8 See e.g. https://www.nationalisacs.org/member-isacs ; and also https://www.enisa.europa.eu/news/enisa-news/cybersecurity-built-on-trust-2013-enisa-supports-member-states-in-establishing-ppps-and-isacs

9 https://www.ee-isac.eu/

10 http://www.fi-isac.eu/ (This currently links to a relevant ENISA page)

11 https://www.africacert.org/home/

- Asia-Pacific: APCERT12
- Europe: TF-CSIRT13 and Trusted Introducer14, which provides the trust infrastructure for the TF-CSIRT community
- The Americas: OAS CSIRT Americas15
- Latin-America: LACNIC CSIRT16

Of these, TF-CSIRT/Trusted Introducer is the relevant candidate for Western Balkans economies. As can be seen in the table in chapter 2, the current status is that all Western Balkans nCSIRTs are TF-CSIRT/TI Accredited (including MUP CERT).

The full TF-CSIRT membership (Accreditation) can indeed be a great benefit to any team. It provides the following advantages:

- For the team to establish and increase its trust relationship within the wider CSIRT community. Trust is the basis of all CSIRT interactions, and thus part of the foundation of success for any team;
- For individual team members to get involved in community initiatives that may also benefit the team;
- For the team as source of information, and particularly as a source of information channels;
- For the team members to develop professionally in concert with colleagues from other teams and economies who share the same challenges we all face, and to all learn from both experienced colleagues, and from colleagues with bright, new ideas;
- There are various TI services for Accredited and Certified teams, which range from informational services to tri-annual connectivity checks.

To benefit optimally from the TF-CSIRT membership, it is necessary to attend the meetings regularly. These meetings take place three times per year, hosted by members in various places all over Europe. Since May 2020 meetings have taken place online, but as soon as possible, in-person meetings will be held again. To regularly participate in these meetings is the best way to get involved, build trust, and become a valued member of the CSIRT community.

There is one optional TF-CSIRT membership step beyond Accreditation, and that is Certification. For that it is required to attend to at least one TF-CSIRT meeting per year. Successful certification is an especially good way to help a team increase their maturity level. We see this as an important opportunity for the Western Balkans nCSIRTs, and this is described in paragraph 5.2 below.

12 http://www.apcert.org
13 https://www.tf-csirt.org/
14 https://www.trusted-introducer.org
15 https://csirtamericas.org/
16 https://csirt.lacnic.net/en

3.1.3 Worldwide Cooperation

Worldwide, several cooperation is notable and useful for nCSIRTs.

One advantage is the National CSIRTs annual meeting, known as NatCSIRT: this is a very successful project of CERT/CC bringing together only national CSIRTs worldwide.[17]

All nCSIRTs from the region are mentioned on the NatCSIRT website. We strongly recommend attending the annual meeting when invited (or to apply for an invitation, if needed), when they resume. This usually coincides with the annual conference of the next (and in our eyes most important) worldwide CSIRT forum - the Forum of Incident Response and Security Teams (FIRST).[18]

All transnational cooperation platforms referred to above, as well as NatCSIRT, liaise with FIRST. This forum has become too large to perform actual incident-handling activities, but it is an extremely valuable resource for connecting with other teams from all CSIRT communities worldwide, including the vendor community. This can help you acquire contacts for incident/threat handling, and it allows you to join projects, training and useful initiatives for your team. Finally, FIRST organizes a conference each year, which is a good place to network in the CSIRT community.

So far, the nCSIRTs from Montenegro and Serbia, and MUP CERT, have joined FIRST. CERT RS, MKD CIRT and AKCESK/NAECCS are members of the FIRST Fellowship program, which also aims at reaching membership. So here as well the Western Balkans teams are making excellent forward strides. And again we highly recommend prospective members taking advantage of the FIRST membership, attending the annual conference when possible, and also attending some of the many regional “TC” meetings; or organizing a TC in the Western Balkans in cooperation with FIRST as SI-CERT did in Slovenia in November 2019. FIRST is the best environment to meet teams from all over the world and learn from them, as TF-CSIRT is the best place to do the same thing inside Europe.

Finally, three other players need to be mentioned. They are not CSIRT cooperations, yet they do important and useful work in this area:

1. Foremost DCAF, which has organized extensive support in the region in the past three or more years, with assessments, training, advice and regional meetings, and is the enabler of this report.
2. On the global telecommunication level, the ITU is strongly committed to advancing cybersecurity. This especially includes nCSIRT development programs.[19] These days, the ITU works together with such organizations as FIRST, GFCE and Open CSIRT Foundation in order to promote the use of open and de-facto standards in the CSIRT community.
3. The Global Forum for Cyber Expertise (GFCE) brings together cybersecurity players on all levels, from political to corporate levels, NGOs and CSIRT cooperations like FIRST. The GFCE is good in bridging such gaps between the different worlds of (cyber) diplomacy and technical cybersecurity experts, among others. Inside the GFCE, there is Working Group B on cybersecurity that delivers useful results. At

---

17 See for their repository of teams: https://sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/

18 https://www.first.org.

19 For the ITU Global Cybersecurity Agenda (GCA) see http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

least one of the Western Balkans economies is represented in this Working Group. The GFCE is also determined to promote open and de-facto standards in the CSIRT community.

