

High Level Regional Conference

***Cyber Resilience and Cybersecurity Capacity Building
in the Western Balkans***

3-5 March 2021

**Cybersecurity Policy Development
and Capacity Building -
Increasing regional cooperation in
the Western Balkans**

Discussion Paper, Panel 2

Contents

EXECUTIVE SUMMARY	2
INTRODUCTION	3
COUNTRY OVERVIEW	7
<i>Albania</i>	7
<i>Bosnia and Herzegovina</i>	9
<i>Kosovo*</i>	10
<i>Montenegro</i>	11
<i>North Macedonia</i>	12
<i>Serbia</i>	13
REGIONAL OVERVIEW	14
WAY FORWARD	17

EXECUTIVE SUMMARY

The Declaration of 2020 Zagreb Summit between the European Union (EU) and Western Balkan leader notes that so-called hybrid activities originating from third-state actors, including disinformation around COVID-19, have become increasingly prevalent in the Western Balkans. Such incidents expose the vulnerability of societies and infrastructure to cyberattacks, cybercrime and hybrid threats. The Declaration calls for increased cooperation to address disinformation and other hybrid activities.

* 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.

The Digital and Green Agenda for the Western Balkans, the Regional Cooperation Council (RCC), the Regional School of Public Administration (ReSPA) and other regional initiatives provide a general framework for enhanced cooperation. Many international actors have supported cybersecurity in the Western Balkans over the years. Countries of the region are also aware of the benefits of regional cooperation. Closer regional collaboration will therefore be beneficial for resilience building, enhancing cybersecurity and strategic communication. The cybersecurity workforce shortage and skills gap are also significant concerns for the economic development and national security, especially given the rapid digitization of global and regional economies. Besides, slow progress in public administration reforms is hindering progress in cybersecurity development.

With clear political support and shared ownership, it would be possible to create more vital regional collaboration, facilitated by a customized joint framework in the form of a regional hub. Western Balkan economies could have a regional framework for cooperation committed to supporting and strengthening cybersecurity strategies, policies, and competence at all levels of public administration, from non-experts to highly skilled professionals. Besides, this regional framework could support economies of the region in raising citizens' awareness of cybersecurity and potential cyber threats and speed up aligning countries' alignment with the EU acquis.

Economies of the region could task the potential regional cybersecurity hub to operate across areas which are within the usual practices of national cybersecurity authorities, and with a focus on:

1. Providing thought leadership and strategic development **direction and analysis** in the cybersecurity space.
2. Raising cybersecurity **awareness** at all levels of government.
3. **Sharing** information, expertise, and knowledge; and
4. Establishing and promoting **best practices** based on common challenges.

Finally, joint activities in this area could potentially count on more considerable donor support if the Western Balkan economies themselves contribute and create greater sustainability of regional cooperation activities.

INTRODUCTION

The COVID-19 pandemic is a global shock that has not spared the Western Balkans (WB). The final extent of its footprint in terms of loss of human lives and damage to the economy is still difficult to assess. However, early estimates foresee a drop of between 4% and 6% of gross domestic product



in the region. During the COVID-19 crisis, inclusive regional cooperation has proven essential.¹ At the Zagreb Summit on 6 May 2020, the European Union (EU) and Western Balkan leaders agreed that deepening regional economic integration has to be a prominent part of the Western Balkans recovery efforts.² Such a common regional market must be inclusive, based on EU rules and built on the regional economic area multi-annual action plan's achievements.

The Zagreb Summit Declaration noted that hybrid activities originating from third-state actors, including disinformation around COVID-19, have become increasingly prevalent in the Western Balkans (and Turkey). Such incidents expose the vulnerability of societies and infrastructure to cyberattacks, cybercrime and hybrid threats. As stated in the Zagreb Declaration, the EU will increase its cooperation with Western Balkan economies to address disinformation and other hybrid activities. Closer collaboration is therefore much needed in resilience building, cybersecurity and strategic communication. The cybersecurity workforce shortage and skills gap is a significant concern for economic development and national security, especially in the global and regional economy's rapid digitization.

There are different opportunities for enhanced regional cooperation. The starting point for this deliberation could be to maintain the status quo. One dimension is to continue with the usual bilateral exchanges between the countries in the WB region and third countries. Secondly, existing regional forums could be used for joint activities, mainly regarding research activities. This has been the case so far within this field, particularly by the Regional Cooperation Council. Bilateral and multilateral donors could continue to provide support to individual countries, but this could lead to parallel rather than joint capacity development. Also, existing differences between the countries and slow pace of EU integration prospects for the region as a whole, could be reinforced if they continue to develop national capacities for cybersecurity at their own pace, without the (additional) possibility of making larger steps together.

Whilst maintaining the status quo, it would be possible to create more vital regional collaboration, facilitated by a customized joint framework. Western Balkan countries could have a regional framework for cooperation committed to supporting and strengthening the enhancement of cybersecurity strategies, policies, and competence at all levels of public administration, from non-experts to highly skilled professionals. Besides, this regional framework could help raise citizens' awareness of cybersecurity and potential cyber threats (e.g. phishing attacks, botnets, financial and banking fraud, data fraud). It would be possible to design regional information campaigns and to support potential national ones, as demonstrated by the DCAF regional project. Such a framework could guide acceptable practices to promote safer online behaviour (e.g. cyber hygiene and cyber literacy) using both good and bad examples from any country in the region.

¹ 2020 Communication on EU enlargement policy, Brussels, 6.10.2020 COM(2020) 660 final.

² Zagreb Declaration, 6 May 2020. <https://www.consilium.europa.eu/media/43776/zagreb-declaration-en-06052020.pdf>

Furthermore, a regional effort could help to speed up aligning countries' actions with the EU acquis, and engage in promoting and analysing cybersecurity academic and professional education by dividing efforts and specializations among the nations in some way. Finally, all countries in the region suffer from similar challenges, such as a shortfall in cybersecurity skills, which could jeopardize both national security and economic development. Since there are multiple efforts to approach the region's economic growth, such as the mini-Schengen initiative, the Green Agenda for the Western Balkans and others, it is reasonable to conclude that the same approach could work for cybersecurity as well. Regional cooperation is vital if the economies in the region move more rapidly towards digitalization and e-commerce. This policy paper aims to document the key features of existing regional cooperation in public policy development and civil servant capacity building, focusing on institutions in charge of cybersecurity policy development and incident response, whilst providing policy advice for future improvements.

