INSTRUMENT FOR PRE-ACCESSION ASSISTANCE (IPA II) 2014-2020

MULTI-COUNTRY

EU support to cybersecurity capacity building in the Western Balkans

Action summary

Information and Communications Technologies (ICTs) and the internet have changed the way we live and work drastically over the past 20 years. This has had many positive impacts, such as economic growth or increased transparency. However, it can also enable risks and vulnerabilities.

The Digital Single Market is the Commission's second political priority. The 2017 Joint Communication on '*Resilience, deterrence and defence: Building strong cybersecurity for the EU*' recognised the significance of capacity building in third countries to increase the global level of cybersecurity. Additionally, the *Western Balkans strategy* and its *Digital Agenda flagship* note the Commission's intention to support cybersecurity capacity building.

This action will aim to build up functioning and accountable institutions in the Western Balkans to strengthen the region's cyber resilience in order to respond effectively to challenges and risks such as cyber attacks.

Enhanced cyber resilience will help developing a safe and secure digital environment, which is necessary to enable digital growth in the Western Balkans region. In addition, stronger capacity to deal with cyber attacks in the Western Balkans and better cooperation will be of benefit to both the region and the EU, as cyberspace knows no borders.

Action Identification	
Action Programme Title	IPA II Multi-country Action Programme 2019
Action Title	EU support to cybersecurity capacity building in the Western Balkans
Action ID	IPA 2019/040-826.15/MC/Cybersecurity
Sector Information	
IPA II Sector	9. Regional and territorial cooperation
DAC Sector	15210 Security system management and reform
Budget	
Total cost	EUR 8 million
EU contribution	EUR 8 million
Budget line(s)	22.020401- Multi-country programmes, regional integration and territorial cooperation
Management and Implementation	
Management mode	Direct management
Direct management: **European Commission**	Directorate-General for Neighbourhood and Enlargement Negotiations– Unit D.5 Regional Cooperation and Programmes
Implementation responsibilities	Directorate-General for Neighbourhood and Enlargement Negotiations, Unit D.5 Western Balkans Regional Cooperation and Programmes
Location	
Zone benefiting from the action	Western Balkans (Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, North Macedonia, Serbia)
Specific implementation area(s)	N/A
Timeline	
Final date for contracting including the conclusion of delegation agreements	At the latest by 31 December 2020
Indicative operational implementation period	72 months from the adoption of the Financing Decision

Policy objectives / Markers (DAC form)			
General policy objective	**Not targeted**	**Significant objective**	**Main objective**
Participation development/good governance	☐	☐	X
Aid to environment	X	☐	☐
Gender equality (including Women In Development)	☐	X	☐
Trade Development	X	☐	☐
Reproductive, Maternal, New born and child health	X	☐	☐
RIO Convention markers	**Not targeted**	**Significant objective**	**Main objective**

* 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.

Biological diversity	X	☐	☐
Combat desertification	X	☐	☐
Climate change mitigation	X	☐	☐
Climate change adaptation	X	☐	☐

1. RATIONALE

PROBLEM AND STAKEHOLDER ANALYSIS

Problem/needs:

1. Cybersecurity systems (institutional and legal framework) are either inexistent or weak and should be clearly defined and aligned with EU.
2. Technical/operational capacity/skills of competent authorities are low (both in terms of staffing and technical knowledge).
3. Cooperation needs to be enhanced between the relevant IPA beneficiaries and with Europe in order to adequately respond to incidents/threats.

However, the level of preparedness differs between the relevant IPA beneficiaries. Therefore, on top of regional actions, windows at IPA II beneficiary level should be considered to address each IPA II beneficiary's specific needs.

There are many studies on this action's subject already available from the work of international organisations, e.g. the International Telecommunications Union (ITU), the Organization for Security and Co-operation in Europe (OSCE), the Regional Cooperation Council (RCC) or the World Bank. These studies, of which references can be found in the section "other key references" below, will form the starting point for the action, and background information for the contracted action coordinator.

The most recent study that gives a comprehensive overview and analysis of the cybersecurity situation in the beneficiaries is the EU financed study commissioned by the RCC called "A New Virtual Battlefield[1]" from December 2018. The study concludes:

"The Western Balkans six have made and continue to make progress in harmonising their cyber security legislation and strategies in line with the EU framework. However, considerable deficits still remain in respect to implementation and operationalisation of practical responses. The most significant challenges are posed by (i) the lack of proper resourcing of Computer Security Incident Response Teams (CSIRTs); (ii) low levels of incident reporting; (iii) limited resourcing of bodies, such as CSIRTS, police, and prosecutors in respect of staffing, technology, and training, which is negatively impacting investigations and procedure; (iv) the lack of significant public-private partnerships, despite recognition of their value; (v) the lack of educational policies and programmes on Information and Communications Technology (ICT) and related areas within the Western Balkans six".

The study provides the following recommendations to help address these challenges and to maximise progress in relation to the harmonisation of strategic and legal frameworks:

National-level recommendations:

- Resource strategies and action plans - A first step to concretely addressing this is to cost strategies and actions plans during the planning phase and then to reinforce such plans with dedicated funds. Solely relying on existing resources and/or donor funds will have significant negative impacts.
- Create and/or improve cyber incident reporting structures – One method to do this is to make it easier for citizens and businesses to report cyber security incidents. Many companies noted that they did not know how to report an incident, what information they would have to supply, and what and how much they could choose not to divulge. It is therefore recommended that CSIRTs reach out to such organisations and inform them about reporting processes and the nature and type of information that needs to be provided.

[1] https://rcc.int/pubs/70/a-new-virtual-battlefield--how-to-prevent-online-radicalisation-in-the-cyber-security-realm-of-the-western-balkans

- Raise awareness - This could be addressed through a number of different measures, including through formal education and professional training. However, Civil Society Organisations (CSOs), community groups, and private sector providers should also be supported to provide information and knowledge in this area, to ensure a multi-layered approach.
- Leverage existing expertise - Creating networks of interested parties, such as the informal network initiated by the OSCE and implemented by the Diplo Foundation and the Geneva Centre for the Democratic Control of Armed Forces (DCAF) in Belgrade, or drawing on existing associations, such as those within the private sector, could be a very productive step. Furthermore, such networks of experts could assist in developing a more strategic approach to cybersecurity given their broad range of perspectives, experience, and vision.
- Identify and develop Public-Private Partnerships (PPP) and build synergies - Effective strategies in all policy realms are built on collaboration. Instead of just acknowledging the need for PPPs within cybersecurity, significant effort should be put into what such partnerships could look like and the areas that may most benefit from their establishment. Joint trainings are an obvious first step to building better relationships.
- Review educational approach to ICT and cybersecurity - The Western Balkans six need to undertake a comprehensive review of its educational approach to ICT and cybersecurity. This should not only enquire into what courses are required and at what levels, but include a longer-term assessment of future needs in this area, and courses developed and offered based on this. It should almost certainly also include development of not just technology-based, but multi-disciplinary programmes to insure the competencies to support better strategic and operational implementation of cyber security strategy are available.