3.2 International Best Practices in the CSIRT Field

We mention here a few highly relevant international best practices in the CSIRT field, strongly recommended to use or take into account in the Western Balkans (some are already effectively being used by most, like SIM3):

- CSIRT maturity development: SIM3, developed and maintained by the Open CSIRT Foundation.[20] This is the standard model for understanding and assessing maturity for all kinds of CSIRTs. To self-assess SIM3 maturity using an online tool, see:[21]
- CSIRT maturity profiles for national CSIRTs: GCMF (Global CSIRT Maturity Framework)[22]. This applies SIM3 to define three nCSIRT maturity profiles, basic, intermediate and advanced (originating from ENISA, but adopted for a worldwide context in the GCMF). The same online assessment tool as for SIM3 can also be used (see above);
- CSIRT services descriptions: FIRST CSIRT Services Framework[23] is a highly structured description of CSIRT services, starting from main service areas. Each service area features several services, and each service features several functions. Each CSIRT should use this as a "restaurant menu", starting from its mandate and responsibility, to choose those service areas, services and functions that the team should offer, while staying within reach of staff and resources available.
- How to set up CSIRTs and SOCs: a new ENISA guideline document exists:[24] The title says it all - pragmatic and recommended.
- CSIRT ethics: the generic ethics frameworks of governments and corporations do not really cover the specifics of the CSIRT work. Two de-facto standards exist in this area, and they are both highly recommended: The Trusted Introducer (TI)[25] is the standard in the TF-CSIRT community; FIRST[26] is of fairly recent date.
- Traffic Light Protocol (TLP)[27] is a must-use for all CSIRTs worldwide.[28]
- CSIRT staff skillsets: CERT/CC's "What Skills Are Needed When Staffing Your CSIRT?" is an excellent starting point.[29]

20 https://opencsirt.org/ (SIM3 is found under the tab "Maturity")
21 https://sim3-check.opencsirt.org/#/
22 https://cybilportal.org/tools/global-csirt-maturity-framework/
23 https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
24 https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
25 https://www.trusted-introducer.org/TI-CCoP.pdf
26 https://ethicsfirst.org/
27 https://www.first.org/tlp/
28 Note that it is possible to translate TLP into your own language and ask FIRST to place it on this site. There are some rules for this at: tlp-sig@first.org
29 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485683

4. Improving the Cooperation of Western Balkans national CSIRTs

Interviews with CSIRT teams presented many important aspects of the current level of cooperation in the region. To date, no particular cooperation model has been proposed or implemented. The observed situation is a result of ad hoc initiatives, very often in the shape of peer-to-peer cooperation. These initiatives are related to both the operational and organizational aspects of cooperation.

4.1 Identifying Multilateral Opportunities and Needs for Cooperation

The interviews and additional analysis gave us a chance to evaluate the existing cooperation as well as propose potential ideas for further facilitation of cooperation in the region. It is important to emphasize that a need for (more) regional cooperation does not automatically mean that a formalized solution needs to be established.

4.1.1 Formal Cooperation

There is no formal form of multilateral cooperation in the region right now. There are a number of mutual agreements, usually in the form of a memorandum of understanding (MoU) between peer parties. These formal agreements have various causes. Sometimes they are the result of real cooperation, during which both parties decided at some stage that it is worth formalizing. Political motivations can also play a role. However, these agreements don't appear to be the result of government pressure and do not illustrate the whole picture of cooperation in the region. In fact, a substantial (and also successful) part of cooperation appears to be based on informal trust relationships between nCSIRT members in the region.

Additionally, some teams reported cooperation agreements with teams outside the Western Balkans region - either politically (with or without membership status in the European Union), or geographically. Among the teams with which such agreements are in place, are Bulgaria, Hungary, Slovenia, Moldova and Romania.

4.1.2 Operational Cooperation

Operational CSIRT cooperation usually starts as cooperation on the incident response aspect of incident management[30] – working together on resolving actual incidents. This is usually a very strong factor in determining cooperation.

In the Western Balkans, teams do work together on incidents ad hoc, but there does not appear to be a strong existence of what could be labelled "regional threats" leading to shared incidents. There are limited examples of incidents which affect (bigger parts of) the region. Specifically, some DDoS attacks, phishing, spam, and sometimes ransomware. These are however not recognized as a problem requiring a special regional approach and can be dealt with using the current MoU-based and other informal forms of cooperation. These common incidents are the result of language similarities in the

30 Incident management includes incident prevention, detection, response and lessons learned. Cooperation starts with the response aspect, later often followed by prevention/detection (threat intelligence, etc.).

region, but still their scale and frequency do not necessitate a formal regional kind of cooperation as yet.

Other, potential reasons for closer operational cooperation, like common vulnerabilities, are so far experienced as very rare – that is to say, they are more of a wider international than regional nature.

