December 2023

A Platform for Sustainable Cybersecurity Cooperation in the Western Balkans

Stiftung
Neue
Verantwortung

Think Tank at the Intersection of Technology and Society

Acknowledgments

Project Lead: Rebecca Beigel
Project Support: Dr. Sven Herpig

This analysis was supported by researcher and practitioner interviews, online collaboration, and a joint workshop on "Identifying the Potential for Regional Cooperation in the Event of Major Cyber Incidents" in Tirana, Albania.

The views and opinions expressed in this paper do not necessarily reflect the official policy or position of the experts or that of their respective employer/s.

In alphabetical order, acknowledging the essential contributions of:

- Erjon Curraj, Science & Innovation for Development
- Rikardo Junčaj, Ministry of Public Administration
- Rexhion Qafa, National Authority on Electronic Certification and Cyber Security
- David Richter, Federal Foreign Office
- Christina Rupp, Stiftung Neue Verantwortung
- Drenusha Salihu, Women4Cyber Kosovo
- Wouter Veenstra, Global Forum on Cyber Expertise
- Orkidea Xhaferaj, Centre Science and Innovation for Development

Additionally, the project team thanks all workshop participants and reviewers, Jasen Ho, Nadine Nagel, Luisa Seeling, Scribendi Editor EM1988, and Alina Siebert, for supporting this publication.

This project was made possible by the generous support of the German Federal Foreign Office and was supported as part of the Berlin Process Initiative to strengthen regional approaches to cybersecurity in the Western Balkans region. The views expressed in this paper do not necessarily represent the official position of the ministry.

Table of Contents

1. Introduction

Recent cyber incidents, such as the 2022 cyber operations targeting the government of the Republic of Albania[1] and compromising the government's IT infrastructure in the Republic of Montenegro[2], have once again emphasized the importance of addressing the issue of cybersecurity in the Western Balkans (WB). The WB is a region at the center of geopolitical and strategic interests. For example, those interests are expressed through the presence and investments of external players such as the European Union (EU)-27, the People's Republic of China, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.[3] The WB are also covered by the EU enlargement policy due to their candidate or potential candidate status for EU membership.[4] Because of these diverse and partly competing interests, the WB is a potential hotspot for cyber operations, such as cyber espionage.[5] Cybercrime is a significant security threat to the region, including malware, phishing, ransomware, and Distributed Denial of Service (DDoS) operations.[6] The region is increasingly digitizing infrastructure and services, thus broadening the attack surface.[7] Therefore, if not appropriately addressed, the problem will only intensify.

Independent from the motivation behind cyber operations, large-scale cyber incidents, such as WannaCry,[8] have taught an essential lesson already in 2017: Cyber threats are not limited to a localized context. Instead, they may transcend borders, spread across sectors, and cause severe harm to economies and societies. At the same time, threat actors interested in the WB, such as cybercriminals, may not limit their activities to one state at a time.[9] Governments and non-governmental enti-

[1] Jason Brodsky (07.09.2022), X; Cybersecurity & Infrastructure Security Agency (23.09.2022): Iranian State Actors Conduct Cyber Operations Against the Government of Albania.

[2] Marash Dukaj (26.08.2022), X.

[3] RCC (26.09.2023): Bregu: A human-centric Europe, with Western Balkans firmly in its fold, is the best investment in peace and security for the entire continent; Branislav Stanicek and Anna Caprile (2023): Russia and the Western Balkans. Geopolitical confrontation, economic influence and political interference, European Parliamentary Research Service.

[4] European Commission (n.d.): EU enlargement; Branislav Stanicek and Anna Caprile (2023): Russia and the Western Balkans. Geopolitical confrontation, economic influence and political interference, European Parliamentary Research Service.

[5] RCC (26.09.2023): Bregu: A human-centric Europe, with Western Balkans firmly in its fold, is the best investment in peace and security for the entire continent.

[6] Metamorphosis (n.d.): A recent look towards Cybersecurity in the Western Balkans: How can we improve the cybersecurity level in the region?; PwC and ISAC Fund (2022): Cybersecurity Ecosystem Report. Western Balkans: Emerging Cyber threats.

[7] PwC and ISAC Fund (2022): Cybersecurity Ecosystem Report. Western Balkans: Emerging Cyber threats; Vesna Tintor, Nikola Jovanović, Veronica Bocarova, and Mihailo Bugarski (2022): Western Balkan Digital Economy and Society Index. WB DESI 2022 Report, RCC.