Regional-level recommendations

The study concludes that progress in cybersecurity would benefit from a more joined-up and forward thinking regional approach, which would build on the work and structures of existing regional institutions, such as the RCC. This regional approach would make better use of scarce resources. Furthermore, it would illustrate a shared political will and proactive approach to cyber security. The following is therefore recommended:

- Develop a more strategic approach to regional cooperation - It is recommended that developing a strategic approach to cybersecurity should be done within existing frameworks, such as that of the EU, rather than creating new ones. For example, developing a Western Balkans six regional cyber strategy, which identifies and sets out regional critical infrastructure, common minimum standards, a Critical Infrastructure Warning Information Network (CIWIN), etc. This will help mitigate risk and ensure better overall protection of Critical Information Infrastructure (CII) as provisioned by Operators of Essential Services (OES).
- Realign support of the international community to the strategy of the region - The support of the international community is valued in this area, as in others, but does not come without criticisms. There is a need for greater discussion about what areas may benefit from international support, what support would have the greatest impact, and related issues. Having a regional strategy would help identify headline issues and, in so doing, identify where best to direct such support. This may help to both alleviate criticisms about duplication of resources and streamline programmes into priority areas for the region.
- Establish a regional centre of excellence – A shared Western Balkans six regional centre of excellence in cybersecurity would be of benefit. While this would not negate the need for basic, yet effective, minimum standards of equipment and technology at the economy level, more elaborate technology and equipment could be housed within a regional centre of excellence. This would

reduce the cost to individual economies, yet provide them direct access to necessary high level technology, support, and expertise when needed.[2]

The mapping of stakeholders during implementation is particularly relevant in the case of cyber-related initiatives due to the focus on a multi-stakeholder approach to internet governance. The multi-stakeholder nature of internet governance is a recurrent theme in many policy documents and has been addressed at length by analysts and researchers. The Internet was developed and operates across borders with input from the public and private sectors, academia and civil society, harnessing the expertise of each. So the multi-stakeholder approach is widely accepted as the optimal way to make policy decisions for a globally distributed network. The focus on ownership is a key component given that external actors do not build capacities but only provide support to capacity-building processes. These observations are particularly relevant for cyber capacity building, where the prevailing paradigm is based on whole-of-society and whole-of-government approaches.[3]

Stakeholders:

- Stakeholders in the relevant IPA II beneficiary (responsible ministries and citizens, competent authorities in the relevant IPA II beneficiaries, Computer Emergency Response Team (CERTs)/computer security incident response teams (CSIRTs), as well as entities involved in provision of essential services/critical infrastructure and businesses.

- Regional bodies: Regional Cooperation Council (RCC).

- European stakeholders : Member State organisations, as represented within the European Union Agency for Network and Information Security (ENISA), Task Force on Computer Security Incident Response Teams (TF CSIRT), Computer Emergency Response Team for the EU institutions (CERT-EU), EU Member States' CSIRTs.

- International (global) stakeholders: International Telecommunications Union (ITU), global Forum of Incident Response and Security Teams (FIRST), Council of Europe (concerning cybercrime), the World Bank, the North Atlantic Treaty Organization (NATO), the OSCE and the OECD.

Current state of play in the region: (based on study by DiploFoundation September 2016[4], annual progress reports, as well as the RCC study "A New Virtual Battlefield" and RCC facilitated dialogues).

Albania: Its first national cross-cutting Strategy on Information Security 2008-2013 briefly mentioned cybersecurity as one of the priority areas, it also envisaged the creation of the National Agency for Cyber Security (ALCIRT) under the prime minister's authority as national institution for response to cyber-incidents. In 2016 it still had very limited human and infrastructure capacities. The Law on Cyber Security was adopted in February 2017 and is partly aligned with the Directive on security of network and information systems (NIS). There is a need to develop a national cybersecurity strategy. The national CSIRT is the NAECCS (National Authority for electronic certification and cyber security), established on May 2017. It also acts as coordinator between national and international stakeholders. In addition, as a NATO member Albania is taking part in NATO cyber exercises and it is implementing OSCE "Confidence Building Measures" for cyberspace since 2014.

Bosnia and Herzegovina: According to the DiploFoundation study of 2016, Bosnia and Herzegovina did not adequately progress in cybersecurity, nor has it harmonized its legislation accordingly and it still lacks a

[2] EU financed study commissioned by the RCC called "A New Virtual Battlefield" p. 8-10.

[3] Operational Guideance for the EU's international cooperation on cyber capacity building, p. 70. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf

[4] https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf

comprehensive overall strategic approach to address the issue of cybercrime and cybersecurity threats. Although Bosnia and Herzegovina currently does not have a state-level law on information security, its entity Republika Srpska has one. There are plans to draft a Law on Network and Information Security for the institutions of Bosnia and Herzegovina. The Council of Ministers of Bosnia and Herzegovina has established a CERT (Computer Emergency Response Team) for the institutions of Bosnia and Herzegovina (government CERT) by the Decision of Council of Ministers of Bosnia and Herzegovina in March 2017 and placed it in the Ministry of Security of Bosnia and Herzegovina. Furthermore, the Ministry of Security of Bosnia and Herzegovina together with other competent institutions for cybersecurity in Bosnia and Herzegovina (from all levels of authority) leads the cyber security related processes in Bosnia and Herzegovina. It is currently running a dialog about a comprehensive overall strategic approach to address the issue of cybercrime and cybersecurity threats, as well as other issues covered by the NIS Directive. In that respect, it has requested an assistance of several international organizations. In addition, cybersecurity has been recognized as important issue in the country's Strategy for combating organized crime 2017-2020 and the Strategy for prevention and combating terrorism 2015-2020.

Kosovo: The legal framework for cybersecurity is still not fully developed, although recently the Regulation on technical and organizational standards for security and integrity of electronic communications networks and services was adopted in accordance with ENISA recommendations and NIS Directive. The regulation introduces the obligation to perform audits of networks and services. In January 2016 the government of Kosovo adopted the Cyber Security Strategy and Action Plan 2016-2019. With heavy assistance of the EU-funded project ENCYSEC, in 2016 KOS-CERT started working as the main CERT. KOS-CERT is a functional unit within the Regulatory Authority for Electronic and Postal Communication. The two main functions of the CSIRT are awareness raising and incidents handling coordination. The European Commission's progress report of 2018 stated that Kosovo needs to make adequate budgetary resources available to implement Kosovo's cybersecurity strategy and action plan for 2016-2019.

Montenegro: The national CSIRT was established in 2012 with the support of ITU and IMPACT and now it operates within the Ministry of Public Administration. The National Council for Cybersecurity was established based on the amendments to the Law on Information Security from 2016, while the establishment of a Cybersecurity Operational Centre is foreseen for the future. Montenegro has advanced fast in the cybersecurity area since 2010 when the umbrella piece of legislation – Law on Information Security - was adopted, along with the Regulation on Information Security Measures. A national Cyber Security Strategy for Montenegro for the period 2013-2017 was adopted in October 2013. In October 2014 the Government of Montenegro adopted the Methodology of identifying Critical Information Infrastructure (CII) and the Action plan for its implementation.

North Macedonia: The first Cybersecurity Strategy has been adopted in July 2018, while development of the Action Plan (2018-2020) is ongoing. For this purpose a working group consisting of the main stakeholders including relevant ministries and CSIRT is established. The working group already prepared the first draft, which recognizes the need for analysis of critical infrastructures as one of its priorities. There are two types of training planned by the end of this year: 30 employees from public sector will be trained on risk management while another 30 participants will pass the training on vulnerability assessment in cyber security.