4.1.3 Barriers and Limitations

We concluded above that neither the pre-existing and functioning formal peer-to-peer cooperation, nor the operational needs, are factors which should lead to more structured forms of regional cooperation. However, there are other aspects, which we can classify as barriers or limitations, which appear to be good reasons to shape increased cooperation in the near future. The aspects that we found to be most important are the following:

- Competences shortages

Most teams report lack of competences within their staff as one of the main barriers in their development. This especially relates to technical competences. More, and more specialized, education/training and exercises/drills are important solutions in this area – and due to the fact that there is considerable language similarity in the Western Balkans, regional cooperation could facilitate that.

- Financial and organizational limitations

Financial limitations seem to be a significant problem, especially in terms of staffing and building international relationships. In some cases, decision makers also do not fully understand the needs of CSIRTs, which is not helpful for challenges like shortage of staff. Regional cooperation could facilitate the recognition and resolution of these issues.

- Political barriers

Some of the state level political relationships in the region are challenging. These problems influence also operations of these economies' national CSIRTs. Regional cooperation on the CSIRT level may help to mitigate this.

4.2 Establishing Improved Cooperation and Collaboration

Based on our analysis of the current situation as well as suggestions received in the interviews – sometimes very clearly verbalized – our general finding is that the national CSIRTs in the region do not need any specifically regional type of operational cooperation, beyond what exists already on peer-to-peer level. By operational we mean mainly related to the daily incident management activities. On the other hand, we did identify a number of ideas which should be taken into consideration in regard the further development of the CSIRT cooperation in the region. These ideas are, by logical consequence, not ways of resolving incidents together, but rather how to work together to improve the incident management capabilities of all CSIRTs in the region, ostensibly national ones, but with the potential to benefit the whole CSIRT landscape.

This should ideally be a flexible type of cooperation, with very little overhead – as lack of staff is a genuine challenge all over, and some representatives of the interviewed teams believe that a too strong focus on regional cooperation could detract from the existing international cooperation and memberships. From their perspective, the most important thing is to participate in existing cooperation platforms like TF-CSIRT or FIRST, and to have access to resources and services provided by ENISA rather than to hermetically seal a Western Balkans cooperation.

4.2.1 Regional Meetings

Regular regional meetings would facilitate a natural development of the cooperation potential. These meetings should be not be focused on resolving specific incidents in the region, but rather to help share experiences of how to operate effectively in similar political and economic environments, and to discuss and prepare the items of training etc. mentioned below. During the meetings, participants could also discuss common initiatives on an organizational level, which could help them to work together with organizations outside the region.

The natural advantage of such meetings is the language similarity in the region. This makes the exchange of ideas and all other verbal communication easier and more natural.

Regular regional meetings, sometimes online and perhaps once a year in person, would become a stable platform for managing any other organizational activities like team development (including the maturity growth based on SIM3) or international cooperation (e.g. FIRST fellowship program).

4.2.2 Training

The idea of shared training was the most often proposed during the interviews. It is based on two important factors – language similarity in the region, and the fact that training addresses the shortage of competences. Technical competences shortages are a particular challenge to overcome for several teams in order to more fully develop their incident management capabilities. Regular training could significantly improve this situation.

Technical training is not the only form mentioned as potentially beneficial. Some other training ideas mentioned are: TRANSITS training[31] and SIM3 training[32].

4.2.3 Exercises

Exercises, drills and similar practical methods for evaluating and developing incident management services, became very popular in the last five years. CSIRTs or their members increasingly participate in various types of such events. Good examples are the periodically organized Cyber Europe events hosted by ENISA.

This practical concept, organized within the Western Balkans region, would become another method for both improving skills and competences, and building trusted relationships among participants. In the mid-term perspective, such events could also pave the way for participation in supra-regional events, e.g. aforementioned Cyber Europe exercises.

It is recommended to not limit the scenarios for such events only to the technical aspects. All other competences - organizational as well as procedural - are at least equally important, especially for teams with national-level responsibilities.

As a continuing learning activity, some kind of friendly competition could be organized. One option to organize such an activity without significant cost would be a series of CtF (Capture the Flag) events, organized by the nCSIRTs themselves. Other CSIRTs in the region could take part if the nCSIRTs would so decide, or exercises with varying scope can be set up only for the nCSIRTs, but with a wider scope.

---

31 https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS_Training.aspx

32 SIM3 training can be requested to the OCF: https://opencsirt.org/

4.2.4 Building Trust

There is no doubt that for all CSIRTs, very much including nCSIRTs, it is very important that their members can interact at the same (or similar) level as the members of well-established teams, in order for them to operate successfully and participate in important collaboration platforms. All interviewees were aware of the fact that this is in practice a "must" for them if they want to be effective as nCSIRTs for their national level constituencies. The teams' representatives all recognized that this requires not only joining international cooperations, but also being active in them. This is the most effective way for building trust with partners in Europe and worldwide.

A potential solution that would support developing the building of trust would be some kind of council, which could engage CSIRTs from the region and representatives from other regional or global organizations (e.g. FIRST, TF-CSIRT, DCAF, Open CSIRT Foundation, ENISA, ITU, GFCE et al.) with the goal to promote and help the Western Balkans teams to build trust with their most important partners. This council should be related to or be a part of the pragmatic and down-to-earth regional cooperation initiative described in this paragraph 4.2. DCAF has been effectively supporting this concept the past few years, and perhaps this model can be further built on.