[8] BBC (13.05.2017): Massive ransomware infection hits computers in 99 countries.

[9] For example, Jamie MacColl, Pia Hüsch, and Jason R. C. Nurse (2022): Beyond the Bottom Line: The Societal Impact of Ransomware, The Royal United Services Institute for Defence and Security Studies; European Union Agency for Cybersecurity (2021): ENISA Threat Landscape 2021. April 2020 to mid-July 2021.

ties across sectors and countries thus face similar challenges in preparing for and responding to these incidents, such as a shortage of cybersecurity skills.[10] This dynamic underscores the importance of addressing cyber threats beyond the national level, for example, by adopting measures to improve national cyber resilience in cooperation with other states.[11] These shared cybersecurity challenges have fueled policy discussions to mitigate them through regional cooperative instruments and initiatives. In the European context, examples of this approach include the recently announced EU Cybersecurity Reserve[12] or the EU Computer Security Incident Response Team (CSIRT) Network[13].

In the WB, the need for a collective approach toward cybersecurity has, for example, been highlighted by the Regional Cooperation Council (RCC), an "all-inclusive, regionally owned and led cooperation framework,"[14] calling for "a joint regional approach to ensure cybersecurity in the region, in line with EU standards."[15] The importance is also underlined by the 2023 chair's conclusions[16] of the Berlin Process, a high-level cooperation platform.[17] The chair's conclusions deem strengthening cybersecurity cooperation essential.[18]

Regional cooperation in the WB is crucial to addressing shared challenges in various aspects and fields.[19] In addition, regional cooperation plays a vital role in stabilizing and associating WB economies with the EU.[20] Regional cooperation is, for example, fostered through the RCC, which, together with the EU,[21] facilitated the Regional

[10] European Union Agency for Cybersecurity (2023): Identifying Emerging Cyber Security Threats and Challenges for 2030.
Aaron Hurst (27.04.2022): Cyber security skills gap contributing to 80% of breaches, Information Age.
[11] Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov (2018): Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms.
[12] European Commission (20.06.2023): The EU Cyber Solidarity Act; European Commission (2023): Proposed Regulation on the Cyber Solidarity Act.
[13] ENISA (n.d.): CSIRTs Network.
[14] RCC (n.d.): About Us.
RCC is a framework that "provides for RCC participants from the SEE, members of the international community and donors to be engaged on subjects which are important and of interest to the SEE with a view to promoting and advancing the European and Euro-Atlantic integration of the region." RCC Board (2013): Statute of the Regional Cooperation Council.
[15] RCC (29.06.2023): Bregu: Regional approach to cybersecurity, in line with EU standards, is a must.
[16] The Berlin Process (n.d.): Chair's Conclusions.
[17] The Berlin Process (n.d.): About Berlin Process.
[18] The Berlin Process (n.d.): Chair's Conclusions.
[19] RCC (26.09.2023): Bregu: A human-centric Europe, with Western Balkans firmly in its fold, is the best investment in peace and security for the entire continent.
Branislav Stanicek and Anna Caprile (2023): Russia and the Western Balkans. Geopolitical confrontation, economic influence and political interference, European Parliamentary Research Service.
[20] European Commission (2022): Commission Implementing Decision of 9.11.2022 on the financing of the multi-country annual action plan in favour of the Western Balkans and Türkiye for 2022.
European Commission (n.d.): Regional cooperation.
European Commission (n.d.): Stabilisation and Association Process.
[21] RCC (n.d.): Stay Charged, Roam Free.

Roaming Agreement,[22] which led to a roaming-free WB and the Berlin Process. Other initiatives that improve regional cooperation include the Regional School of Public Administration (ReSPA), a hub for public administration reform[23] and the South East European (SEE) Digital Rights Network.[24] For regional cybersecurity cooperation specifically, the RCC strengthens cybersecurity capacities in the region and its respective economies, for example, by raising awareness of cybercrime as part of its broader work.[25] Other examples of initiatives are the Center for Cybersecurity Capacity Building in the Western Balkans (WB3C),[26] the projects and initiatives of the Geneva Centre for Security Sector Governance (DCAF),[27] the Global Forum on Cyber Expertise (GFCE),[28] and the e-Governance Academy.[29]

Against the backdrop of these regional cybersecurity initiatives, a common topic emerged in discussions with researchers and practitioners[30]: How could regional cooperation in the WB be improved even further in providing practical operational support, consolidating initiatives, and sustainably increasing the cybersecurity baseline?