Public administration reform (PAR) is essential for improving governance at all levels.³ Such reform includes increased transparency and accountability, sound public financial management, and administration of a more professional nature. The existing capacities for governmental cybersecurity policies are strongly related to the countries' general public administration reform developments. Modest effects concerning PAR (in areas such as public policy drafting and implementation, accountability, human resources management, and professional development of civil servants), are influencing cybersecurity policies, capacities of lead institutions, and cybersecurity incident handlers.

The annual EU assessment⁴ is that Albania, North Macedonia, Montenegro, and Serbia are only moderately prepared regarding public administration reform. In Serbia no further progress has been made, as the number of acting senior manager positions remains excessive, rather than being reduced. Kosovo* has achieved some level of preparation, while Bosnia and Herzegovina is at an early stage. There has been some progress in improving policy planning, but further efforts are needed in all countries to ensure substantial central government quality control. Montenegro has strengthened and rationalized policy planning and achieved a reduction in the number of strategic documents. Policies, legislation and public investments are still often prepared without impact assessments.⁵ Managerial accountability and professionalization of the civil service still need to be ensured in most countries, and excessive politicization has to be addressed. Transparent and merit-based procedures for recruitment, promotion, demotion and dismissal need to be embedded in the legislative frameworks and consistently implemented across public services. The structure of the state administration should ensure effective lines of accountability. Most countries have made efforts to improve services to citizens and businesses, especially in the area of e-service delivery.⁶ The EU has concluded that enhanced inter-institutional coordination is needed to fully implement public administration reforms in the Western Balkans.

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0260>

⁴ 2020 Communication on EU enlargement policy, Brussels, 6.10.2020 COM(2020) 660 FINAL.

⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0260>

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0260>

National authorities focusing on cybersecurity should base their work on strategies and action plans developed in an inclusive process that benefits from input from academia, the business sector and civil society organizations. They should have significant human resources, both in terms of numbers of personnel and competences, and rely on a solid retention policy to enable long-term developments to be put in place. Public administrations have always been information-processing organizations. In general, public administration bodies must have IT-related business processes that are secure by design and a high level of related knowledge for all members of the public administration. Clear accountability and reporting lines for staff are essential, and for all senior managers dealing with sensitive public information and personal data. Public organizations are dealing with a high volume of sensitive data and many have vulnerable cyber defences, which in some cases poses a risk for regional government organizations and the public sector in general. Furthermore, digitalization of public administration services is a vital priority for Western Balkan countries. The more government organizations embrace technology, the more exposed they are to threats in cyberspace. Nowadays, digital government agendas worldwide seek to keep abreast of digital networking and digital changes in a society based on information technology. Ever-increasing digitalization leads to fundamental changes in the business processes of public administrations as they try to offer customer-friendly services to citizens and businesses.

Considering this, governments need to implement new safeguards in the form of continuous information security and legally compliant data protection. Cybersecurity measures are continually improving. Just as criminals are developing unknown attack vectors, firewalls, encryption and other security measures are becoming more robust. It would be a mistake, though, to think of this as a primarily technology-related issue. The greatest weakness of public organizations will always be the human factor. The biggest threat will usually come from within – either from a malicious action or a fundamental human error.

Attacks are still mostly due to someone making a mistake – either revealing information through an email or clicking on a suspicious link.⁷ Therefore, the most crucial tool for protecting internal systems is to ensure that staff are adequately trained. This can be initiated by developing a comprehensive training programme for everyone from top-level management to the most junior office assistants. They must realize the importance of following security protocols.

The Western Balkan governments should develop robust frameworks for cybersecurity, in line with EU standards, including adopting strategies and action plans. Since the EU prescribes frameworks which are continuously being developed (for example, the EU announced a new cybersecurity strategy⁸ in December 2020), countries would benefit from following these developments and ‘moving targets’ set by the EU. The role of line ministries is to ensure a functional legal framework in line with EU legislation and cybersecurity strategies. Still, there is usually a delay in the harmonization process, due to the heavy normative agenda, political processes, frequent calls for

⁷ <https://www.itsecurityawareness.ie/public-administration>

⁸ https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

early elections, and other challenges, including the lack of civil service members skilled in cybersecurity. Besides, line ministries should ensure an adequate level of human resources for the competent authorities to ensure effective cybersecurity, such as computer security incident response teams (CSIRTs). As defined by the Directive on security of network and information systems, the national competent authorities, which may differ from the line ministry in charge of public administration, should ensure proper cyber resilience and capacity to deal efficiently with threats and attacks. Since public administration reform requires a strong focus on multiple divergent issues (for example, capacity building vs downsizing within the civil service), this could prove a demanding task for national administrations struggling to enable better horizontal cooperation and a whole-of-governance approach to reforms. Reinforced regional cooperation could prove useful to keep the momentum of capacity building in cybersecurity, if some countries at a given moment focus more towards downsizing their administration or decreasing wages in order to maintain fiscal stability. The competent authorities could provide more efficient regional cooperation, and with the EU, when supported by a new or enhanced regional framework for collaboration with the line ministries.

The function of all CSIRTs in the six Western Balkan countries is very similar, which is unsurprising. They have all been structured primarily in line with European Union Agency for Cybersecurity guidelines.⁹ Therefore, it seems that a regional approach makes sense because leading institutions with similar functions and setups already exist. A single regional effort could provide momentum and quality assurance in cybersecurity policies and practices in such an environment.

COUNTRY OVERVIEW

Albania

Albania¹⁰ is moderately prepared in the reform of its public administration. Still, it continues to make efforts in several related areas. Albania has achieved progress in enforcing the guidelines on regulatory impact assessments across line ministries, developing the legislative package related to policy planning, increasing the number of e-services, and improving transparency in data collection and human resources management between the central and local levels. Managerial accountability is not yet protected in the legislation and in administrative practice. Decision making in the institutions is centralized and, in practice, a minimal number of decisions are delegated. Vertical accountability is very weak between policy-making and policy-implementing entities. Governance arrangements ensuring strategic plans with defined objectives, performance indicators, and precise monitoring and reporting lines between parent ministries and subordinated agencies, are still lacking.

⁹ <https://www.enisa.europa.eu/>

¹⁰ Based on the 2020 EU Progress Report for Albania, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/albania_report_2020.pdf, and Report on Cybersecurity Maturity Level in Albania, <https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf>

The EU specifies in the progress report for 2020 that Albania should¹¹ establish a more effective law-enforcement response focusing on the detection, traceability and prosecution of cybercriminals and address the growing phenomenon of child pornography online.