Serbia: Serbia's legal and institutional framework in the area of cybersecurity is based on the Law on Information Security, which was adopted at the beginning of 2016. The European Commission's progress report of 2018 recommended Serbia to develop a national strategy on cybersecurity. The national CSIRT is established within the Regulatory Agency for Telecommunications and Postal Services (RATEL). Raising public awareness on cyber incidents and information security would be an important task in the future for the CSIRT.

The Global Cybersecurity Index (yearly published by the International Telecommunications Union) is a survey that measures commitment to cybersecurity in order to raise awareness. The index of 2017 shows that from the Western Balkans region North Macedonia globally ranks best with 54, Montenegro's rank is 70, Albania 88, Serbia 89, and Bosnia and Herzegovina 135. This means that North Macedonia and Montenegro

are scoring better than the three EU member states least committed to cybersecurity. Albania and Serbia have scores just below the least committed EU member states.

The table below from the study "A New Virtual Battlefield" provides an overview of the study's findings related to cybersecurity legislation and capacity in the region.

	Albania	Bosnia and Herzegovina	Kosovo	North Macedonia	Montenegro	Serbia
Budapest Convention on Cybercrime	Ratified 2002 24/7 Point of Contact (POC)	Ratified 2006 24/7 POC	24/7 POC	Ratified 2004 24/7 POC	Ratified 2010 24/7 POC	Ratified 2009 24/7 POC
National CIRT	✓ 2016	Very limited functionality 2017	✓ 2016	✓ 2016	✓ 2012	✓ 2016
CIRT Location	National Authority of Electronic Certification and Cyber Security	Ministry of Security	Regulatory Authority for Electronic and Postal Communications	Agency for Electronic Communications	Ministry of Public Administration	Republic Agency for Electronic Communications and Postal Services
Law on Cyber Security	✓ Adopted 2017	×	✓ Adopted 2010	×	✓ Adopted 2010	✓ Adopted 2016
Cyber Security Strategy	Policy acts in lieu, 2015-2017	×	Strategy and action plan 2016	Strategy Adopted in July 2018	Strategy and action plan 2018-2021 (2nd strat.)	✓ no action plan 2017
3rd level education on Information Security	×	✓	✓	✓	✓ multi-disciplinary	×
Critical Information Infrastructure Defined	✓	×	✓	×		×
CVE/Terrorism Strategy includes reference to cyber/online	✓	✓	✓	✓	✓	✓
Key Challenges	Technical, financial, expertise and accessing and retention staffing					

Figure 1. Synopsis of relevant information and findings from study "A New Virtual Battlefield", December 2018.

OUTLINE OF IPA II ASSISTANCE

The main expected results and key activities should ensure that legislation is implemented and enforced properly to address the challenges of cyber resilience and ensure overall security, taking EU and EU Member States' legislative experience as a benchmark. Private sector and civil society concerns and opinions should have been taken on board in development and implementation of strategies, legislation and policies. Cooperation regionally and with competent authorities within the EU (including CSIRTs) should be established to enhance cross-border responses to incidents and threats. Public and businesses should become more resilient in their use of digital technologies, be more aware of cyber risks and have better knowledge on how to avoid becoming a victim of a cyber-attack. Competent authorities (including CSIRTs) have clear mandates and are fully operational. In addition, their staff has been trained to raise the technical capacity to an adequate level. Operators of essential services (with the definition of critical infrastructure being the same as in the NIS directive) should be mapped properly and risks related to those entities managed effectively using proper frameworks. Good cooperation exists between CSIRTs and operators of essential services.

Apart from the competent authorities in the relevant IPA II beneficiaries, their private sector and general public, the EU Member States' experts should be involved in the implementation process.

RELEVANCE WITH THE IPA II MULTI-COUNTRY STRATEGY PAPER AND OTHER KEY REFERENCES

- Revised Multi-Country Indicative Strategy Paper 2014-2020, C(2018)3442, adopted on 31 May 2018, refers to the importance of digital development for the future economy and society of the Western Balkans. Cybersecurity is essential in keeping the digital economy and society healthy and successful. In addition, enhanced cybersecurity in the Western Balkans is of benefit to the EU.

- Western Balkans Strategy flagship 2 (Security) and 5 (Digital Agenda) both stress the need to address cybersecurity in the region. This action document is the direct result of these references.

- EU-Western Balkans Sofia Declaration and the Sofia Priority Agenda both refer to the importance of the development of the digital economy and society in the Western Balkans. Cybersecurity is essential in ensuring the successful development.

- The Council conclusions on EU External Cyber Capacity Building Guidelines, adopted by the General Affairs Council at its 3629th meeting held on 26 June 2018, include the following references relevant to this action:

"STRESSES the need to prioritise the EU's cyber capacity building efforts in its neighbourhood and in developing countries with fast connectivity growth, as indicated in its Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU21 and in general to pursue evidence-based prioritisation on the basis of internet access growth statistics, strategic interests and threat assessments such as Europol's Internet Organised Crime Threat Assessment (iOCTA) and ENISA's Threat Landscape Reports, with the aim of closing the cyber capability gap;

STRESSES the need to ensure coherent and efficient use of resources by the EU and its Member States, to make full use of the relevant EU external financial instruments and programmes, and to leverage the expertise of EU Member States' national competent cyber authorities, the EU's relevant specialised agencies (notably ENISA, EC3 at Europol, Eurojust, CEPOL and eu-LISA), and networks (e.g. European Cyber Crime Training and Education Group, European Judicial Cybercrime Network) as well as existing expert, academic, technical and industry networks (for example GÉANT, FIRST and Meridian);

WELCOMES the proposal to set up an EU External Cyber Capacity Building Network to mobilise the collective expertise of EU Member States for EU-funded external cyber capacity building programmes, support effective coordination of EU-funded external cyber capacity building activities, and increase training opportunities in light of proliferating initiatives in partner countries and regions and the growing demand for cyber-related training; cooperating with and complementing the GFCE network;

CALLS ON the European External Action Service and the Commission to continue the prioritisation and exchange of information on cyber capacity building activities in their bilateral dialogues with strategic partners as well as at relevant international and regional fora;"

- The yearly EU progress reports (enlargement package) contain references to the need for cybersecurity strategies aligned to the EU's strategies and NIS directive (see result 1.1 in specific).

- EU policy on cyber (the Network and Information Security – NIS – directive, Directive (EU) 2016/1148 and Communication on Strengthening Europe's Cyber Resilience System, COM(2016)410) as well as the EU's Cybersecurity Act proposal COM(2017)477[5] and Joint Communication JOIN(2017)450[6]. This is the legislation and a Commission communication to which the beneficiaries should align (see result 1.1 of this action in specific). The Joint Communication JOIN(2017)450 notes: "Evidence suggests that people from around the globe identify cyber-attacks

5 https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF
6 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2017:450:FIN

from other countries as among the leading threats to national security. Given the global nature of the threat, building and maintaining robust alliances and partnerships with third countries is fundamental to the prevention and deterrence of cyber-attacks – which are increasingly central to international stability and security. The EU will prioritise the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements."