In response to that question, this paper explores a path toward sustainable[31] cybersecurity in the WB. Its initial design is a joint platform for WB economies under regional ownership to focus on practical operational support for the conceptualization and development of regional cooperation projects to sustainably increase the regional cybersecurity baseline. Instead of creating another stakeholder from

[22] RCC (2019): Regional Roaming Agreement for the Western Balkans.
RCC (n.d.): Roaming.

[23] European Commission (n.d.): Regional cooperation.
ReSPA (n.d.): Who We Are.

[24] SEE Digital Rights Network.

[25] RCC (2021): See 2030 Strategy.
RCC (n.d.): Trust and security.

[26] Ambassade de France à Podgorica (n.d.): Western Balkans Cyber Capacity Center (WB3C).
Cybil Portal (n.d.): Western Balkans Cyber Capacity Centre (WB3C).
Ministry for Europe and Foreign Affairs (16.11.2022): Montenegro – Center for Cybersecurity Capacity Building in the Western Balkans (16 November 2022).

[27] Such as DCAF's whole-of-government, whole-of-society "Good Governance in Cybersecurity in the Western Balkans" project. DCAF (n.d.): Cybersecurity Governance.

[28] Such as GFCE's (informal) donor coordination meetings, or meetings of the GFCE WB Stakeholder Group (knowledge exchange amongst donors, implementers and WB governments).
For example, Global Forum on Cyber Expertise (2022): GFCE ANNUAL MEETING 2022 REPORT.

[29] Such as the "Cybersecurity Capacity Building in the Western Balkans" project, implemented by the e-Governance academy, amongst others. e-Governance Academy (n.d.): Cybersecurity Capacity Building in the Western Balkans.

[30] These discussions were part of a workshop on "Identifying the Potential for Regional Cooperation in the Event of Major Cyber Incidents" with participants from WB economies, online collaboration, and researcher and practitioner interviews.

[31] In this context, sustainability means the sustainability of implemented projects in the region. A project is considered sustainable "when it continues to deliver benefits to the project beneficiaries and/or other constituencies for an extended period" even after the project period, and thus, donors terminate their funding. Casimiro Vizzini, Alex Da Silva, and Rodrigo San Martín (2017): Deliverable D5.1. Sustainability Plan, European Commission.

scratch, the proposed platform could be embedded in an existing regional institution to leverage existing regional structures, bundle scarce resources, and prevent duplication of efforts. It is intended to benefit the entire WB cyber ecosystem, not just governmental or public institutions. Instead, institutions from the private sector, civil society, and academia would also be encouraged to benefit from it. This paper outlines the platform's potential institutional structure, activities and benefits, potential challenges, and initial steps to take should further exploration of the proposal be considered.

This paper contains an explorative idea intended to be iterative. Further research is necessary to delve deeper into this topic, and valuable feedback from researchers and other stakeholders regarding the proposed platform is greatly appreciated. If the implementation of the platform is considered, it should be further refined and adapted to the specific needs and interests of the national and regional actors involved.

2. Platform for Sustainable Cybersecurity Cooperation in the Western Balkans - Explanation and Benefits

Regional cooperation in cybersecurity is essential to maximize the efficient use of resources[32] such as IT security staff, threat intelligence, or funding. The proposed Platform for Sustainable Cybersecurity Cooperation could be a joint instrument for WB economies under regional ownership. Its defining feature is the emphasis on regional cooperation projects[33] that either cultivate collaborative regional efforts or tackle common challenges, ideally benefiting more than one WB economy and, thus, multiple stakeholders in the region. Its primary aim is to provide tangible, practical support to WB economies for regional cooperation projects, while sustainably increasing the cybersecurity baseline and embedding them in a comprehensive platform-specific roadmap. **The platform should not be envisioned as an implementing entity for regional cooperation projects, but as a mechanism to enhance such project concepts.**[34]

Upon request, the platform would thus extend **practical support to WB states in formulating, developing, and refining regional cooperation projects.** Additionally, it is intended to furnish an **overview** of the requirements and collective challenges commonly faced by regional institutions, but most importantly, of existing and planned regional cooperation projects. This approach aims to **enhance efficiency** by streamlining efforts and reducing the duplication of activities for regional cooperation. Furthermore, the platform can potentially promote access to an **extensive network of stakeholders** that may contribute to project advancement and prospective implementation. This network, for example, encompasses cybersecurity experts affiliated with the platform or with implementing organizations. These experts may be consulted to advance project proposals or as potential implementing partners for the prospective implementation of projects.