The Albanian School of Public Administration's (ASPA) training programmes contribute to the professional development of civil servants. However, an integrated training management cycle still needs to be established. The ASPA has developed two training courses on computer security, a 3-day introductory course and a 2-day advanced learning course. Within the public institutions, training on cybersecurity issues for IT staff and general staff is minimal. It often depends on the institution's individual management policy, to determine whether a specific staff member can attend an available cybersecurity training or certification course. Internationally accredited IT security and governance training and certification courses are being offered in Albania. As mentioned by the review participants, the perception of cybersecurity held by the private sector boards and CEOs requires significant improvement. Another concern shared by the participants is the challenge of retaining security professionals within Albania, as they often leave the country to seek better opportunities in the EU or in North America.¹²

The Law 'On Cyber Security' is only partly aligned with the EU Directive on security of network and information systems (NIS Directive). Albania has established a list of critical information infrastructures and the necessary implementing legislation. In 2019, the National Authority for Electronic Certification and Cyber Security (AKCESK) drafted a national cybersecurity strategy that still needs to be adopted. Albania's commitment to cybersecurity and cyber resilience has notably progressed after adopting various national digital transformation and national security strategies. Three central authorities are responsible for different parts of incident response in Albania. The Ministry of Defence (MoD) is responsible for handling cyber incidents related to the MoD and the air force. The Cybercrime Investigation Unit of the Albanian State Police and the prosecutor's office addresses cybercrime. However, the AKCESK serves as the official national coordinating body to report and manage cybersecurity incidents for key information infrastructures and critical information infrastructure operators.

The Law No. 2/2017 'On Cyber Security' defines Critical Information Infrastructures as well as Important Information Infrastructures and their responsibility for reporting incidents.

A national programme for raising cybersecurity awareness, led by designated organizations (from any sector) which addresses a wide range of demographics, is yet to be established. In the last few years, Albania has periodically carried out awareness activities for a safer internet and participated in activities on international Safer Internet Day. Albania celebrates October as cybersecurity awareness month. One successful initiative is the Albanian Cyber Academy, whose last (4th) edition, in 2020, was supported by DCAF.¹³ Moreover, there is a week in March that is dedicated to child

¹¹ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2020:354:FIN>

¹² <https://cybilportal.org/wp-content/uploads/2019/10/AlbaniaCMMReport.pdf>

¹³ https://cesk.gov.al/publicAnglisht_html/aktivitete/aca4.html

cybersecurity. The officially recognized computer incident response team – AKCESK – is the legally mandated agency created by the decision of the Council of Ministers to organize awareness campaigns, training, and to publish informative materials for the private and public sectors. AKCESK, in conjunction with the Ministry of Education, Sport and Youth, and the banking sector, conducted a pilot programme for schools on raising awareness on cyberbullying. Additionally, the Cybercrime Unit works with NGOs visiting schools and providing training for children. The private sector is starting to consider cybersecurity awareness; however, it is still at an early stage.

Bosnia and Herzegovina

The EU progress report for 2020¹⁴ finds that Bosnia and Herzegovina (BiH) is still at an early stage with regard to public administration reform. According to the EU report, there has been no substantial progress in ensuring a professional and depoliticized civil service and a coordinated countrywide policy-making approach. All levels of government have adopted the strategic framework on public administration reform and now need to embrace the related action plan. A political body steering the coordination of such a reform has not yet been established.¹⁵ Professional civil service procedures must be based on principles of merit and free from political interference. Human resources management remains highly fragmented. Civil service agencies and training units do not coordinate appropriately. In general, governance structures need to be fully functional to provide a tool for improvement in any related area, such as cybersecurity.

The administrative capacities and coordination of civil service agencies and integrated training units need to be strengthened. Managerial accountability is not yet embedded in the organizational culture of the public sector. Across government levels, basic accountability mechanisms between ministries and subordinated agencies are not in place, and effective management of subordinate bodies is not ensured.

The BiH Civil Service Agency adopted a training plan for 2020 with two courses offered: computer networks security and web-based applications. Training for judges and prosecutors remains insufficient. Significant improvements in the duration and quality of mandatory training are urgently needed.

Bosnia and Herzegovina needs to establish a computer security incident response team (CSIRT) network to facilitate strategic cooperation and information exchange.¹⁶ In general, the country needs to further align its legislation on cybercrime with the EU acquis and ensure there are adequate tools and enough well-trained staff to detect, trace and prosecute cybercrimes. We could conclude

¹⁴ Bosnia and Herzegovina 2020 Progress Report, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/bosnia_and_herzegovina_report_2020.pdf

¹⁵ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2020:350:FIN>

¹⁶ Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina, Sarajevo, October 2019, <https://www.osce.org/files/f/documents/1/a/438383.pdf>

that without these foundations as a precondition, it would be difficult for law enforcement authorities to take part in a whole-of-governance approach to building resilient cybersecurity. Unfortunately, BiH lacks an official and agreed strategic approach and framework for responding to cybersecurity threats. Although some strategies partly address cybersecurity, BiH remains the only country in south-eastern Europe without a national-level cybersecurity strategy and CSIRT.

Inadequate coordination, an insufficiently harmonized approach, deficient capacities, and the absence of a strategic vision remain issues of concern. Moreover, existing legislation is yet to be fully harmonized with the relevant EU acquis, and there is no overarching law on information security. The 2017 Decision of the Council of Ministers of BiH on the designation of a computer emergency response team for BiH's institutions still requires institutional operationalization. Also, key national priorities in the 2017-2022 information security management policy for the BiH institutions are yet to be operationalized - namely, establishing mechanisms to adequately respond to the current challenges of the digital age. All this leaves the public and private sectors in BiH, as well as individual citizens, highly vulnerable to the evolving threats of cyberspace, including cyberattacks and terrorism targeting critical infrastructure.

A significant development has been the establishment of the informal 'Neretva group', as part of the Organization for Security and Co-Operation in Europe's (OSCE) efforts in Bosnia and Herzegovina and inspired by similar OSCE efforts supported in Serbia (formerly the Petnica group, now Cybersecurity Network Foundation). The Neretva group supported Public-Private Partnership, a crucial precondition for cybersecurity. The Neretva group has improved information sharing, cooperation and coordination in this essential sphere. It is now also the generator of new cybersecurity initiatives, including e-learning courses, and information security for the public administration. Under the auspices of the OSCE Mission, a diverse group of state and entity-level stakeholders have developed Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina. The main achievement of the development of these guidelines is related to the inclusive policy development process which serves as an example of good practice.