4.2.5 Information Sharing

Even given the fact that teams generally do not see a special benefit for regionally organized incident response, they do believe that actionable information sharing is important - within as well as outside of the Western Balkans.

One practical solution for sharing Indicators of Compromise (IoCs) would be to establish a "Western Balkans MISP platform". The fact that there seems to be few incidents with a specifically regional (rather than national, or international) character may not be the strongest impulse to create such a MISP platform right away. However, it is quite likely that information about such threats/incidents will not be found in external information sharing platforms – and actually, this could also be a relatively low-cost way to make MISP work for all nCSIRTs in the region. Naturally, feeds from other existing MISP platforms (e.g. SI-CERT, CIRCL) can be used to good effect. Also, this could be a testbed for operational cooperation, and should be run as a pilot first, because in cybersecurity you are never quite sure about what you may or may not miss, until you find out.

We do advise to start a pilot like this only after examining and realizing the above cooperation ideas, which are more pressing at this moment.

5. Improving the Maturity of Western Balkans National CSIRTs

While we began our report by addressing international and regional issues, it is obvious that any cooperation with teams outside any given nCSIRT's own economy depends on the team's capabilities – and even more so on the capacity available for such activities. Improving regional cooperation is a long-term effort compared to any acute attack or threat to the critical infrastructure of an economy. But whenever a service-oriented organization like a CSIRT is faced with the pressing needs of open incidents and attacks, their ability to spend critical work time on long-term issues is greatly reduced.

Any improvement (including other areas identified in the previous chapters, but even for the handling of attacks and incidents) must be supported by the internal set-up and maturity of each single team. Therefore, we took such aspects into account for all teams. Some of the teams supported this part by executing a SIM3[33] self-assessment, providing us with the ability to identify whether some common patterns might exist. All findings have been generalized without referencing individual teams, in order to highlight issues that need to be considered for all teams.

We understand that the priorities of each economy (particularly now during the pandemic) are manifold and that a nCSIRT is usually not the most important priority. We offer recommendations without considering that landscape, as it is out-of-scope for this report, but we trust in the fact that the recipients of this report will be able to attach an appropriate priority to this, given the fact that national cybersecurity is of vital importance for any economy and its citizens, and must also be well protected in case of attacks of all kinds. National CSIRT programmes play a crucial role in this landscape.

In the following paragraphs we will be describing the maturity of Western Balkans national CSIRTs based on the interviews and the maturity self-assessments provided by some of these teams. In the second paragraph we provide recommendations on how to improve the maturity of the nCSIRTs in general, though we are not examining any team specifically within our report but are outlining approaches and findings that can be applied to all. The third paragraph focuses on recommendations improving the maturity of cybersecurity strategy on a national level related to the role of the nCSIRT.

5.1 Maturity Assessment

For an assessment of the conditions that impact the maturity of nCSIRTs, very few frameworks exist. The best-known one is the Security Incident Management Maturity Model – SIM3. It was adopted by ENISA for measuring the maturity of nCSIRTs and is therefore very applicable. SIM3 is also used by TF-CSIRT since 2010 for the purpose of CSIRT certifications, and FIRST is adopting it as part of their membership process.

5.1.1 Lawmaking

Most nCSIRTs have been established based on laws which were introduced many years ago. In almost all of the six economies that we interviewed team members of, efforts are underway to modernize the laws and regulations for cybersecurity, but unfortunately some of these efforts have not made much progress in the last two or three years. All economies are also taking the EU NIS Directive into account for their lawmaking, but as

[33] The SIM3 standard is maintained by the OCF (see https://opencsirt.org/) and describes the maturity of CSIRTs by means of 44 parameters in four areas (organization, human aspects, tools and processes).

the new laws have not yet passed, there is no common baseline for what exactly constitutes a nCSIRT. For the economies for which these new laws have not yet passed, this also implies that no modern cybersecurity strategy has been fully adopted yet. Henceforth, nCSIRTs in the region will show substantial differences in mandate, given authority and responsibility - and even their constituencies (the target group they work for) show a lot of variation.

5.1.2 Sectoral CSIRTs

Following a trend that can be observed globally and was also adopted in the EU NIS Directive it is most likely that economies will establish sectoral CSIRTs that coordinate the incident management activities within specific "sectors". It can safely be expected that the establishment of sectoral CSIRTs will require the support of the nCSIRT in each economy, and a recent ENISA CSIRT/SOC set-up guideline can be put to good use[34] there. A challenge is that most nCSIRTs are currently not well prepared for this new task, neither by design nor by the capacity of their team.

But the integration of sectoral CSIRTs will also require changes in the processes and ways that a nCSIRT handles attacks and incidents. Perhaps the most severe change when establishing such sectoral teams is the need to coordinate the various CSIRT-related activities inside each economy.

5.1.3 Neutrality and Trust

It is under those circumstances indispensable that the organizational setup of the nCSIRT will ensure its neutrality in order to allow the nCSIRT to act as a trusted partner in all of this. But also right now, when several of the Western Balkans nCSIRTs are still the single most important contact point in regard cybersecurity incident management in their economies, this neutrality and trustworthiness are essential factors.