[32] GFCE (2017): Global Good Practices. [website deleted]

[33] An illustrative project idea conducive to regional cooperation could involve the establishment of a regional (sectorial) CERT platform that connects (sectorial) CERTs or CERT-like structures. Such a project would focus on enhancing operational-level regional cybersecurity cooperation. Another exemplary initiative could revolve around regional cyber security competitions, exercises and training - focusing on fostering shared educational experiences.

[34] These may, for example, include preliminary and comprehensive outlines of proposed initiatives, delineating potential objectives, scope, methodologies, and anticipated outcomes of a potential project on regional cooperation. They may further include other elements, such as the identification of key stakeholders, anticipated challenges, resource requirements, a description of relevance and the potential project impact. Such concept documents may represent the initial stage in the project planning process, offering a basis for further refinement and development before the formal initiation of the project.

2.1 Institutional Structure

The proposed platform could be incorporated into an existing regional organization. Doing so would use regional institutional and legal structures efficiently and guarantee regional ownership, legitimacy, and regional agency while avoiding creating another stakeholder from scratch.[35] For example, it could draw on existing legal frameworks and memoranda of understanding.

Functionally, the platform should be considered an administrative secretariat, exercising a liaison function between various economy-specific, regional, and international actors integrated into a regional organization. That administrative secretariat would be the focal point for communication with all involved parties and would provide practical support, among other tasks as outlined in the section on platform activities. It is **not an implementing entity, but can be understood as a mechanism that drives the conceptualization and development of regional cooperation projects.** The questions that may guide the secretariat's work may be:

a) How can a project idea be developed to optimize its capacity to foster regional cooperation or effectively address shared challenges within the defined project scope?
b) Can the project leverage existing efforts? Are there connections to ongoing initiatives within the region?
c) Which funding sources could potentially provide financial backing for the project, if required? Additionally, which implementing organizations possess the capacity to offer support and expertise for project execution and serve as suitable partners for the project duration, if necessary?

The regional institution into which the platform is integrated would be responsible for staffing it with appropriately skilled personnel, starting with a small core team. Due to the nature of its work, the secretariat's staff may comprise administrative personnel and subject matter experts specializing in cybersecurity, cyber capacity building (CCB), and regional cooperation. Administrative personnel may assume responsibility for communication matters and liaise with various stakeholders. Concurrently, subject matter experts would collaborate with WB economies to enhance incoming project proposals. Staff members could have permanent or temporary contracts (it may, for example, be feasible to hire consultants for a defined period). Additionally, staff from other institutions may be seconded to bolster staffing levels (e.g., from CCB-organizations internationally or economy-specific entities from the WB). Stakeholders that would be in some way connected to the secretariat include:

[35] One of several options of such an institution could, for example, be the Regional Cooperation Council. RCC (n.d.): About Us.

Designated Contacts: Each WB economy can appoint a so-called Designated Contact responsible for interacting with the platform, appointed by the respective government. The Designated Contacts may be the economy-specific entity overseeing cybersecurity, such as the cybersecurity agency or relevant ministries specializing in information and telecommunications. This ensures political buy-in and commitment. Some governmental Designated Contacts may not be viable for reasons such as institutional maturity, challenges in governance structure, or insufficient political backing. In such cases, alternative stakeholders, be they non-state institutions or individuals with the capacity to spearhead cooperation, could be appointed by a particular economy to assume this role.

The Designated Contacts serve as intermediaries with the dual purpose of establishing a centralized point of communication for all WB institutions seeking to utilize the platform and providing a point of reference for consultations with the administrative secretariat.[36] This approach streamlines resources and facilitates a standardized approach.

Moreover, Designated Contacts may initiate their own projects or collaborate with counterparts from other economies. They may also play a pivotal role in disseminating information about the platform and its advantages within their respective WB economies and entities across all sectors (e.g., through knowledge-sharing initiatives). This outreach is crucial for amplifying awareness that institutions from the private sector, civil society, and academia are also eligible to submit project proposals to the platform through their respective Designated Contact.