Kosovo*

Kosovo* has achieved some level of preparation in the reform of its public administration and in cybersecurity.¹⁷ A critical assessment of the annual EU progress report is that instances of political influence on recruitment to senior civil service positions, and non-merit-based recruitment continues to undermine trust in the public administration. The limited budget of the Kosovo Institute for Public Administration and lack of ability to provide the necessary training, prevents the recruitment of civil servants and their professional development. Although the government promotes a user-oriented administration, there are weaknesses in the leadership, policy direction and coordination of the overall reform process. Many institutions continue to implement their solutions alongside central

¹⁷ Based on the 2020 Progress Report for Kosovo, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/kosovo_report_2020.pdf and Cybersecurity Capacity Review, March 2020, <https://gcsc.ox.ac.uk/files/cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf>

electronic identification (eID) tools being developed. Ways to collect feedback from citizens and businesses on service delivery quality still need to be systematically developed.

The Academy of Justice is responsible for delivering initial in-service training for judges and prosecutors and legal and administrative staff for the courts, prosecution offices, and 21 Councils. Further in-service training is needed, including on values and professional skills.

Legislation on cybercrime is generally in line with the EU acquis. The new Law 'On Cyber Security' which incorporates relevant provisions from the existing 'Law on Preventing and Fighting Cybercrime' has not yet been adopted. Progress has been noted in the area of cybercrime, for the detection, traceability and prosecution of cybercriminals. However, issues must be addressed, such as the handling of electronic evidence by people with insufficient knowledge, and the limited availability of cybercrime training for newly appointed judges and prosecutors.

Regarding the information society, Kosovo* has continued to align with the Regulation on electronic identification and trust services, the Directive on security of network and information systems, and the Broadband Cost Reduction Directive. The computer security incident response team (set up in 2014) remains understaffed.¹⁸

Montenegro

The EU progress report for 2020 states that Montenegro is moderately prepared on the reform of its public administration.¹⁹ However, strong political will is still needed²⁰ to effectively ensure depolitization of the public service, to optimize state administration, and implement managerial accountability. The Human Resources Management Authority (HRMA) is responsible for the professional development of civil servants and state employees and provides the necessary training. The HRMA has prepared a course on IT data security, and cybersecurity. The 2019–2020 action plan accompanying the judicial reform strategy encompasses implementation of the Judicial Training Centre strategy. Montenegro needs to address some horizontal systemic deficiencies in its criminal justice system, including how organized crime cases are handled in the courts. Over the coming year, Montenegro should increase the efficiency of its criminal investigations, in particular by improving the access of law enforcement agencies to crucial databases and establishing an interoperable system with a single search feature; restore the full use of special investigative measures (SIMs), in full respect of constitutional principles; and increase the number of investigators and experts in critical areas such as financial investigations, cybercrime, forensics, and SIMs.

In the area of cybercrime, the country has strengthened its institutional capacity. This has resulted in a 50% surge in the number of cases initiated (111 preliminary investigations and 4 criminal

¹⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2019:216:FIN>

¹⁹ <https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-montenegro-report.pdf>

²⁰ <https://europeanwesternbalkans.com/2020/10/06/key-findings-of-the-2020-european-commission-report-on-montenegro/>

investigations were launched for a broad range of cyber offences, such as online fraud, hacking, ransomware, selling of counterfeit goods, extortion, hate speech, and child pornography). Human resources need to be further strengthened with regard to the police and the prosecution service, to address cyber-crime and cyber-enabled crime threats.

Over the coming year, Montenegro should establish a track record to demonstrate an administrative capacity to enforce the EU acquis for electronic communications, information society services and audiovisual media services, including regulatory independence. The information society is under the responsibility of the Ministry of Public Administration. The government has adopted the 2019 action plan implementing an information society development strategy. The strategy, which is based on the Digital Agenda for Europe and the Digital Single Market Strategy, identifies critical steps to achieve necessary standards, such as the accessibility of broadband services, cybersecurity, digital business, eHealth and e-education. In general, positive developments have been hindered by a lack of administrative capacities to be able to utilize strategic and legal frameworks fully, so the strategy's implementation has not been followed through. There was also a national cybersecurity strategy²¹ adopted in 2018, The competent authority for cybersecurity is the National Security Agency of the Ministry of Defence (as of November 2020) based on modifications to the Law on Classified Information (2020).

North Macedonia

North Macedonia is moderately prepared for reform of its public administration, according to the EU progress report 2020.²² The Ministry of Information Society and Administration has reinforced its coordination and monitoring role to manage human resources across the public administration.²³ Professional development is still not systematic and there is no centralized database of the training offered by various institutions. Some institutions even report to both their line ministry and the government, in parallel. North Macedonia took steps at both central and local levels to improve managerial accountability and delegate responsibility to various management levels. However, the delegation of decision-making authority to middle management remains limited. Further efforts are needed to efficiently mainstream managerial accountability across the whole of the public administration. The Academy for Judges and Public Prosecutors has continued to improve its operations, by strengthening its curricula for primary and ongoing training.

In July 2019, the National Cyber Security Council was established in line with the national cybersecurity strategy (2018-2022). The Council is composed of the minister of defence, the interior minister and the minister of information society and administration. The Council is responsible for coordinating and monitoring the implementation of the strategy and providing strategic guidance. North Macedonia should strengthen its law enforcement, focusing on detection, traceability and the prosecution of cybercriminals. As part of the Digital Agenda for Europe, the country has continued

²¹ <http://www.cirt.me/ResourceManager/FileDownload.aspx?rid=296491&rType=2&file=Strategija%20sajber%20bezbjednosti%20Crne%20Gore%202018-2021.pdf>

²² https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/north_macedonia_report_2020.pdf

²³ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2020:351:FIN>

to implement the priorities set out in the 2019–2023 national broadband strategy and the 2018–2022 national cybersecurity strategy.

Serbia

The 2020 EU progress report for Serbia²⁴ finds that it is moderately prepared with regard to public administration reform. However, overall, the government has made no progress, as the public administration services have not reduced the excessive number of acting senior manager positions. The lack of transparency and respect for a merit-based recruitment procedure for senior civil service positions is an issue of increasingly serious concern. The structure of the public administration has yet to be streamlined. The lines of accountability between agencies and their parent institutions remain blurred, contributing to overlapping functions, fragmentation, and unclear reporting lines.²⁵ With regard to professional development, the National Academy of Public Administration has continued to develop a national training framework and organizes training courses for all public officials, including at the local level. A comprehensive professional development programme for senior civil servants was adopted as part of the training programme for 2020. The training centre of the National Academy of Public Administration provides general training on IT security and IT security for critical IT systems.