- Multi-annual Action Plan for a Regional Economic Area in the Western Balkans[7] – Digital integration pillar section IV.2.1. "Enhance Cybersecurity, trust services and data protection". This section contains the following actions: harmonisation of cybersecurity in the region, identification and protection of critical infrastructures, setting up of a regional dialogue and information exchange between CSIRTs in the region, strengthening the capacities of CSIRTs, and establishing a regional dialogue and information exchange between authorities in charge of network and information security. The results of this action listed below (under intervention logic) cover all these points.

- This action document builds on the United Kingdom action 2018-2020 (implemented by Geneva Centre for the Democratic Control of Armed Forces) focussing its training on Montenegro and Serbia and providing regional round tables to the Western Balkans region.

- The results on cooperation and on identification and protection of operators of essential services this action document are in line with the Joint Counter-terrorism Regional Action plan[8], which was adopted by the Western Balkans on 5 October 2018. In particular its objective 5: "Strengthen the protection of citizens and infrastructure". This objective points out that each Western Balkan partner should seek amongst others to: improve the protection of its public spaces as well as of its critical infrastructure, to enhance the protection of its cyberspace, and to engage in sharing best practices. The objective also points out that the EU should seek: to continue to invite Western Balkans partners to identify concrete projects and topics for cooperation (e.g. specialised trainings, sharing of good practices on critical infrastructure protection, hybrid threats and cyber security), and to share guidance and best practices for the protection of public spaces.

- The action is in line with the "Joint Framework on countering Hybrid Threats" with specific focus on action 18, which tasks HRVP Mogherini and the Commission to launch hybrid risk surveys in partner countries to build partners' capacities and strengthen their resilience to hybrid threats. The Joint Framework in particular stresses the need to build resilience in the protection of critical infrastructure and cybersecurity as a whole, as well as to increase cooperation with third countries. These are all key aspects addressed in this action document.

- The action document has been drafted keeping in mind the "EU operational guidance for the EU's international cooperation on cyber capacity building"[9].

OTHER KEY REFERENCES

- The EU financed study commissioned by the RCC "A New Virtual Battlefield" indicates that all Beneficiaries progress in cybersecurity, however more needs to be done. The study gives recommendations on bilateral and regional level.

- "Guide through Information Security in the Republic of Serbia 2.0"[10], by OSCE, November 2018.

---

7 https://www.rcc.int/docs/383/multi-annual-action-plan-for-a-regional-economic-area-in-the-western-balkans-six
8 https://ec.europa.eu/home-affairs/news/signature-joint-action-plan-counter-terrorism-western-balkans_en
9 https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building

10 https://www.osce.org/mission-to-serbia/404255?download=true

- "Cybersecurity Capacity Review – North Macedonia"[11], July 2018, conducted in cooperation with the World Bank and the University of Oxford.

- Annual reports by the International Telecommunications Union: "Global Cybersecurity Index" (GCI). As well as recent actions undertaken by ITU on cyber capacity building. CSIRT assessment reports were done in 2018 for Albania and Bosnia and Herzegovina. A cybersecurity strategy workshop for the Western Balkans will be held in 2019 in North Macedonia. A FRIST training conducted for 60 participants, including Western Balkan representatives, took place in Cyprus in 2018. ITU Regional Cyberdrills were conducted in 2017 in Moldova and in 2018 in Cyprus with participation of the Western Balkans. Next Cyberdrill will be in Bucharest in May 2019. A Regional Cybersecurity Forum was held in Bulgaria in 2016 and the next one to be held in 2020 with participation of the Western Balkans. Child Online Conferences will be organised in Albania in February 2019 [Safer Internet Day] with ITU support. Other relevant ITU actions that are open for participation of the Western Balkans are: Regional and International Child Online Protection conferences and the Cybersecurity Public Private Dialogue conferences.

- World Bank reports on cybersecurity maturity levels in cooperation with the Global Cyber Security Capacity Centre and the University of Oxford.

LESSONS LEARNED AND LINK TO PREVIOUS FINANCIAL ASSISTANCE

This action builds on previous projects of the EU, Council of Europe, Member States, and the European Cybercrime Centre at Europol in the field of cybersecurity and cybercrime. Due to fast developments in some areas, links with previous and existing projects are therefore essential to avoid overlaps in training and other capacity building activities. These links will be established from the onset through contacts with coordinators, including in the Directorate General for International Cooperation and Development and the European External Action Service, of the most recent and relevant projects.

- Project on Enhancing Cyber Security Governance in the Western Balkans. This is an UK funded project for July 2018 - March 2021 and being implemented by Geneva Centre for the Democratic Control of Armed Forces (DCAF). Activities in this IPA action should be aligned to the actions undertaken under the UK project, such as TRANSITS II courses, NATO cyber defence activities, awareness raising activities, capacity development workshops, assessments, round tables and tailored trainings.

- ENCYSEC pilot project, which ran between 2014 and 2016 in Kosovo, Moldova and North Macedonia.

- Cyber@EaP II and III Global Action on Cybercrime: GLACY and GLACY+

- Activities organised in the Western Balkan partners through the European Commission's Technical Assistance and Information Exchange instrument (TAIEX).

- European Programme for Critical Infrastructure Protection (EPCIP) activities.

There are several common lessons learnt from the security-related actions. The challenging security and political context in the relevant beneficiaries, as well as obstacles as massive staff rotation in beneficiary institutions and agencies, can be obstacles in achieving progress or attaining significant consolidation of results. The role of beneficiaries in planning the activities has to be strong in order to facilitate greater ownership and to enhance the effectiveness and sustainability of the actions. A demand-driven approach on the basis of a comprehensive needs assessment is therefore necessary. In addition, the incorporation of human rights safeguards in the design and implementation of such actions is vital to ensure that EU values

[11] http://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

are reflected throughout the implementation of activities.

Specifically in the area of cybersecurity, one of the main challenges and lessons learnt from previous projects developed by the Directorate-General for International Cooperation and Development is that the policy and technical communities and stakeholders do not cooperate, especially between the security authorities and the business sector. Different communities, officials/diplomats, security experts, and law enforcement and development agencies need to work together more effectively in order to ensure greater security of networks and essential services. Evidently, cybersecurity, especially when owned by a defence, law-enforcement or intelligence community in a country can complicate trust-building between different policy communities.

On a technical level, in relation to CSIRT capacity building, it seems that experts are working well together due to the nature and aims of their work. On the other hand, in the strategic realm close attention is necessary for fostering a multi-stakeholder involvement. In terms of the potentially leading role academia can play, while many universities in third countries have curricula in place, there is lack of infrastructure to efficiently execute the research agenda.