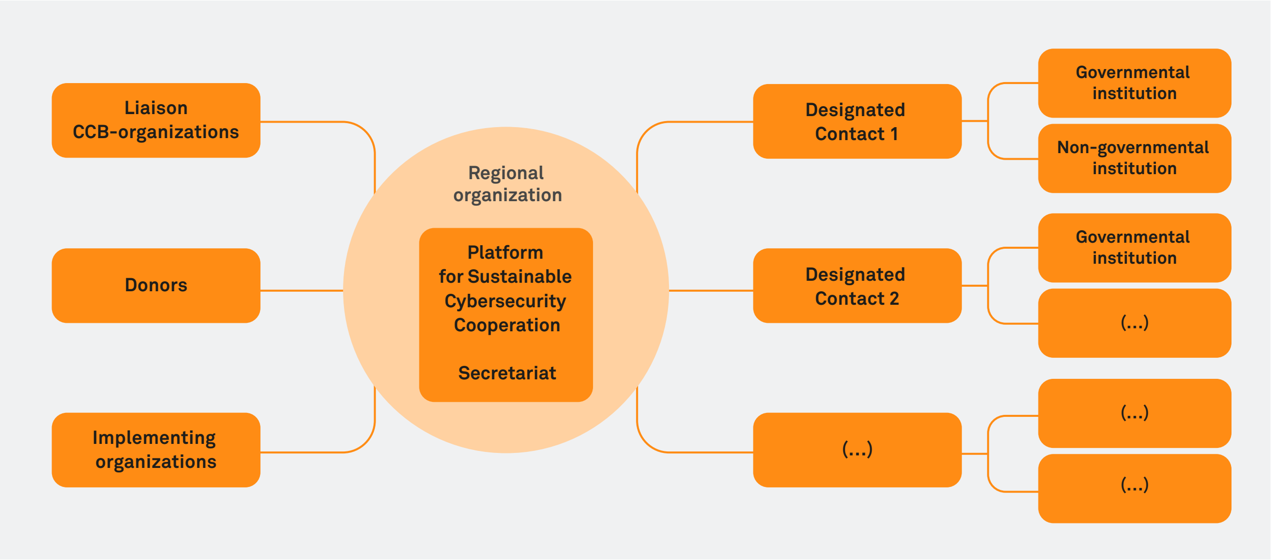
Economy-specific institutions: Entities from all governmental and non-governmental sectors may submit project concepts on regional cooperation through their respective economy-specific Designated Contact.

Donors and implementing organizations: If requested by the Designated Contact, the platform may forward project concepts to funding and implementing organizations from the WB and beyond that could contribute resources, such as funding or expertise, should the project be implemented. This could further assist with the development of the initiative. If there is interest, informal talks between these stakeholders and the Designated Contacts may follow. The ultimate determination regarding the incorporation of these institutions and their resources, including funding and expertise, in the subsequent phases of the project lies with the originators

[36] The staff of the Designated Contact should be provided by the office acting as Designated Contact and must be increased accordingly to be able to fulfill these tasks.

of the project concept[37] and the respective funding or implementing organizations reached through mutual consensus.

In addition, a **liaison with cyber capacity building organizations** for a defined period may be considered.



Architecture of the Platform for Sustainable Cybersecurity Cooperation

2.2 Platform Activities

The proposed platform may add value through the following activities:

a. Practical operational support in enhancing projects of regional cooperation.
b. Improvement and assurance of the sustainability of projects.
c. Development of a roadmap to guide the platform's work.

These activities are suggested, but may be adapted and further refined to the specific needs and interests of the national and regional actors involved.

[37] Originators of such concepts encompass (a) the entity serving as the Designated Contact, which is the institution authorized by each WB state to liaise with the platform on behalf of other entities, (b) a consortium of Designated Contacts, or (c) economy-specific governmental and non-governmental institutions that interface with the platform through their Designated Contacts.

2.2.1 Practical operational support to enhance regional cooperation projects

The platform is designed to operate on a **demand-driven basis** and would be activated only upon engagement by WB economies, presenting an (initial) project concept on regional cooperation. The sooner the platform engages through a Designated Contact, the more advantageous it will be. This early engagement allows consultations during the initial deliberative phase, which can then be refined and developed collaboratively. The key to its work is guiding projects toward a path that contributes significant value to regional cooperation. Practical operational support may be provided in the following ways:

Project design and planning: The secretariat may assist in the conceptualization, development, and planning of projects on regional cooperation, helping to define objectives, scope, and outcomes in alignment with its roadmap while making them sustainable (see hereafter). This support is provided to streamline and consolidate initiatives (thus funding). Hence, the project design and planning consider ongoing regional efforts, ensuring that the project complements and enhances existing collaborative endeavors. Publicly available resources from GFCE[38], EU Cyber Net,[39] and close consolidation with other stakeholders, such as RCC,[40] may help establish an overview of regional initiatives. The project design and planning process is done in close coordination with the respective Designated Contact(s) and is an iterative process.