The Judicial Academy is mandated to provide both initial training for qualified law graduates who aspire to working in the judicial service and in-service training for judges, prosecutors and court staff. The Judicial Academy operates under the supervision of the Ministry of Justice. There is still an urgent need to improve the academy's professionalism, notably regarding its internal capacity and organization.

The Ministry of Interior completed legislative reform concerning the human resources management system in June 2019. It provides for adequate staffing in several areas, such as asset recovery and cybercrime. It is too early to assess its full impact. The reform was also relevant for the consistent application of the intelligence-led policing mode. With regard to cybercrime, the Judiciary rendered convictions against 49 individuals (first instance). The Ministry of Interior strengthened the police's operational capacity to effectively address cybercrime, including establishing special investigative units to deal with credit card, e-commerce and e-banking abuse, and to suppress illegal and harmful content on the internet. Staff numbers in the cybercrime department have increased from 15 to 22, whilst Serbia's cybercrime strategy, adopted in late 2018, is being implemented.

Digitalization continues to top the list of government priorities. The government adopted the 2020–2024 Strategy of Digital Skills Development, in February 2020, to raise the digital literacy level and to achieve more effective cross-sectoral collaboration using all available resources. The education system has further promoted digital skills, informatics and computer science, engineering and technology subjects in primary schools' curricula. Key actors are the Ministry of Trade, Tourism, and Telecommunications (MTTT) as creator of policy and competent national authority, and Serbia's Regulatory Agency for Electronic Communications and Postal Services (RATEL) as the national computer emergency response team.

²⁴ https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/serbia_report_2020.pdf

²⁵ https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/serbia_report_2020.pdf

The amended Law on Information Security was adopted in October 2019, aiming to further align itself with the EU Directive on network and information systems. RATEL became an associate member of the expert group on resilience and security of communication infrastructure, networks and services of the European Union Agency for Cybersecurity – ENISA. RATEL would benefit from association with the Agency's other expert groups as well. MTTT, on the other hand, is in charge of developing and implementing national policies, and it would benefit from the building of administrative capacity for these tasks (there are not enough people, and in particular, no 'talent pipeline').

REGIONAL OVERVIEW

The EU remains the main actor in the Western Balkans integration and cooperation efforts. The European Commission launched the Digital Agenda for the Western Balkans²⁶ in June 2018 at the Digital Assembly in Sofia, Bulgaria. The Digital Agenda aims to support the transition of the region to a digital economy and bring digital transformation benefits, such as faster economic growth, more jobs, and better services. The EU and Western Balkan countries' commitment to the Digital Agenda should help modernize public administrations, strengthen cybersecurity, increase connectivity, and improve the business climate. Ministers from six Western Balkan countries (WB6) committed to, among other things, increasing cybersecurity, trust, and the digitization of industry.

Cybersecurity in the Western Balkans has been a subject for many actors over the years. Of particular interest to this paper are reports from the DiploFoundation and the Regional Cooperation Council (RCC). The Oxford Cybersecurity Capacity Maturity Model for Nations reports should also be noted, but also the fact that these assessments have been consistently carried out in different periods throughout the region, by various stakeholders, and that there is an evident lack of continuous monitoring for cybersecurity policy developments in the WB6.

The report from the DiploFoundation was drafted as part of the Cybersecurity Capacity Building and Research Programme for South-Eastern Europe project in 2016. The report aimed at analysing policy-related gaps and mapping existing institutional frameworks in the Western Balkans, to further discuss the current openings through enhanced cooperation and investments in the region. The report, among other useful findings, provided an overview of major international players offering assistance in cybersecurity in the Western Balkan region: the EU, NATO, the Organization for Security and Co-operation in Europe, the Council of Europe, the United Nations Development Programme, and the International Telecommunication Union. Also, it listed various regional security mechanisms and opportunities for cooperation in cybersecurity.

When it comes to potential further building of regional cooperation among public administrations in this area, the Regional School of Public Administration (ReSPA) and the Regional Cooperation Council are the most relevant. They are still the only regional initiatives of this type, and continue to

²⁶ <https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-digital-agenda-western-balkans>

be supported by the European Union, with an established track record and significant ownership by the countries in the region.

The RCC published a paper called *A NEW VIRTUAL BATTLEFIELD – How to prevent online radicalisation in the cyber security realm of the Western Balkans*, in December 2018.²⁷ The main objective of this study was to provide a comprehensive overview and analysis of the region's cybersecurity. The study recognized some of the challenges, such as the lack of proper resourcing of computer security incident response teams (CSIRTs). Low levels of incident reporting and limited resourcing of bodies, such as CSIRTs, the police and prosecutors with regard to staffing, technology and training, negatively impact investigations and procedures.²⁸ Despite recognizing their value, the study noted the lack of significant public-private partnerships and the lack of educational policies and programmes on information and communications technology and related areas within the WB6. The report also provided many valuable recommendations to address these challenges and maximize progress concerning harmonizing strategic and legal frameworks, both at national and regional levels, including establishing a regional centre of excellence for cybersecurity. Many findings from this study are still relevant and useful when discussing regional cooperation in cybersecurity for the Western Balkans.

As has been mentioned, the ReSPA and RCC are important actors for contemplating regional efforts in cybersecurity. The ReSPA²⁹ is the inter-governmental organization for enhancing regional cooperation, promoting shared learning, and supporting public administration development in the Western Balkans. ReSPA members are Albania, Bosnia and Herzegovina, North Macedonia, Montenegro and Serbia, while Kosovo* is a beneficiary. The purpose of the ReSPA is to help governments in the region develop better public administration, public services and overall governance systems for their citizens and businesses, and prepare for membership of the European Union. The ReSPA establishes close cooperation with ministers, senior public servants and heads of function in member countries. The ReSPA also collaborates with the EU, specifically the Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR), other regional players such as the OECD/SIGMA Regional Cooperation Council, as well as agencies and civil society organizations.