2. INTERVENTION LOGIC

LOGICAL FRAMEWORK MATRIX

OVERALL OBJECTIVE	**OBJECTIVELY VERIFIABLE INDICATORS (*)**	**SOURCES OF VERIFICATION**	
To support the Western Balkans in increasing and enhancing their cyber-resilience capacities, using a rights-based and whole-of-government approach, to better address the challenges of cyber threats and improve their overall security.	IPA II beneficiary's position in SMART study - *Monitoring Digital Economy and Electronic Communications Services in the Western Balkans and Turkey.* IPA II beneficiary's position at ITU's Global Cybersecurity and Cyber-wellness Index	SMART study - *Monitoring Digital Economy and Electronic Communications Services in the Western Balkans and Turkey.* Annual progress reports. Civil society scrutiny reports on oversight of national cybersecurity policies and executive measures (privacy/surveillance, freedom of expression online, access to content). OECD "Competitiveness in South East Europe: a Policy Outlook" Oxford University Global Cyber Security Capacity Centre's Cyber Security Capability Maturity Model ITU IMPACT programme	
SPECIFIC OBJECTIVE	**OBJECTIVELY VERIFIABLE INDICATORS (*)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
1) To create and/or strengthen the cybersecurity system at beneficiary level (including through the development and implementation of cybersecurity strategies and the development and implementation of legislation and action plans, in line with the NIS directive); 2) To increase the operational capabilities of competent authorities in the relevant IPA II beneficiaries to deal with cyber threats and incidents and to mitigate risks (including through clear mandates for competent authorities); 3) To identify and strengthen the protection of critical information infrastructure as provisioned by operators of essential services in the Western Balkan region.	Number of laws, strategies, and competent authorities established and/or improved (in line with NIS directive). Number of mandates of competent authorities established/improved. Number of operators of essential services/critical infrastructures identified/strengthened.	International indices of cyber security preparedness, namely: • Global Forum for Cyber Expertise • Cyber Readiness Index 2.0 (Potomac Institute for Policy Studies) • Estonian eGovernment Academy (National Cyber Security Index)	Political stability in the region No major adverse events occurs (national security, natural hazard, cyber attack, or public health crisis) Ownership of the programme by the Western Balkans
RESULTS	**OBJECTIVELY VERIFIABLE INDICATORS (*)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
Result 1: 1.1 Cybersecurity strategies and legislation in line with NIS directive are adopted and (being) implemented after the start of this action. 1.2 Cooperation established between the competent authorities in the relevant IPA II beneficiaries as well as with experts from EU Member States has been established and/or improved. 1.3 Increased cyber awareness and hygiene across all layers of society through awareness raising campaigns and civil society engagement. 1.4 Increased involvement and participation of the private sector and civil society in the development and implementation of cybersecurity policies and measures, for example thought public private partnerships.	Number of the relevant IPA II beneficiaries with adopted and implemented cyber strategies and legislation in line with NIS, which were not present at the start of the action. Number of joint cyber operations and investigations in the region. Number of (and attendance to) awareness-raising workshops/campaigns. Number of key private sector entities (especially from critical infrastructure/services) and civil society (including women representatives) participating in the development and/or	Progress reports. Public opinion surveys. Action update reports. Reports from cyber-coordinating Ministries Press releases reports Civil Society reports Regional organisation's reports	Cybersecurity and legislation are implemented and enforced properly to address the challenges of cyber threats and ensure overall security. Cooperation regionally and with Europe (between competent authorities, including CSIRTs) ensures adequate response to incidents and threats. Public and businesses are more aware of cyber risks and have better knowledge to

	implementation of the cyber strategies.	Government reports Security Incident Management Maturity Model 3 (SIM3) assessments TF CSIRT (Geant) FIRST Trusted Introducer Freedom House's Freedom on the Net report	avoid becoming a victim. Private sector and civil society concerns and opinions have been taken on board in development and implementation of strategies, legislation and policies. Competent authorities (including CSIRTs) have clear mandates and are fully operational. Competent authorities staff has been trained and capacity increased to adequate level. Operators of essential services have been mapped properly and risks related to those essential services managed effectively using proper frameworks. Good cooperation exists between CSIRTs and identified operators of essential services.
Result 2: 2.1 Clearly established competent authorities in cybersecurity with clear mandates. 2.2 Increase capacity of personnel to deal with cyber attacks and mitigate risks and a clear mandate of the CSIRT. 2.3 CSIRTs designated and operational capacities for incident management created and further strengthened, taking into account the respective levels of readiness. 2.4 Cooperation between designated CSIRTs in the Western Balkan region increased. 2.5 Increased international recognition and trust of CSIRTs in the Western Balkan region.	Number of CSIRTs established and/or functional in the Western Balkans region. Number of staff and division of labour of each CSIRTs (including incident responders, threat analysts, IT support, computer forensics, a manager and lawyer/public relations-communications expert). Number of formal or informal cyber information sharing networks created and/or enhanced, that facilitate incident report sharing/early warning/mitigation of serious cyber incidents. Number of CSIRTs that are recognized by private sector and key government agencies as central and international focal points for cyber incidents. Number of CSIRTs that have a training programme in place and are part of the international professional cyber associations (e.g. TF CSIRT, FIRST, Trusted Introducer). Number of table-top exercises and mock operations undertaken within the action framework.	ProjectAction update reports. Reports from cyber-coordinating Ministries Press releases CSIRT reports Civil Society reports Regional organisation's reports Government reports (including statistical office reports)	
Result 3: 3.1 Mapping of operators of essential services in line with the NIS directive. 3.2 Strengthened management and mitigation of the cybersecurity risks posed to the operators of essential services. 3.3 Framework developed on managing and responding to major cybersecurity incidents relating to operators of essential services. 3.4 Cooperation between designated CSIRTs within and between relevant IPA II beneficiaries and operators of essential services on managing cybersecurity incidents improved.	Number of Western Balkans IPA beneficiaries adopting NIS approach to protecting digital assets through identification of operators of essential services. Number of IPA beneficiaries where the incident response organisations are organisationally linked to the its crisis response framework, and there is an elected/political/democratic oversight on the activities of this technical organisation. Number of cooperation MoUs signed between governments and private sector stakeholders.	Action update reports. Reports from cyber-coordinating Ministries Press releases CSIRT reports Civil Society reports Regional organisation's reports	

DESCRIPTION OF ACTIVITIES

For each result, non-exhaustive list of activities and deliverables are suggested below.

A prioritisation system will be stablished to focus first on the institutional governance and legal and policy framework, and subsequently the technical, operational and cooperation activities.

The overall objective of this action is to increase and enhance the cyber-resilience of the IPA II beneficiaries to better address the challenges of cyber threats and improve their overall security. The action will also build on a regional, individual and multi-country approach, promoting EU best practice and ensuring compliance with human rights.

Specific objective 1: To create and/or strengthen the cybersecurity system (including through the development and implementation of cybersecurity strategies and the development and implementation of legislation and action plans, in line with the NIS directive).

Result 1.1 Cybersecurity strategies and legislation in line with NIS directive are adopted and (being) implemented after the start of this action.

- Capacity building across all the objectives through the provision of legal advice, strategic and operational analysis and institutional set-up guidance, including technical assistance and advice for the definition and implementation of cybersecurity priorities, incorporating modules on human rights, data protection safeguards and oversight.

- Steer, assist and support the elaboration of amendments to legislation, or to the formulation new legislation proposed, in accordance with the EU legal framework – i.e. NIS Directive.

Result 1.2 Cooperation established between the competent authorities in the relevant IPA II beneficiaries as well as with experts from EU Member States has been established and/or improved.

- Bilateral and multi-country training sessions (including train-the-trainers) and round tables to ensure proper mechanisms to cooperate internationally are established and/or improved.

Result 1.3 Increased cyber awareness and hygiene across all layers of society through awareness raising campaigns and civil society engagement.