In some Western Balkans economies, the currently established nCSIRT may be moved into a new entity . This can be a good step, as long as it ensures or improves this required neutrality and provides for an appropriate set-up supporting a trusted and well-respected nCSIRT in the long run.

Similar to the new tasks related to sectoral CSIRTs, several more tasks will be assigned to the nCSIRTs once the pending laws will finally have passed. This will also require preparatory steps and will take a toll on the available workforce while adjustments and additions are elaborated and integrated.

5.1.4 Shortage of Staff

The interview findings suggest that almost all teams are low on staff, and they already have a hard time finding qualified and experienced people to tackle the current tasks, let alone take on new ones. Therefore, in terms of governance it is crucial to ensure not only that the nCSIRT's budget is available, but even more so that this budget can actually be spent on filling all open positions and staff the teams accordingly. Currently, some teams offer 24/7 service levels but have actually less than 4 FTEs: this means that the operational base for 24/7 coverage is neither dependable nor sustainable – at least not if these service levels involve real-time activities on a regular basis.

We found that some teams are not able to fill open positions (some have up to 40% of all positions open), because the required skillsets call for more senior experts, which are

[34] See https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

very difficult to find. Rather than leaving matters to chance, it is advised to reassess the situation and see what activities can be undertaken by a less experienced team, or even fairly junior team members, so that the senior experts can focus on matters that require advanced experience. If this also necessitates hiring more junior people, this may even have a positive budgetary effect.

Another important aspect of having open positions for longer periods of time is the fact, that part of the existing work simply does not get done – at least not on the level expected by stakeholders and higher governance. As a result, new expertise will hardly be built up, and there is no room for improvement beyond simple stasis.

In sum, unless adequate funding is actually available, the funding is also spent on the intended causes, and enough hands are allowed on the job, then any nCSIRT might still exist, but it is unclear to what degree it can perform its crucial duties and assigned tasks.

5.1.5 Information Exchange

Another area that concerns us is the need for more information exchange, both manual and automatic. The availability and processing of all kinds of actionable information is at the heart of each nCSIRT, as public, CII and private entities will depend on timely and accurate information. Teams across the globe are working to integrate automated and scalable approaches like MISP. But teams who lack agile staff members, or who are only calibrated for incident response (as is the case with several Western Balkans teams) will struggle to cope with this necessary progress. And that could cause those who depend on the nCSIRT's input to also fall behind in their ability to provide adequate cybersecurity to their infrastructures, sectors, agencies, businesses or organizations. It's important to remember that cybercriminals and terrorists remain active in their pursuit of automation, machine learning, AI, etc., hence for CSIRTs and governments to remain behind in this 'arms race' is simply not an option.

A more automated exchange of actionable information is therefore crucial to allow nations to manage cyber-crises timely and effectively. But at the same time, automation has the added benefit of freeing staff from routine processes and manual steps, thereby allowing more time to focus on core issues and other aspects that can make a difference. Therefore, automation must be considered one of the cleverest investments to make. Do expect a learning curve however; meaning that in order to reap the harvest, you need to sow the seeds first, and work the land. This takes extra effort, and therefore it is strongly recommended to implement new tools, techniques and automation for well-defined projects - preferably with the help of extra people (project leaders, extra staff, trainers, etc.).

5.1.6 Maturity Self-assessments and GCMF/ENISA Maturity Stages

As stipulated above, the common model to measure CSIRT maturity with is the SIM3 model. An online tool is available that allows teams to perform SIM3 self-assessments.[35] ENISA has established three maturity stages based on SIM3: Basic, Intermediate and Advanced. This ENISA model has been generalized for worldwide use in the Global CSIRT Maturity Framework.[36]

A more detailed analysis of the SIM3 self-assessments provided by four (of six) teams showed the following issues that are affecting at least three of the teams (which means

35 See https://sim3-check.opencsirt.org/
36 See this link to the GCMF

at least 50% of the economies). For the SIM3 parameters listed below, those three teams are not meeting the GCMF/ENISA "Intermediate" stage:

- Responsibility (O-4) and Service Description (O-5, including Service Level Description (O-7): This can only be attributed to a legal baseline that does not address all required details or is vague in expressing clear guidance on how far the responsibility of the nCSIRT goes. This is a well-known problem often found with laws on cybersecurity established before 2012, where often a nCSIRT is called for without clearly defining its role. In such cases it is critical for the nCSIRT to find supporting documents and guidance on its mandate in other regulations. Nowadays, the EU NIS Directive does provide a clear set of requirements that should be considered for all nCSIRTs.
- External Networking (H-7): Based on our interviews we conclude that this shortage is based on a lack of (human) information exchange with other teams. One of the quick gains here is to actively participate in the European TF-CSIRT, and to regularly attend their meetings. This is cost effective (no or very low meeting fees) as TF-CSIRT meetings are organized as a community effort. Participating does require an extra effort for smaller teams, as the one or two-team members at the meeting can't be expected to perform their normal duties for a few days. The outcome is however very much worth this investment.
- Audit/Feedback Process (P-8): As a nCSIRT is carrying a great responsibility, governance needs to be applied on the right level as well. This is why the maturity stage expected in the GCMF/ENISA approach for such aspects as mandate, constituency, authority and services is high, and in practice this is often defined in specific legislation. But where the governance level expects so much of the nCSIRT, that same governance level needs to ensure that proper auditing or reviewing of the team takes place and is sufficiently validated and communicated. Therefore, it should not be left to just the team itself to review its core values. P-8 is the parameter that covers this issue of auditing and feedback. The fact that this parameter does not always score very high can often be attributed to older laws or regulations that do not address this issue.
- Emergency Reachability Process (P-9): While all teams have the technical means to ensure reachability utilizing smart phones etcetera, the underlying issue is again related to the availability of team members. If a team has less than 5 FTE, a 24/7 service cannot be maintained in a responsible way. Depending on the national mandate and other more technical issues, a 24/7 service might not be strictly needed yet, but in the near future, for any national CSIRT also acting as national point-of-contact, 24/7 availability will be the default. Therefore, it is mandatory to provide the required staff level to sustain such service levels and reachability.