Since its inception, the ReSPA has contributed to capacity building and networking activities through in-country support mechanisms, peering, and regional research material production. The European Commission (EC) directly manages funds to support ReSPA activities (research, training and networking programmes) in line with the EU accession process. The current EC grant supports implementing the actions required for achieving the three strategic objectives during the period 2019–2021. The ReSPA works primarily through regional networks which operate at three levels: ministerial, senior officials, and networks/working groups of experts and senior practitioners.

One of the networks consists of a programme committee composed of the representatives of institutions in charge of public administration reform, public financial management and government

²⁷ <https://www.rcc.int/swp/pubs/1/a-new-virtual-battlefield--how-to-prevent-online-radicalisation-in-the-cyber-security-realm-of-the-western-balkans>

²⁸ https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/ipa_ii_2019-040-826.15_cybersecurity.pdf

²⁹ <https://www.respaweb.eu/>

policy planning, and the European integration coordination process, as well as five working groups: (1) centre-of-government institutions; (2) better regulation; (3) human resource management and development; (4) governance; and (5) quality management.

The ReSPA does not provide many training courses for the regional public administrations but acts more as a think-tank and networking agent on their behalf. The ReSPA has not been directly involved in training on cybersecurity but has been using in-country support to assist member states. The in-country mechanism is the ReSPA activity that enables its members to apply for related support in expertise. In the framework of the latter activity, the ReSPA provided two senior e-government experts in cybersecurity to review the draft cybersecurity strategy for Albania and make preparations for the aligned cost analysis to design passport indicators.

The Regional Cooperation Council³⁰ is an all-inclusive, regionally owned and led cooperation framework. This framework engages RCC participants from South-East Europe (SEE), members of the international community and donors on essential subjects and of interest to the SEE, to promote and advance the European and Euro-Atlantic integration in the WB region.

In digital transformation, one of the RCC objectives is building a self-reliable regional cyber threat response system. Some of the envisaged results include enhanced regional capacities on developing digital skills strategies, enhanced regional capabilities on electronic identification and trust services, networked CSIRTs and supported cybersecurity capacities.

Digital trust is the foundation for a healthy development of the digital environment. The Western Balkan economies recognized the rapid growth of digital technologies and their effect on building digital trust in the WB region. In keeping with this, and in accordance with the conclusions of the second Western Balkans Digital Summit, the Western Balkan economies have agreed to work together on the process of mutual recognition of trust services, harmonization of legislation with the eIDAS Regulation on electronic identification and trust services for electronic transactions in the internal market, and upgrading of the registries for trust services.³¹ With this in mind, the RCC has committed to the following next steps in their work:

- Maintain permanent regional dialogue and cooperation among CSIRTs in all WB economies;
- Enhance regional cooperation between CSIRTs and build their capacities;
- Support processes that lead to the improvement of interoperability across the WB region;
- Enable processes aimed at recognition of trust services;
- Support processes towards the free flow of non-personal data and more generous data interoperability.

This course of action taken by the RCC will contribute to cybersecurity capacity building of the public sector in the Western Balkan countries.

³⁰ <https://www.rcc.int/>

³¹ https://www.rcc.int/priority_areas/55/cybersecurity

WAY FORWARD

All Western Balkan (WB) countries share similar challenges regarding CSIRTs' capacities and operations: limited financing, understaffing, and technology deficits, coupled with a lack of awareness on the part of politicians of the risk of insufficient cyberspace security capacity. They also share very similar shortcomings in public administration reform, hindering progress in cybersecurity as well.

Bearing in mind the limitations in the capacity of national administrations for tackling cybersecurity-related risks, the significant challenges for general public administration reform, and COVID-19-related social and economic consequences (amongst which rapid digitalization of public service delivery and e-commerce are included), it would be recommendable to look for appropriate joint regional action. Such a regional effort should be based on a functional analysis of existing institutional capacities. It could provide a training needs assessment for various beneficiaries within the administration; standardization of business processes; threat assessment and incident response support; knowledge management, best practice dissemination, and coaching and mentoring.

Regarding the reform process in public administrations in recent years, there has been a change in emphasis away from structural decentralization and single-purpose public organizations, towards a more integrated approach to public service delivery. Various terms 'one-stop government,' 'joined-up government' and 'whole-of-government,' the movement from isolated silos in public administration to formal and informal networks is a global trend. Various societal forces drive a whole-of-government approach. For example, the growing complexity of problems calls for a collaborative response; the increased demand from citizens for more personalized and accessible public services (planned, implemented and evaluated with their participation); and the opportunities offered by the internet to transform the way the government works for the people. Cybersecurity would also benefit from a similar, whole-of-government approach, with a strong regional dimension for the Western Balkans.

Regional ownership of joint activities in cybersecurity is a must, and is explicitly expected by the EU. Countries will have to be willing to invest expertise, time, presence and money. Donor funding may support this regional approach, but it would be essential to ensure strong regional ownership in such an activity, mainly through financial contributions from the countries in the region. This would guarantee sustainability and increase the likelihood of continuous benefits from such a regional framework. The motivation for progress in this area needs to come from within, so it can be self-sustaining into the future.

Experts have noted³² that while EU twinning projects and the provision of training and mentoring are valuable, projects alone cannot garner their actual value because of a lack of hardware, software, and other logistical necessities. Lack of resources is most often due to the failure of national governments to reallocate appropriate resources to declared activities/goals/institutions due to the previously mentioned challenge to balance different public administration reform goals.

³² <https://www.rcc.int/swp/pubs/1/a-new-virtual-battlefield--how-to-prevent-online-radicalisation-in-the-cyber-security-realm-of-the-western-balkans>

That said, donor support, in terms of finance, training, and knowledge sharing, especially from the EU and EU member states, should be encouraged and facilitated by such a regional effort. The European Union Agency for Cybersecurity (ENISA), DCAF, the Regional School of Public Administration (ReSPA), Regional Cooperation Council (RCC), and NATO are all potential facilitating partners in this increased cooperation and could be part of some future advisory board for a regional centre.

North Macedonia, Albania and Montenegro could proactively obtain lessons learnt from NATO, where possible, to conduct regional exercises. Such an approach would take considerable funding but could provide positive spill-over effects for Euro-Atlantic integration, parallel and complementary to EU integration, essential in the security sector.