- Bilateral, multi-country and regional training modules and mentoring cycles addressing the concerned stakeholders (also via a train-the-trainers approach) of relevant public officials, including on cyber threats and response, cyber-hygiene, human rights, data protection safeguards and oversight mechanisms;

- Public awareness raising campaigns and trainings organised and delivered to inform citizens, businesses and civil society organisations about cyber threats and to improve their consciousness of individual cyber hygiene.

Result 1.4 Increased involvement and participation of the private sector and civil society in the development and implementation of cybersecurity policies and measures, for example through public private partnerships.

- Set-up dialogues with private sector and civil society on cybersecurity and cyber hygiene;

- Support the revision, update and/or conclusion of cooperation agreements with the private sector service providers through orkshops at relevant IPA II beneficiary level and regional activities, including the development of procedures for access and/or exchange of data held by private

sector entities, as well as training on the application of standard templates and procedures for access to data through case studies and simulation exercises (bilateral or regional level);

Specific objective 2: To increase the operational capabilities of competent authorities in the relevant IPA II beneficiaries to deal with cyber threats and incidents and to mitigate risks (including through clear mandates for competent authorities).

Result 2.1 Clearly established competent authorities in cybersecurity with clear mandates.

- Bilateral and multi-country training sessions and round tables to establish/improve national competent authorities as well as assistance and support in the formulation of mandates and possible new legislation or amendments.

Result 2.2 Increased technically trained personnel to deal with cyber attacks and mitigate risks and a clear mandate of the CSIRT.

- Organisation of joint cyber incident management meetings, table-top exercise(s) and mock operations to simulate a cyber-attack situation and operational meetings, to promote inter-agency and trans-national cooperation, trust, transparency, exchange of information and predictability.

Result 2.3 CSIRTs designated and operational capacities for incident management created and further strengthened, taking into account the respective levels of readiness.

- Support to strengthen incident management within CSIRTs through joint cyber incident management meetings, table-top exercise(s) and mock operations to simulate a cyber-attack situation and operational meetings.

Result 2.4 Cooperation between designated CSIRTs in the Western Balkan region increased.

- Regional dialogues/round tables, facilitated by the RCC.

- Support for the organisation of joint cyber operations and investigations;

- Facilitation of operational meetings promoting inter-agency and trans-national cooperation in actual cyber incidents;

- Supporting, promoting and further consolidating existing regional networks.

- Explore whether there is any need, and under which format, for a regional cybersecurity training scheme.

Result 2.5 Increased international recognition and trust of CSIRTs in the Western Balkan region.

- Assistance in preparations to become member of or to participate in activities with international networks such as FIRST.

Specific objective 3: To identify and strengthen the protection of critical information infrastructure as provisioned by operators of essential services in the Western Balkan region.

Result 3.1 Mapping of operators of essential services in line with the NIS directive.

- Technical assistance for the elaboration of critical information infrastructure and private service providers critical for cybersecurity purposes mappings;

Result 3.2 Strengthened management and mitigation of the cybersecurity risks posed to the operators of essential services.

- Develop comprehensive organisational schemes and mechanisms to create links between the incident response organizations or CSIRTs and the relevant IPA II beneficiary's Critical Information Infrastructure Protection systems.

Result 3.3 Framework developed on managing and responding to major cybersecurity incidents relating to operators of essential services.

- Support for the definition of action plans and/or systematic processes for the protection of all critical information infrastructure developed;

Result 3.4 Cooperation between designated CSIRTs within and between relevant IPA II beneficiaries and operators of essential services on managing cybersecurity incidents improved.

- Organisation of joint cyber incident management meetings, table-top exercise(s) and mock operations to simulate a cyber-attack situation and operational meetings, to promote inter-agency and trans-national cooperation, trust, transparency, exchange of information and predictability.

RISKS

Risk (medium level): The multifaceted and rapidly evolving target sector of the action implies that expertise, both at EU and IPA II beneficiary level, might be difficult to find for the implementation phase. *Mitigation*: All possible channels of communication will be used to reach out to the EU Member States (i.e. Council Horizontal Working Party on Cyber Issues) and the private sector since the early stages of the identification phase to raise awareness and interest.

Risk (medium level): Lack of or insufficient Rights Based Approach in the IPA II beneficiaries in their cybersecurity and cybercrime framework and operations. *Mitigation*: Mainstreaming fundamental rights into the programme activities. This will include focusing on an external and internal oversight mechanism.

Risk (low level): Limited interest, trust, and/or stakeholder buy-in. *Mitigation*: The action is developed in direct response to demands from beneficiary governmental bodies and private sector stakeholders. It is extremely unlikely that beneficiaries will not remain committed. Lack of interest, trust and/or buy-in will be overcome through the demonstration of concrete results that can be derived from cooperation. Action activities will be adjusted accordingly should there be limited interest.

Risk (medium level): Share of the list of critical infrastructures per country. *Mitigation:* This risk is only limited, as such lists, considered extremely sensitive, are highly classified and very rarely shared. In the EU, in application of Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, only the number of European Critical Infrastructures (ECIs) and their sector are communicated to the European Commission; all other elements of the identity of such ECIs are kept secret by Member States.

Assumptions: The political and security situation allows for the implementation of action activities and does not deteriorate to an unacceptable level. Government partners remain committed and support action implementation. Trust is built among stakeholders. Relevant IPA II beneficiaries will demonstrate ownership, which is requisite for sustainability of the action deliverables.

CONDITIONS FOR IMPLEMENTATION

The relevant ministries agree to put their legislation as soon as possible in line with the EU's NIS directive and cybersecurity strategy. In addition, governments are committed to ensure the adequate level of human resources for the competent authorities ensuring cybersecurity, such as the CSIRTs.

This will be checked through reporting mechanisms within the action as well as the usual progress reports published by the European Commission each year.

3. IMPLEMENTATION ARRANGEMENTS

ROLES AND RESPONSIBILITIES

The responsibility of the programme lies with the European Commission. The steering of the action will be led by Directorate-General for Neighbourhood and Enlargement Negotiations, Unit D5. Other European Commission services (such as Directorate-General for Communications Networks, Content and Technology and Directorate-General for Development and Cooperation) and the European External Action Service will be closely associated as relevant.

An annual steering committee will be led by European Commission services for reviewing the three results of the action and guide the way forward with main stakeholders.

Regular meetings will be hold between the European Commission and the service provided in a format of a Management Group.

The European Commission will ensure the coordination and communication with the interested stakeholders, including relevant European Commission Services and EU Delegations. Programme-specific contact points shall be nominated at headquarters, in EU Delegations and in field offices to ensure coordinated internal and external communication. The Steering Committee will be chaired by the European Commission, and where relevant of the European External Action Service and of any other concerned Directorate-General of the Commission. ENISA will be invited as observers. The Steering Committee is responsible for monitoring the implementation of the Action on the basis of activity reports presented by the service provider. The Steering Committee shall meet at least twice a year to be updated on the annual activities and for the monitoring of the implementation. With the support of the service provider an annual meeting chaired by the European Commission will be organised with representatives of the Western Balkans. EU Member States may also be invited.

It is the role of the line ministries responsible to ensure a functional legal framework in line with EU legislation as well as cybersecurity strategies are in place. In addition, line ministries should ensure the adequate level of human resources in for the competent authorities ensuring cybersecurity, such as the CSIRTs.