At least two (out of six) of the teams expressed issues with the below mentioned SIM3 parameters. Again, these teams' results are not meeting the requirements for the GCMF/ENISA "Intermediate" stage. This would imply that between 33-66% of the national teams may share the same issues:

- Constituency (O-2) and Authority (O-3): We attribute these issues again to older laws or regulations which do not provide clear details for the constituency and authority of the national CSIRT. It is necessary to know what the nCSIRT needs when adopting new laws governing their operation.
- Personnel Resilience (H-2): Based on our findings above (for H-7 and P-9) it is clear that smaller teams, and even more so when there are vacancies, are simply over-

worked. Therefore, there is a lack of personnel resilience even in normal times, let alone in times where critical staff members are ill or otherwise absent – and it could mean the team cannot deliver their services according to their mandate.

- Internal Training (H-4) and (External) Communication Training (H-6): The interviewed teams appear to depend mostly on external training, as they simply do not have the manpower available to develop and organize internal training for new and existing team members. This is not a significant problem in itself, as external training can be adequate (though often costly), but it does stress again the critical aspect of staff shortage.
- Escalation to Governance Level (P-1) and Escalation to Legal Function (P-3): For these parameters as well as for O-2 and O-3 above we attribute the issue to unclear mandate and authority. All nCSIRTs need to have immediate access to higher governance levels and need to be able to consult legal experts on short notice, as attacks and threats sometimes require critical decisions that involve both higher management as well as legal advice.

It is promising that no team reported issues with the more technical SIM3 parameters. This could also be concluded from the interviews as most of the technical problems that were mentioned could be tracked back to either missing training or a lack of available staff.

5.2 Improving CSIRT Maturity in the Region

Each and every improvement must start with a national CSIRT within each economy. Given the number of open positions in several teams and the difficulty of filling those, we urgently recommend reviewing those open positions and identifying new ways to fill them. This might include creating incentives that attract younger people in particular who have finished university (or similar) studies recently in subjects related to cybersecurity and safety.

We were unable during our short project to conduct a detailed analysis of all teams covering all aspects, but as described in the previous paragraph, the available results do make such an assessment highly recommended.[37] This is even more important as we were not able to consider the legislation - either old, new or developing - for all economies in a more detailed fashion. This should really be taken into account as part of such assessments – and not by lawyers, but by CSIRT experts who also understand common legislation in this field. When such experts consider the proposed drafts in the various economies, important conclusions can be reached that will help the teams to better prepare for the future laws, and the changes in mandate, authority and responsibilities that will bring.

In this context it would be highly useful to organize independent in-depth SIM3 assessments for reviewing the organizational set-up of teams, as well as the human factors, the tools/technology aspects and policies/processes/procedures. The objective would be to identify particular issues, starting with the availability of staff, and also addressing the other issues raised in this report. We would expect that based on such a SIM3 assessment, an action plan with short-term and ad hoc activities can be established right away. Furthermore, the mid-term to long-term activities could then be written up and presented as a comprehensive roadmap with a clear timetable. This timetable should be

[37] We recognize that at least one of the teams has already engaged with the help of external consultants in such activity.

based on the goal to reach the GCMF/ENISA "Intermediate" stage in the short-term (1-2 years) and allow for a Certification under the TF-CSIRT/TI Framework in the mid-term (2-4 years). For one or two teams this Certification can already be achieved in the short-term, as those have a bigger workforce and are already engaging in a maturity-based development path. Following on Certification, achieving the GCMF/ENISA "Advanced" stage can be planned.

All teams we considered have a need for developing new capabilities and gaining more practical experience. The topics are not only related to the use of tools like MISP, the analysis of malware, the execution of forensic analysis of compromised systems, or how to improve an existing incident taxonomy to represent incidents of particular industry sectors. While this is important to provide the core functions of any national CSIRT, they also need more practical experience to exercise the workflows, identify flaws and weaknesses in their internal processes as well as difficulties in working with other teams that are important while responding to a cross-border incident or attack.

We recognize a shared need in this area and therefore recommend furthering research opportunities to improve the teams' capabilities by training and exercises organized in the region, as argued in chapter 4. This will also help in collecting the critical mass for any such event, and it will be more cost-effective. In addition, exercises and drills will help all participants to improve their response during real incidents later on.