When it comes to cybersecurity and national designated authorities, we must be aware that the situation varies from country to country in the Balkans, but there could be enough similarities to enable a regional approach. In most cases, similarities exist regarding institutional set up and leading authorities, but also when it comes to the challenges, such as the shortage of skilled personnel. Differences exist between countries as they are at different levels of development in cybersecurity, but still more similar one to another between themselves when compared jointly with EU countries and established standards. None of the national CSIRTs in the Western Balkans 6 (WB6) are stand-alone agencies, but their positioning within governments is different across the region. The national CSIRT in Serbia is, for example, positioned within the Regulatory Agency for Electronic Communications and Postal Services (RATEL), in North Macedonia it is the Agency for Electronic Communications, and Bosnia and Herzegovina's national CSIRT is in the Ministry of Security. ENISA also encourages sectoral CSIRTs. The existence and number of these sectoral CSIRTs (e.g. finance, telecommunications, energy, etc.) is not consistent across the WB6. Still, this should not prevent their increase in cooperation, but it needs to be addressed during the planning and design phase of any new regional framework.

On a technical level, regarding CSIRT capacity building, experts work well together due to the shared nature and aims of their work. This strong cooperation has primarily been a result of donor support, mainly DCAF-led and UK-financed interventions. On the other hand, in the strategic realm, close attention is necessary for fostering multi-stakeholder involvement. Developing robust and sustainable partnerships between the government and other actors in society (i.e. the private sector, civil society organizations, research institutes) is critical for ensuring a whole-of-society approach.³³ Resources for building cyber resilience are distributed at many levels (i.e. individual, community, state), so the national authority must clearly define responsibilities for each. However, it is difficult for national administrations to demonstrate effective and inclusive public policy developments, as recognized in the EU integration process.

Thus, it seems that a regional instrument could be useful to improve capacity building for multi-stakeholder involvement, and strategy development and implementation. Some stakeholders are transnational (EU, big tech) and a regional approach can offer best practice, as well as peer learning and incentives for national change agents. Still, challenges remain firm at the national level when it

³³ https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/ipa_ji_2019-040-826.15_cybersecurity.pdf

comes to a multi-stakeholder approach, and there is no miracle that will improve the situation overnight. Countries still need strong support to engage stakeholders at the national, bilateral and regional levels to create partnerships and networks; promote civil society and the private sector; manage extensive group processes and open dialogue; mediate divergent interests; and establish collaborative mechanisms. They would benefit from focused support and best practices defined and shared. A centre of expertise could be set up to collect evidence of an improved approach to multi-stakeholder management from any country in the region. It is easy to miss the opportunity of learning from peers if there is no continuous influx of practical examples that can be easily replicated.

Public-private partnerships play a vital role in this respect. They contribute to building trust and improving the understanding between public-private, private-private and public-public entities. According to ENISA, CSIRTs should also be tasked with responding to incidents and providing dynamic risk and incident analysis, and situational awareness. To enable them to do this, the security of network and information systems (NIS) directive states that “security and notification requirements should apply to operators of essential services and to digital service providers to promote a **culture of risk management** and ensure that the most serious incidents are reported”.³⁴ However, many experts note³⁵ that private sector companies are reluctant to report incidents despite legal obligations. Companies fear reputational damage if they report cyberattacks, with a significant concern that reports will be leaked to the media. There appears to be a lack of confidence that law enforcement is adequately equipped to conduct investigations and prosecutions in this area, with reporting therefore viewed as a waste of time.

Finally, many companies cannot be identified when attacked, thereby making it impossible to document. This situation is not unique to the WB6. The EU Cyber Security Strategy³⁶ notes that the private sector “still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, **to embrace a risk management culture** or to invest in security solution”.

As the economies of the WB6 become more connected, a joint regional effort could also contribute to commercial investment and partnerships across borders. If business sector representatives active in digital transformation and e-commerce from one country are thinking about investing in another country, they will make rigorous risk assessments regarding their potential investments or joint operations. If they lack detailed information, they could be misleading with regard to the risks involved. The same applies if they think about working with the public sector from another country within a donor project requiring private sector involvement. If there are frequent possibilities for more ambitious companies to participate in regional discussions on cybersecurity, they could develop a more agile approach to regional operations. At the same time, if they conclude that individual countries are not progressing fast enough in cybersecurity, they could use the regional framework to request greater efforts and commitment from any government, since as a rule they are all represented at every regional event.

³⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>

³⁵ <https://www.rcc.int/pubs/70/a-new-virtual-battlefield--how-to-prevent-online-radicalisation-in-the-cyber-security-realm-of-the-western-balkans>

³⁶ <https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=JOIN%3A2013%3A0001%3AFIN> page 6

The challenging public administration context found in the WB6 countries, as well as obstacles such as massive staff rotation in beneficiary institutions and agencies, can hinder progress or the ability to achieve significant consolidated results.³⁷ Therefore, a demand-driven approach based on a comprehensive and continuous national needs assessment regarding national cybersecurity authorities, is necessary. The comprehensive needs assessment should look at the following: levels of legal harmonization within the EU, organizational capacities of national authorities, the number of people working in cybersecurity and their competences, the level of horizontal and vertical cooperation at the national level between public institutions, the level of inclusiveness regarding civil society and the business sector during the process of developing public policies, existing cooperation frameworks at the national level, working cooperation agreements with counterparts from EU member states, absorption capacities for development aid, and levels of awareness in general administration regarding cybersecurity threats. This would also enable regional benchmarking and help identify areas where more advanced countries could share their expertise with colleagues from the region. Assessment of human capacity is an integral part of such an effort. EU reports have highlighted that human resources management and merit-based recruitment, training needs assessment and delivery, remain significant challenges for public administrations in the region. Management and employees need to understand the pivotal role they play for the cybersecurity of public organizations. But national training efforts are still limited in size and extent, and an in-depth needs assessment could show what kind of advances should be made a priority.

The learning process in organizations must be based on a user-centred approach, which pays attention to target groups, gender, and culture, based on personal knowledge and skills, and concrete workplace needs and contexts. The user-centric system should also allow staff exchanges regarding cybersecurity along the business process chain. This requirement is a lot to be taken on by existing national central training institutions, without sustainable regional support. The ReSPA is well-positioned to initially provide such an exchange regarding specialist knowledge for cybersecurity human resources management (HRM). Through their Human Resources Management and Development (HRMD) Working Group, the ReSPA aims³⁸ to empower civil servants of the Western Balkan governments by providing them with critical insights, knowledge, tools and connections needed to establish efficient services, which will benefit citizens and businesses alike. By organizing various capacity-building events, conducting tailor-made research, composing documents with recommendations, and establishing inter-governmental regional networks among senior HRMD civil servants, the ReSPA could provide some exchange experience and best practices for HRM in cybersecurity.