Expertise: Through its own personnel and a network of additional subject matter experts—who, for example, work in implementing organizations—the secretariat may be able to offer access to expertise in areas relevant to the project, providing guidance on subject-related questions, best practices, methodologies, among other aspects.

Resources: The secretariat may help identify resources needed to further enhance a regional cooperation project, such as funding or expertise. The secretariat could help identify relevant stakeholders—such as donor and implementing organiza-

[38] Such as the Cybil knowledge-sharing portal that provides an overview of projects and actors in a particular economy or for certain beneficiary groups, such as the Western Balkans. Cybil (n.d.): The Knowledge Portal for Cyber Capacity Building.

[39] EU CyberNet has published a CCB project mapping tool, focusing solely on external CCB projects funded by the EU or EU Member States. These can, i.e., be filtered by geographical areas, such as the Western Balkans and Turkey, or allow to see whether projects are bilateral, regional or global. EU CyberNet (n.d.): CCB Projects mapping. EU-funded and EU Member States (MS) funded external cyber capacity building projects in the third countries.

[40] RCC (n.d.): About Us.

tions—or may support applications for public funds or calls for proposals[41] at the economic or international levels (e.g., at the EU level) if applicable. To allow for this, the platform should continuously work on expanding its network of institutions from its implementation. This can be achieved, for example, through proactive outreach to institutions and subsequent trust-building, through participation in conferences and events with a thematic connection to cybersecurity in the WB, or through exchanges with other cyber capacity-building actors such as GFCE[42] and EU CyberNet.[43]

Coordination: After identifying and engaging relevant stakeholders—such as donors and implementing organizations—the secretariat may foster collaboration, if necessary, and ensure that all parties are informed and involved in project development, if applicable. It may further assist in organizing informal meetings with relevant stakeholders to define the project further. In the event of disagreements or challenges during project development, the secretariat may serve as a neutral mediator, helping to find mutually agreeable solutions. The final decision about including stakeholders and their resources (such as funds or expertise) in the further course of the project rests with the originators of the project idea—the Designated Contacts or economy-specific institutions and the respective funding or implementing organizations by mutual agreement. The platform, therefore, does not endorse a competitive approach among economy-specific Designated Contacts, as it abstains from arbitrating the allocation of funding or expertise.

Legal and regulatory guidance: The secretariat may help navigate relevant legal and regulatory frameworks, ensuring that the project complies with regional and international standards.

Document preparation: The secretariat may further aid in developing project documents, including proposals, agreements, and progress reports, facilitating clear communication and documentation of project activities.

Monitoring and reporting: The secretariat may assist in establishing monitoring and evaluation systems, collecting data, and preparing regular progress reports to track project implementation and impact. By providing practical operational support in these ways, the secretariat plays a crucial role in ensuring the smooth and effective development of regional cooperation projects, enhancing their chances of success and impact. The platform's practical support is only activated when requested by the Designated Contacts; hence, it is entirely demand-driven. The level of practi-

[41] An example for a Call for Applications: SMART Balkans (31.05.2023): Call for Applications – Regional Grants.
[42] GFCE (n.d.): Strengthening cyber capacity and expertise globally through international collaboration.
[43] EU CyberNet (n.d.): EU CyberNet – the bridge to cybersecurity expertise in the European Union.

cal support depends primarily on the needs of the Designated Contacts, which are supposed to benefit from this activity. The platform should support Designated Contacts with as little bureaucracy as possible to avoid additional hurdles.

2.2.2 Improvement and Assurance of Project Sustainability

Additionally, the platform may contribute to the sustainability of regional cooperation in the WB. First, the path toward the platform itself can be considered a sustainable cyber capacity measure. The platform may contribute to the sustainability of regional cooperation through its administrative center, its persistent collaboration with Designated Contacts (and thus with economy-specific institutions), and the development of a consistent network of institutions that may contribute resources to projects on regional cooperation, such as donors and implementing organizations.