Furthermore, all teams should more strongly engage in external networking on at least the European level. The TF-CSIRT approach is in particular brings a wide range of different CSIRTs together and provides access to lessons learned by those teams. By by more closely interacting in this community, teams will be able to fill the gaps that cannot easily be filled right away by internal training, or even regional-level training, as it first takes sufficient experience to grow.

Most certainly these team-oriented suggestions are already providing benefits and creating opportunities, but the overarching goal right now should be to further improve the maturity - and not just the nCSIRTs. The ultimate goal is to improve the whole cybersecurity landscape of each economy. This requires more activities as outlined in the following section.

5.3 Improving the National Cybersecurity Landscape

When an economy defines or has defined their national cybersecurity strategy, it should also refer clearly to national-scale incident management, which goes from prevention, via detection and response, to lessons learned, and then back to prevention. Where incident management is addressed, it should give attention to all organizational aspects as described by SIM3 (the "O" parameters). The mandate of the nCSIRT (and potentially sectoral teams as well - see below) must be formally defined, and sufficient detail about constituents, authority, responsibility, services and associated service levels must be present. Only then will the nCSIRT (and related teams) be able to fulfil their mission in a meaningful way.

Already recognized by all Western Balkans economies, to a knowable extent, is the value of integrating similar approaches and compatible structures as defined in the EU NIS Directive. Additionally, we recommend taking the recognized best practices of how to establish CSIRTs (and SOCs) into consideration – if not already done so.[38]

[38] See e.g. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

We understand that most economies will start to build sectoral CSIRTs and based on our interviews, and we want to underline and stress the need to do so. Especially incidents and attacks within the banking sector and energy sector might require specific attention and activities – and possibly this could also stimulate sector-specific information exchanges within the region. Be aware that it's not just the languages similarities that allow easier attacks on users in various economies, but also it is the case that some banks and energy providers are active in more economies. This will render some attacks and incidents not economy-specific, but rather company-specific, requiring all involved nCSIRTs to cooperate and participate in the incident management.

Under all circumstances the set-up of sectoral CSIRTs and other CSIRTs or SOCs in general will require an integrative approach, which is best facilitated by the national CSIRT. An established best practice is to set up a national forum of incident response teams. Certainly, for those economies with fewer than five teams this might not be an immediate issue. However, the networking between teams inside the economy must be started as early as possible to avoid some kind of vacuum.

A very useful approach would be to share lessons learned and invite other teams to join the exchange of actionable information and monitoring of national threats. That way, insights of various teams in an economy can be processed and utilised to better serve the nations' drive towards increased cybersecurity.

As to information from across the borders, it is usually the nCSIRT that more easily connects to such sources of actionable information (like from SI-CERT or CERT-EU), and then all other CSIRTs and SOCs in the economy can benefit, as they would be members of the trusted collaboration that has been established inspired by their national CSIRT. This double role both within the economy, and outside, can be – and must be – taken on by the nCSIRT. For most other teams in an economy (with few exceptions), it is unlikely that they have the staffing or the position to maintain such a network by themselves.

The nCSIRT's experiences and lessons learned can also be deployed in organizing national exercises and training that fosters national collaboration and expedites information exchange and trust relationships. It is very important to mention here that a lesson learned all over the world is that the nCSIRT can play this role most effectively when they facilitate and enable national cooperation, rather than trying to dominate it. Inspiring leadership is simply more effective, as has been learned time and again in the CSIRT community.

In any case, these unique opportunities require that the national CSIRT is recognized by all stakeholders as relevant and independent to fulfil their mission without inappropriate influence from bias, making it the trusted single point of contact for all concerned for cybersecurity within the nation. Experience also tells that to enable such a role, the nCSIRT functions best when it has a relatively independent position within the civil service, or in an agency. Placing the nCSIRT in more authoritarian or secretive environments is in general not advised.[39]

[39] See [forthcoming in March 2021] Getting started with a national CSIRT, Don Stikvoort and Dutch TNO

6. Summary of Recommendations

In this chapter we summarize the recommendations (R#) made above, keeping the original numbering scheme. For more detail and clarification, see the full texts above.

3.1 International CSIRT Cooperation

3.1.1 Sectoral Cooperation

R1: For those economies wishing to join the EU: as becoming a member of the EU will also involve the cybersecurity aspect, it is useful to work with the higher political levels in Western Balkans economies to see what kind of cooperative approach could be taken towards ENISA and the CSIRTs Network.

R2: Consider joining ISACs, like EE-ISAC for the European energy sector, and the European FI-ISAC for the financial sector.

3.1.2 Transnational Cooperation

R3: All interviewed teams are TF-CSIRT/TI Accredited teams. A strong recommendation is to visit the three annual TF-CSIRT meetings regularly, and budget for that. This is the best way to get involved, build trust and become a valued member of the CSIRT community.

3.1.3 Worldwide Cooperation

R4: All nCSIRTs from the region are mentioned on the NatCSIRT website. We strongly recommend that teams attend the NatCSIRT annual meeting (or apply for that, where needed), when possible again. This usually coincides with the annual conference of FIRST.