It is the role of the central competent authorities to ensure adequate levels of cyber resilience and capacity to deal efficiently with threats and attacks. Together with the line ministries, the competent authorities have to ensure cooperation regionally and with the EU.

As stipulated in the Multi-annual Action Plan for a Regional Economic Area in the Western Balkans, the RCC is already active as coordinator in cybersecurity in the region. Through this coordinating role the RCC ensures a harmonised regional approach, regional dialogue and the exchange of information. This role will be further enhanced as specified in the action "Strengthening regional cooperation and the development of a competitive Regional Economic Area (REA)" under IPA II Multi-country Action Programme 2019.

The involvement of ENISA as an associate in the implementation of some of the activities will be further described at a later stage (e.g terms of reference).

IMPLEMENTATION METHOD(S) AND TYPE(S) OF FINANCING

The action will be implemented in direct management through procurement. Detail on the eligibility criteria will be defined in the tender document, but the intention would be to ensure the participation of agencies from the European Union member states. The indicative duration of the service contract will be 36 months.

4. PERFORMANCE MEASUREMENT

METHODOLOGY FOR MONITORING (AND EVALUATION)

The action will be monitored by a Programme Manager in the Unit NEAR D.5. This will be done through the Management Information System (MIS), the actions progress reports, the coordination meetings with the implementing body.

The implementing partner shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its results (outputs and direct outcomes) as measured by corresponding indicators, using as reference the logframe matrix. The report shall be laid out in such a way as to allow monitoring of the means envisaged and employed and of the budget details for the action. The final report, narrative and financial, will cover the entire period of the action implementation.

The European Commission may carry out a mid-term, a final or an ex-post evaluation for this action or its components via independent consultants, through a joint mission or via an implementing partner. In case a mid-term or final evaluation is not foreseen, the European Commission may, during implementation, decide to undertake such an evaluation for duly justified reasons either on its own decision or on the initiative of the partner. The evaluations will be carried out as prescribed by the Directorate-General for Neighbourhood and Enlargement Negotiations Guidelines on linking planning/programming, monitoring and evaluation. In addition, the action might be subject to external monitoring in line with the European Commission rules and procedures.

INDICATOR MEASUREMENT

Indicator	Baseline (2010)	Target 2022	Final Target (2023)	Source of information
Number of laws, strategies, and competent authorities established and/or improved (in line with NIS directive).	**0**	**1 law, strategy and competent authority / beneficiary (at least partially)**	**1 law, strategy and competent authority / beneficiary**	Progress reports, government reports, CSIRT reports, Action update reports.
Number of mandates of competent authorities established/improved.	**0**	**4**	**6**	Progress reports, government reports, CSIRT reports, Action update reports.
Number of operators of essential services/critical infrastructures identified/strengthened.	**0**	**4 / beneficiary**	**6 / beneficiary**	Government reports, CSIRT reports, Action update reports.
Number of the relevant IPA II beneficiaries with adopted and implemented cyber strategies and legislation in line with NIS, which were not present at the start of the action.	0	6	6	Progress reports.
Number of joint cyber operations and investigations in the region.	0	1 / year	2	CSIRT reports
Number of awareness-raising workshops/campaigns.	0	1 / year / beneficiary	1 / year / beneficiary	Actionupdate reports.
Number of key private sector entities (especially from critical infrastructure/services) and civil society (including women representatives) participating in the development and/or implementation of the cyber strategies.	0	10	30	Civil Society reports, Action update reports.
Number of CSIRTs established and/or functional in the Western Balkans region.	0	6	>6	Government reports, CSIRT reports.
Number of formal or informal cyber information sharing networks created and/or enhanced, that facilitate incident report sharing/early warning/mitigation of serious cyber incidents.	0	1	3	CSIRT reports, TF CSIRT (Geant) , FIRST, Trusted Introducer.
Number of staff and division of labour of each CSIRTs (including incident responders, threat analysts, IT support, computer forensics, a manager and lawyer/public relations-communications expert).	0	3 (depending on beneficiary)	6 (depending on beneficiary)	Government reports, CSIRT reports, Action update reports.
Number of CSIRTs that are recognized by private sector and key government agencies as central and international focal points for cyber incidents.	0	3	6	Government reports, CSIRT reports, Action update reports.
Number of CSIRTs that have a training programme in place and are part of the international professional cyber associations (e.g. TF CSIRT, FIRST, Trusted Introducer).	0	6	>6	Government reports, CSIRT reports, TF CSIRT (Geant), FIRST, Trusted Introducer.
Number of Western Balkans IPA beneficiaries adopting NIS approach to protecting digital assets through identification of operators of essential services.	0	4	6	Government reports, CSIRT reports, Action update reports.

Number of IPA beneficiaries where the incident response organisations are organisationally linked to the its crisis response framework, and there is an elected/political/democratic oversight on the activities of this technical organisation.	0	4	6	Government reports, CSIRT reports, Action update reports.
Number of cooperation MoUs signed between governments and private sector stakeholders.	0	6	12	Government reports, Action update reports.
Number of table-top exercises or mock operations undertaken within the project framework.	0	2	3	Government reports, Action update reports.

5. CROSS-CUTTING ISSUES

GENDER MAINSTREAMING

In addition, the action will strive to promote gender equality and equal opportunities in all activities and trainings. Gender equality incentives will be incorporated particularly in capacity building activities. Also, where possible, collected data will be gender-disaggregated. The action will strive to encourage women to build their up their cyber skills and encourage governments to motivate girls and women to study ICT and cybersecurity.

In addition, cyber- violence against women and girls (VAWG), is a global problem with serious implications for societies and economies around the world. The statistics pose risks to the peace and prosperity for all enshrined in the Charter of the United Nations, and, in particular, to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement. The sheer volume of cyber VAWG has severe social and economic implications for women and girls and responses have yet to be fully addressed.

There exist various forms of cyber VAWG, including, but not limited to, online harassment to the desire to inflict physical harm including sexual assaults, murders and suicides, cyber stalking, non-consensual pornography (or 'revenge porn'), 'sextortion', and electronically enabled trafficking.

Research suggests that women are disproportionately the targets of certain forms of cyber violence compared to men. In line with the international human rights legal framework, including the Istanbul Convention, this action will accompany the IPA II beneficiaries to improve institutional responses to cyber VAWG, in order to protect women both online as well as offline. The action will raise awareness about VAWG and encourage governments and/or civil society organisations to take this problem into account in the awareness raising activities on cybersecurity at IPA II beneficiary level.

EQUAL OPPORTUNITIES

All activities under this action will be designed and implemented in accordance with the principles of good governance and human rights, gender equality, the inclusion of socially or economically deprived groups and environmental sustainability, wherever these issues are of particular relevance to the institutions and beneficiaries to be assisted.

Cybersecurity, also in relation to capacity building, involve a wide range of stakeholders including from national security and law enforcement agencies. Therefore, particular focus should be placed in the incorporation of safeguards in the proposed action in relation to human rights, data protection and good governance, in line with the EU Cybersecurity Strategy, the EU Strategic Framework and Action Plan on Human Rights and Democracy, and the EU Human Rights Guidelines on Freedom of Expression Online and Offline. The 2015 EU Council Conclusions on Cyber Diplomacy reaffirm the need to "foster open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures".