In addition, the platform may help to improve the sustainability of the proposed projects on regional cooperation. From the moment Designated Contacts approach the platform with a project idea, the platform should consider the project's sustainability and actively support them in improving initial project ideas. Sustainability can be achieved by prioritizing open-source software over proprietary solutions so that third parties can be under contract in the future[44] – for example, for further development and improvement of existing solutions.[45]

2.2.3 A Roadmap to Guide the Platform's Work

Another suggested activity of the platform, which goes beyond practical support, could be to develop a roadmap that specifies the platform's own work priorities and the direction of its activities in a specified period. The roadmap would provide the backbone for the platform's operational support. The document may further enhance the platform's work and help to prioritize its activities. For example, when developing a project, the roadmap would make it possible to showcase to Designated

[44] For example, Sven Herpig (2023): Fostering Open Source Software Security Blueprint for a Government Cybersecurity Open Source Program Office.

[45] For example, the United Nations Sustainable Development Goals (SDGs) could be used as guidance to capture whether projects for regional cooperation are sustainable. This logic could classify projects as sustainable if they align with certain SDGs. In particular, SDG 8, "Decent work and economic growth", SDG 10 "Reduced inequalities", or SDG 17 ", Partnerships for the goals" could be central to this. Targets and indicators can be found on the respective websites and could be adapted accordingly by the platform. In addition, one could also look at cybersecurity projects in the region that have already achieved sustainability and analyze how they were able to do so.
United Nations (n.d.): The 17 Goals.

Contacts which key topics are relevant for regional cooperation during the project period.

The platform's administrative secretariat may develop the roadmap in close coordination with the Designated Contacts. Existing roadmaps of institutions and projects from other regions can serve as examples.[46] A possible approach to developing the roadmap could be identifying topics or aspects of regional cooperation that could or should be promoted in the short, medium, and long term. The platform could deprive these topics of the regional threat landscape or expected trends.[47] In addition, regular evaluations should already be planted into the roadmap so that improvements can be initiated if necessary. The platform's administrative secretariat could, for example, achieve this goal by developing clear project objectives for each topic category, defining possible results (such as outputs and outcomes) and SMART[48] indicators, or similar metrics, for each respective result, identifying stakeholders that potentially contribute to achieving the objectives, assessing potential risks to the development of the categories, and establishing monitoring and evaluation mechanisms.[49]

[46] For example, CONCORDIA (2022): Work Package 4: Supplement to Deliverable D4.4: Cybersecurity Roadmap for Europe.
Danielle Santos, Sanjay Goel, John Costanzo, Debbie Sagen, and Patty Buddelmeyer (2020): A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce, National Institute of Standards and Technology.

[47] PwC and ISAC Fund (2022): Cybersecurity Ecosystem Report. Western Balkans: Emerging Cyber threats.

[48] The abbreviation SMART stands for: specific, measurable, assignable, realistic, and time-related. Doran (1981): There’s a S.M.A.R.T. Way to Write Management’s Goals and Objectives.

[49] For example: Dawn Roberts and Nidhi Khattri (2012): Designing a Results Framework for Achieving Results: A How-to Guide. Washington, D.C.: World Bank Group.

3. Challenges

There are region-specific and platform-specific challenges that could affect the process of establishing the Platform for Sustainable Cybersecurity Cooperation in the WB. Their significant influence on the platform's concept and future implementation, if this should be considered, is acknowledged.

Region-specific challenges may include the following:

a) Political commitment and buy-in of the respective WB economies are essential to building the platform. At the outset, the political support of two or three economies may be sufficient to take initial steps toward further development of the platform.
b) Political (bilateral) disputes may influence the implementation of this or similar ideas.
c) There is a shortage of IT and cybersecurity specialists.[50]
d) The varying maturity levels and capacities[51] of the cybersecurity entities in the respective WB economies and other (political) institutions may affect the platform's further development.
e) Each WB economy has a unique political and economic landscape, including, for example, legal and strategic frameworks, unique decision-making bodies, and different stages of digitalization.