R5: FIRST membership is recommended for all interviewed teams – some are already members, while some are in the FIRST Fellowship program.

R6: We strongly recommend attending the annual FIRST conference when possible, and also attend some of the many regional "TC" meetings – or organize a TC in the Western Balkans in cooperation with FIRST yourselves, like SI-CERT did in Slovenia in November 2019.

R7: Consider participation of your economy in the very useful Global Forum for Cyber Expertise (GFCE), that brings together cybersecurity players on all levels from political to corporate, NGOs and CSIRT cooperations like FIRST.

3.2 International Best Practices in the CSIRT Field

R8: Use or consider the following highly relevant international best practices in the CSIRT field (some are already effectively being used by most, like SIM3):

- CSIRT maturity development: SIM3
- CSIRT maturity profiles for national CSIRTs: GCMF
- CSIRT services descriptions: FIRST CSIRT Services Framework
- How to set up CSIRTs and SOCs: new (2020) ENISA guideline document
- CSIRT ethics: Trusted Introducer CCoP and/or FIRST ethics framework
- Traffic Light Protocol: TLP

- CSIRT staff skillsets: CERT/CC's "What Skills Are Needed When Staffing Your CSIRT?"

4.2 Establishing Improved Cooperation and Collaboration

R9: Rather than focusing on a regional type of operational cooperation (no perceived need for this in the interviews we did), we recommend focusing on methods of working together – beyond pre-existing peer-to-peer relationships – to improve the incident management capabilities of all CSIRTs in the region, including national ones, to potentially benefit the whole CSIRT landscape. Examples follow below in R10 to R14.

4.2.1 Regional Meetings

R10: Regular regional meetings would facilitate a natural development of the cooperation potential. These meetings should be not focused on resolving specific incidents in the region, but rather help to share experiences of how to operate effectively in similar political and economic environments, and to discuss and prepare the items of training and other shared initiatives.

4.2.2 Training

R11: Organize regional training, especially technical ones, but also e.g. TRANSITS and SIM3.

4.2.3 Exercises

R12: Organize regional exercises, ranging from highly technical to organizational/procedural ones. Target groups can vary from CSIRTs and other technical security communities to the political and management levels.

4.2.4 Building Trust

R13: Support the building of trust by means of a "council", which could engage CSIRTs from the region and representatives from other regional or global organizations (e.g. FIRST, TF-CSIRT, Open CSIRT Foundation, ENISA, ITU, GFCE et al.) with the goal to promote and help Western Balkans teams to build trust with their most important partners. This could build on work effectively supported by DCAF in recent years.

4.2.5 Information Sharing

R14: Consider creating a "Western Balkans MISP platform" for sharing Indicators of Compromise (IoCs), with feeds from other existing MISP platforms (e.g. SI-CERT, CIRCL). This could also be a testbed for further operational cooperation.

5.2 Improving CSIRT Maturity in the Region

R15: Given the number of open positions in several teams and the difficulty of filling them, we urgently recommend to reconsider those open positions and identify new ways to fill them. This might include creating incentives that attract in particular younger people who have finished university (or similar) studies recently in subjects related to cybersecurity and safety.

R16: Organize independent in-depth SIM3 assessments for reviewing the organizational set-up of teams, as well as the human factors, the tools/technology aspects, and policies/processes/procedures. Use the results to define roadmaps with improvements. Aim to reach the GCMF/ENISA "Intermediate" stage in 1-2 years and apply for TF-CSIRT/TI Certification in 2-4 years (a few teams could apply now already, as they already seem to have reached "Intermediate"). Following on Certification, achieving the GCMF/ENISA "Advanced" stage can be planned.

R17: We recommend that teams develop new capabilities and gain more practical experience. This is not just related to the use of tools like MISP, malware and forensics analysis, or how to improve an existing incident taxonomy to represent incidents of particular industry sectors – but also to gain more practical experience to exercise the workflows, identify flaws and weaknesses in internal processes, as well as difficulties in working with other teams that are important while responding to a cross-border incident or attack. Training and exercises can contribute to this and can be shared within the region (R11 and R12).

5.3 Improving the National Cybersecurity Landscape

R18: Start to build sectoral CSIRTs and ensure that the nCSIRT plays a pivotal role in the cooperation with and between those teams, ensuring proper information sharing and incident reporting.

R19: Ensure that the nCSIRT is well connected internationally and receives important information feeds on IoCs, ongoing incidents and other actionable information – and that the nCSIRT has both the right and duty to spread this information inside the economy to sectoral CSIRTs and other relevant players (ISPs, NREN, etc.).

R20: Ensure that the nCSIRT inspires and facilitates cybersecurity training and exercises inside the economy.

R21: To be truly effective in improving national cybersecurity, we strongly recommend taking into consideration the following two lessons learned worldwide:

- nCSIRTs can be at their most effective when they facilitate and enable national cooperation, rather than trying to dominate it. Inspiring leadership is simply more effective, as has been learned time and again in the CSIRT community.
- nCSIRTs can function and cooperate best when they have a relatively independent position within the civil service, or in an agency. Placing the nCSIRT in more authoritarian or secretive environments is in general not advised.

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