Strengthening domestic security and prosecution capacity, whilst strongly integrating human rights, may help mitigate the risk of "cultures of impunity" becoming entrenched. In this light, all assistance and training aspects must include precautionary measures to assure international human rights standards and norms are met.

In providing technical assistance and capacity building, the issue of corruption will be carefully considered. To mitigate the challenges posed by corruption, anti-corruption actions will be comprehensively integrated into the training and awareness raising activities.

MINORITIES AND VULNERABLE GROUPS

Participation in the implementation of the action will be based on equal access regardless racial issues or ethnic origin, religion and beliefs, age or sexual orientation. Besides, the infrastructure investment projects shall provide benefits to groups of population without distinction, including people belonging to minorities and vulnerable groups.

ENGAGEMENT WITH CIVIL SOCIETY (AND IF RELEVANT OTHER NON-STATE STAKEHOLDERS)

The involvement of Civil Society Organisations (CSOs) important for this action. As indicated in results 1.3 and 1.4, respectively "Increased cyber awareness and hygiene across all layers of society through awareness raising campaigns and civil society engagement" and "Increased involvement and participation of the private sector and civil society in the development and implementation of cybersecurity policies and measures, for example thought public private partnerships".

CSOs are one of the key stakeholders alongside government actors, the private sector and community representatives. Engagement of stakeholders should take place through all stages of the action. Some activities that help to ensure meaningful engagement include consultative processes, communication concerning initiatives, dialogue and coordination efforts.

Developing robust and sustainable partnerships between the government and other actors in society (i.e. the private sector, civil society organisations, research institutes) is key for ensuring the whole-of-society approach. Resources for cyber resilience building are distributed at many levels (i.e. individual, community, state) so it is crucial that responsibilities at each are clearly defined. This implies a capacity to engage stakeholders at the bilateral and international levels, such as to identify, motivate and mobilize stakeholders; create partnerships and networks; promote engagement of civil society and the private sector; manage large group processes and open dialogue; mediate divergent interests; and establish collaborative mechanisms. Public-private partnerships play a particularly important role in this respect as they contribute to building trust and improve the understanding between public-private, private-private and public-public entities[12].

The study "A New Vitual Battlefield" (mentioned above) noted that for proper awareness raising measures the CSOs, community groups, and private sector providers should also be supported to provide information and knowledge in this area, to ensure a multi-layered approach.

The World Summit on Information Society also gives importance to the role of CSOs as it defined internet governance in general as 'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programs that shape the evolution and use of the internet[13] .

Instead of having only the government at the centre of cyber-related decision-making, the European Union has repeatedly confirmed the importance of having all stakeholders involved in internet governance and its commitment to strengthening the multi-stakeholder model, which is supported by like-minded countries.[14]

12 Operational Guidance for the EU's international cooperation on cyber capacity building, p. 61. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf

14 Idem. 43-44.

14 Idem. 43-44.

ENVIRONMENT AND CLIMATE CHANGE (AND IF RELEVANT DISASTER RESILIENCE)

The action has no direct link to the EU environmental acquis and the action does not affect the environment. However, this action is of importance for the protection and management of natural resources such as energy and water supply.

Climate action relevant budget allocation: EUR 0.

6. SUSTAINABILITY

The action is expected to be sustainable beyond its implementation period as it will focus on activities directly assisting in the drafting and implementation of relevant laws, as well as strategies, on cybersecurity. It will build up institutions and technical capacities dealing with cyber threats and attacks.

The action is closely linked to the political goals of the region as expressed in the Multi-annual Action Plan for a Regional Economic Area (MAP REA), adopted at the summit in Trieste in 2017. These goals were reconfirmed through the statement of support signed by Western Balkan leaders at the Sofia Summit in 2018.

In addition, through the regular letters of Commissioner Hahn to the beneficiaries about the MAP REA priorities, the importance of building up staff and budget for cybersecurity has been stressed. Implementers of the various activities will further stress the importance that trained officials and contact points remain at these positions for a significant amount of time or that a proper internal handover is ensured so that the competencies acquired will remain in the institutions and not attached to the person itself.

Furthermore, the action aims at levels of alignment with EU *acquis* and of internal capacity that would enable beneficiaries to engage continuously in European and International cybersecurity networks, sharing best practices and participating in trainings in order to stay up to date with fast evolving developments.

The EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber-stability, as well as contributing to Europe's strategic autonomy and security in cyberspace, always guided by the EU's core values and fundamental rights. The EU prioritises the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements. As part of the strategic framework for conflict prevention, the EU promotes the application of international law, and in particular the United Nations Charter, in cyberspace.

7. COMMUNICATION AND VISIBILITY

Communication and visibility will be given high importance during the implementation of the action. The implementation of the communication activities shall be funded from the amounts allocated to the action.

All necessary measures will be taken to publicise the fact that the action has received funding from the EU in line with the EU communication and visibility requirements in force. All stakeholders and implementing partners shall ensure the visibility of EU Financial assistance provided through IPA II throughout all phases of the programme cycle.

Visibility and communication actions shall demonstrate how the intervention contributes to the agreed programme objectives and the accession process as well as the benefits of the action for the general public. Actions shall be aimed at strengthening general public awareness and support of interventions financed and the objectives pursued. The actions shall aim at highlighting to the relevant target audiences the added value and impact of the EU's interventions and will promote transparency and accountability on the use of funds.

Visibility and communication aspects shall be complementary to the activities implemented by the Directorate-General for Neighbourhood and Enlargement Negotiations and the EU Delegations in the field. The European Commission and the EU Delegations shall be fully informed of the planning and implementation of the specific visibility and communication activities.

This action shall contain communication and visibility measures, which shall be based on a specific Communication and Visibility Plan of the action, to be elaborated at the start of implementation.

The contractor and the European Commission will develop a joint consolidated communication and visibility plan for the action based on an agreed communication narrative and master messages customised for the different target audiences (stakeholders, civil society, general public, etc.).Key results will be communicated to all governmental, non-governmental and other stakeholders. All reports and publications produced will be widely disseminated. All activities will adhere to the European Union requirements for visibility on EU-funded activities. This shall include, but not be limited to, press releases and briefings, reports, seminars, workshops, events, publications.

Outreaching/awareness raising activities will play a crucial part in the implementation of the action (esp. cyber awareness). The implementation of the communication activities shall be the responsibility of the contractor and shall be funded from the amounts allocated to the action.

The contractor shall report on its visibility and communication actions, as well as the results of the overall action to the relevant action committees and the European Commission as appropriate. This action will be communicated externally as part of a wider context of EU support to the beneficiary, where relevant, and the Western Balkan region in order to enhance the effectiveness of communication activities and to reduce fragmentation in the area of EU communication.

Effectiveness of communication activities will be measured inter alia through public surveys in the IPA II beneficiaries on awareness about the action and its objectives, as well as the fact that it is funded by the EU.

The contractor shall coordinate all communication activities with EU Delegations as well as regional communication initiatives funded by the European Commission to the extent possible. All communication strategies developed as part of this action shall ensure they are in line with the priorities and objectives of regional communication initiatives supported by the European Commission, such as the "Digital Agenda for the Western Balkans".