Platform-specific challenges may include, among others:

a) (Further) reinforcement of regional authority and leadership, notwithstanding the platform's envisioned integration into a regional entity.
b) Allocation of required financial resources to establish initial roles within the administrative secretariat of the platform.
c) (Further) reinforcement of regional authority and leadership, notwithstanding the platform's envisioned integration into a regional entity.
d) The funding of (additional personnel) necessary to fulfill the activities of the Designated Contacts, should this not be feasible through the organization representing the Designated Contact.
e) The selection of Designated Contacts in instances where several institutions are vying for the position. Determining which entity should be mandated to make this selection should be subject to critical review. One potential avenue could be the economy-specific entity in charge of cybersecurity, among other options.

[50] For example, Alina Clasen (2023): Summit highlights digital shortcomings in Western Balkans.
For example, Dražen Maravić (n.d.): Cybersecurity Policy Development and Capacity Building – Increasing regional cooperation in the Western Balkans.

[51] For example, Fabio Barbero and Nils Berglund (2021): Cybersecurity Capacity Building and Donor Coordination in the Western Balkans.
For example, Global Cyber Security Capacity Centre (2023): CMM Reviews around the World.

Should the platform be explored further, and implementation considered, the challenges above become pivotal in its conceptualization. Some challenges will endure to some extent, while others may be mitigated during the initial design phase. Consequently, the proposed platform should be regarded as a medium-to long-term project in a region of strategic significance, given the geopolitical dynamics at play.

4. Initial Setup

The initial steps toward implementation include, but are not limited to, the following:

1. Identify a governmental or non-governmental entity or person in each of the WB economies that serves as an initiator to promote the platform. As previously discussed, the initial political support of two or three economies may be sufficient to take these initial steps toward platform development.
2. Gather political support to further promote steps toward the platform in the respective economy by that entity or person.
3. Designate an economy-specific contact to liaise with the platform by the respective WB economy—possibly through the economy-specific entity in charge of cybersecurity. As discussed, governmental Designated Contacts would guarantee political commitment. However, non-governmental Designated Contacts may spearhead cooperation if governmental Designated Contacts are not feasible.
4. One of the Designated Contacts would present the idea to a regional organization that could prospectively house the platform when established.
5. Establish a working group within the regional organization to advance the establishment of the platform.
6. Staff the positions for the administrative secretariat by the working group. Secondments from other organizations may also be necessary to increase staffing levels.
7. The working group would develop a public communication strategy to convey the platform's benefits and spread the message to the WB economies.
8. Contact between the working group and cyber capacity building stakeholders to explore synergies and links with the platform and its administrative secretariat through, for example, a liaison officer.

5. Outlook

There is a need for regional cooperation in the WB to counter the threat of malicious cyber activities, particularly when resources, such as skilled workers, are limited. One means to foster regional cooperation could be a Platform for Sustainable Cybersecurity Cooperation in the WB.

In its initial design outlined in this paper, the platform would bring several benefits to WB entities while upholding regional ownership. They include tangible, practical support in the conceptualization, development, and planning of regional cooperation projects; an overview of existing and planned regional cooperation projects to strengthen regional cooperation; and increased efficiency, as coordination through the platform may lead to streamlined initiatives and less duplication of efforts. In addition, the platform would ease access to an extensive network of stakeholders, from subject matter experts to potential funders. This resource could be harnessed for project advancement and prospective implementation and could enable further enhancement of regional project sustainability while embedding activities in a platform-specific roadmap. The platform should not be considered a newly established, independent structure, but rather an instrument integrated into the existing regional organization to guarantee resource effectiveness.

There are many challenges to implementing the platform, such as different maturity levels of political institutions in the WB and the necessary political commitment of WB economies. Additionally, even better integration of multiple stakeholders from the respective WB economies, such as entities from the private sector and civil society, should be further explored. These aspects will undoubtedly factor into further exploration of the platform and should not be underestimated. If further exploration of the platform is considered, it should be classified as a medium- to long-term project. However, if thoughtfully considered, the platform may contribute to sustainably fostering regional cooperation in cybersecurity in the WB.

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent, non-profit think tank working at the intersection of technology and society. The core method of SNV is collaborative policy development, involving experts from government, tech companies, civil society and academia to test and develop analyses with the aim of generating ideas on how governments can positively shape the technological transformation. To guarantee the independence of its work, the organization has adopted a concept of mixed funding sources that include foundations, public funds and corporate donations.

Contact:
info@stiftung-nv.de

Imprint

Stiftung Neue Verantwortung e.V.
Ebertstraße 2
10117 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97
https://www.stiftung-nv.de/en
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Thorsten Kirchhoff