However, there will be additional needs for specialist improvement of HRM practices in cybersecurity in the region. It would be difficult for the ReSPA to provide this, bearing in mind their general mission. It would take sustained effort and significant expertise to provide crucial support to WB countries in HRM in the cybersecurity field. There is a need for detailed competence frameworks for various positions and seniority levels in the administration, specialized assessments

³⁷ https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/ipa_ii_2019-040-826.15_cybersecurity.pdf

³⁸ <https://www.respaweb.eu/10/pages/42/what-we-do>

for recruitment, for career paths and a specialized retention policy, as well as push and pull factors from growing regional markets. It could be beneficial to devise the possibility of certifying specific posts in the administration, and to request continuous learning and knowledge assessments from reliable and responsible civil servants.

Finally, all regional public administrations would benefit from additional regional training, mentoring and coaching possibilities, bearing in mind the limited capacities of national training institutions. Besides, there is a need for more specialized courses for people working in national authorities, and at the same time, a need for more general cybersecurity training for all civil servants. Managers are a separate target group for training, and cybersecurity courses could become mandatory for senior members of the administration. It should also be noted that regional training is obliged to require transnational trust among cybersecurity and other professionals. These are complex tasks for national training institutions. At the same time, the ReSPA now aims more towards establishing and maintaining networks whilst departing from the training provider's initial role.

Cybersecurity is a developing area and efficient exchanges between the region's CSIRTs would be useful to speed up developments. We should also bear in mind amendments to the EU NIS Directive,³⁹ proposed in December 2020. The NIS Directive poses a baseline checklist for any country aiming to develop a sound national cybersecurity field approach. The new proposal **significantly expands** the scope of the current Directive by adding **new sectors**⁴⁰ based on their criticality to the economy and society. While the sectors covered by the current Directive are limited to energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure, the recent proposal now applies to:

- Certain public or private 'essential entities' operating in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water, **wastewater**, digital infrastructure, **public administration** and **space**; as well as
- Certain 'important entities' operating in the sectors of **postal and courier services, waste management, manufacturing, production and distribution of chemicals, food production, processing and distribution, manufacturing and digital providers.**

It would be challenging for the WB6 to provide rapid harmonization with the new Directive without some regional effort to speed-up the process and provide quality assurances. It is difficult for each national administration to continuously follow developments in this area on their own and plan for legal harmonization, in particular to anticipate future developments in this area in the EU and be future-proof. This difficulty is a general challenge, not only in cybersecurity.

One of the tasks of national CSIRTs is to monitor cyber incidents at a national level. Working as an observation lab, the regional centre could continuously observe trends, acting as a knowledge management and repository facility and keeping track of lessons learnt. Besides, incorporating human rights safeguards in the design and implementation of all actions is vital to ensure that international standards and EU values are reflected throughout the performance of activities.

³⁹ <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union>

⁴⁰ <https://www.mondaq.com/austria/security/1020144/cybersecurity-on-the-rise-the-nis-directive-20>

A conclusion of this analysis, as was previously suggested, and what is still a reasonable proposal, is that a shared WB6 regional cybersecurity hub (as a centre of expertise) would benefit the WB6 countries. The potential regional cybersecurity hub could be tasked to operate across areas which are within the usual practices of national authorities, and with a focus on:⁴¹

5. Providing thought leadership and strategic development **direction and analysis** in the cybersecurity space;
6. Raising cybersecurity **awareness** at all levels of government;
7. **Sharing** information, expertise, and knowledge; and
8. Establishing and promoting **best practices** based on common challenges.

It is vital to coordinate and redirect research and development (R&D) efforts since no single individual or organization at national level is aware of all cyber-related R&D activities. Having a regional centre helps eliminate redundancies in nationally funded cybersecurity research, identify research gaps, prioritize R&D efforts, and ensure that taxpayers are getting full value for money as countries shape their strategic investments and donors look for sustainable support.

It would also be useful to task such an initiative to provide appropriate recommendations, support professional education through training, mentoring and coaching, and to facilitate networking. While millions of euros are being spent on new technologies to secure the European and regional governments in cyberspace, people with the right knowledge, skills and abilities to implement those technologies will determine its success. However there are not enough cybersecurity experts within the regional governments or private sector, nor is there an adequately established cybersecurity career field in the public administration. Existing cybersecurity training and personnel development programmes, while good, are limited in focus and lack unity of effort. To effectively ensure their continued technical advantage and future cybersecurity, the WB countries must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of prospective employees. The majority of efforts will take place at national level, but countries' progress could be significantly speeded up if they can learn from each other and benefit from a regional depository of best practices.

A cybersecurity hub should provide expert commentary, tools and resources, developed through obtaining data and interviewing national authorities, stakeholders and analysts throughout the industry to deliver practical and strategic advice. The regional hub could support research regarding existing standards. It could encourage standard-setting processes, support the development of competence frameworks, and develop general references for standard equipment and technology requirements at national level. The hub could provide direct access to information, technology, support, expertise, etc., as and when needed.

Furthermore, it could also deliver thought leadership, house a regional institute or think tank, one looking towards the future, but from a regional perspective, drawing on the work at national level, and influencing policy and long-term thinking. However, this process is necessary to ensure cybersecurity, in all its appearances, risks and challenges, mainstreamed in areas such as democracy, governance, markets, and human rights.

⁴¹ <https://www.perficient.com/-/media/files/guide-pdf-links/five-guiding-principles-of-a-successful-center-of-excellence.pdf>

Regarding the structure of such a hub, it would be advisable to have a governing board functioning at the level of high-level representatives of national authorities as in the case of the NIS Directive (e.g. ministers) and a governing board operating at the level of senior representatives of national CSIRTs. The hub could have different working groups dealing in more detail with strategic and policy development, legal harmonization, HRM, business processes, and so on.

The hub could engage in an annual assessment of needs for capacity development and provide regular reporting on accomplishments. It would be essential to have a flagship report, giving an in-depth overview and offering thought leadership possibilities in regional cybersecurity for practitioners. It would also be necessary to develop multiple learning opportunities and peer-to-peer exchange, with alumni-type support. Various visibility activities could be designed, including annual regional cybersecurity awards. Most importantly, the hub should guide and support capacity developments, and promote and exchange local knowledge and expertise between one country and another.

A regional hub for cybersecurity could start out as a project activity and output, and if proven to be a valuable contributor to cybersecurity developments, could grow towards being a more permanent structure.