EN

ANNEX

Neighbourhood, Development and International Cooperation Instrument (NDICI) – Global Europe

Exceptional Assistance Measure regarding the Western Balkans

1. IDENTIFICATION

Action:	Supporting resilience to cybersecurity threats in the Western Balkans
Action Reference:	NDICI CR 2023 / 45
Cost:	EUR 1 800 000 (European Union (EU) contribution).
Budget Line:	14 02 03 10
Duration:	Maximum 18 months. The authorising officer responsible may decide to extend this period twice by a further period of up to six months, up to a total maximum duration of 30 months, under the conditions laid down in Article 23(6) of Regulation (EU) 2021/947.
Lead service:	FPI

2. ACTION SUMMARY

This 18-month exceptional assistance measure takes further steps towards building up operational cyber response capacity in Albania, Montenegro and North Macedonia in the short term. The goal is to empower the governments' technical agencies to address the risks of cyber incidents in the short term, assess how these incidents impact networks of government entities or critical service providers, collect and share data across government to help understand and respond to attacks and thus limit their adverse impact. While Albania, Montenegro and North Macedonia are at a similar level of preparedness on cyber incident response, the action will respond to the specific domestic needs of each partner country.

This action is in line with the Tirana Declaration of 6 December 2022 on the occasion of the EU-Western Balkans Summit, which stressed the EU's determination to step up its support for resilience against cyberattacks in the Western Balkans and increase cooperation on cybersecurity. While the action focusses on enhancing capacity in the form of rapid and targeted assistance to the national agencies concerned, it also complements previous EU interventions, ongoing and future EU-financed activities under the Instrument for Pre-accession Assistance III, targeting the entire region.

3. BACKGROUND AND RATIONALE

3.1 BACKGROUND

The repercussions of the unprovoked and unjustified Russia's war of aggression against Ukraine heighten the threats to democratic integrity in the wider region.

The level of cybersecurity threats has also markedly increased, affecting some of the EU's partners in the region. North Macedonia, Albania and Montenegro were declared "unfriendly States" by Russia, following their full alignment with the EU sanctions against Russia. Hacktivism has been posing a threat of malicious cyber activities against official networks and critical infrastructure.

In July 2022, Albania suffered a cyberattack that seriously compromised government data and shut down services. Between September and December 2022, cyber actors launched another wave of cyberattacks against Albania, leading to the country becoming the first in history to sever diplomatic ties over a cyberattack.

The digital infrastructure of Montenegro has been affected by a series of unprecedented cyberattacks starting as of the second half of 2022, causing damage to the entire State administration and the system of services to citizens in the period August-December 2022, with the system regaining functionality only in June 2023. The attacks have exposed the vulnerabilities of the country's cybersecurity system linked to institutional setup and capacities. During the period of March-June 2023, the country reported further attempted breaches of its cybersecurity systems ahead of and during presidential and legislative elections, demonstrating the potential of cyberattacks to interfere with democratic processes with potential implications for subsequent electoral processes scheduled in May 2024 in North Macedonia.

During his visit to the region in March 2023, the High Representative/Vice President noted the need to address related challenges and promised to further step up support for information resilience and cybersecurity. The present situation makes it necessary to adopt an exceptional assistance measure regarding the selected partner countries in the Western Balkans.

3.2 RATIONALE FOR CRISIS RESPONSE ACTIONS UNDER THE RAPID RESPONSE PILLAR OF THE NEIGHBOURHOOD, DEVELOPMENT AND INTERNATIONAL COOPERATION INSTRUMENT

The Russia's war of aggression against Ukraine continues to pose a high level of cybersecurity threats having the potential to negatively impact regional stability. Given the close proximity of Albania, Montenegro and North Macedonia to the EU and their increasing level of integration, there is a real risk of escalation and spillover effects of such activities manifesting in the EU, its Member States and other partner countries. The initial assistance provided has bore good results but the needs continue to be significant. This constitutes an exceptional and unforeseen situation in the sense of Article 4(4) (a) of the NDICI Regulation.An adequate response cannot be provided under any other European Union Instrument due to the urgency with which the funds are required and due to available resources already being firmly committed.

Annex IV, paragraph 1, second paragraph, points (d), (f) and (n) of Regulation (EU) 2021/947 specifically provides for the use of the NDICI rapid response pillar to provide (d) support for the development of democratic, pluralistic state institutions, including measures to enhance the

role of women in such institutions, effective civilian administration and civilian oversight over the security system, as well as measures to strengthen the capacity of law enforcement and judicial authorities involved in the fight against terrorism, organised crime and all forms of illicit trafficking; (f) support for reinforcement of State capacity - in the face of significant pressures to rapidly build, maintain or restore its core functions, and basic social and political cohesion, and (n) support for measures to promote and defend respect for human rights and fundamental freedoms, democracy and the rule of law, and the related international instruments.

3.3 RISKS AND ASSUMPTIONS

Risk	Risk level H/M/L	Mitigation measures
Increased cyber capabilities could be used for illegitimate or illegal activities.	**L**	The implementing partner to be identified will be required to build capacity in line with relevant international norms, European standards and best practices, minimising the risk of abuse. The main beneficiaries of the cybersecurity support are State authorities responsible for the legality in the area of cybersecurity.
Necessary capacity-building for the functioning of the new cybersecurity capabilities exceeds the duration of the action.	**M**	Close cooperation with all actors along the humanitarian-development peace-nexus is ensured to improve the conditions for sustainability and a sound continuation of the established capacities after the end of the 18-month action.
Lack of coordination among donors resulting in duplication of efforts or inefficient allocation of resources.	**M**	The design of the action specifically includes provisions for improved donor coordination. The EU Delegations in the region will be closely involved in the action and will participate in coordination with EU Member States and other donors.

4. OBJECTIVES

4.1 OVERALL OBJECTIVE

The overall objective of the action is to support partners in the Western Balkans in responding to increased cybersecurity threats in the region as a result of the Russia'swar of aggression against Ukraine and other risk factors.

4.2 SPECIFIC OBJECTIVES

4.2.1 To contribute to the establishment of Security Operations Centres/Computer Security Incident Response Teams (CSIRTs), in Albania, Montenegro and North Macedonia in order to respond effectively to the risks and threats of cyberattacks.

4.2.2 To contribute to the capacity of Albania, Montenegro and North Macedonia to coordinate their response to large-scale cybersecurity incidents and crises effectively at national level, regionally with each other, and with the EU and EU Member States, including with relevant EU level bodies and networks.

4.2.3 To mitigate and manage the risk of cyberthreats to the resilience of democratic institutions and processes in the target countries.

5. ACTION COMPONENTS AND EXPECTED RESULTS

This exceptional assistance measure will strengthen cybersecurity capacities in Western Balkans states with an elevated hybrid threat level, notably Albania, North Macedonia and Montenegro.

The main expected results/outcomes include:

Expected Result (1): Strengthened capacity of Albania, North Macedonia and Montenegro to detect and effectively counter cybersecurity threats in the short term.

Activities (indicative):

5.1.1 Facilitate the design of frameworks assigning roles and responsibilities for the national competent cybersecurity authorities and other involved government agencies;

5.1.2 Enable the formulation of procedures and information sharing practices regarding the notification and classification of cyber incidents and vulnerabilities;

5.1.3 Provide tools for network traffic identification, monitoring, logging and to systematically assess cyber risks, vulnerabilities and incidents;

5.1.4 Provide training in monitoring capabilities and the use of analysis tools (incident response; logging, alerting, archiving; performing cyber threat intelligence while deploying open-source tools; and monitoring operations for the security of networks and data centres);

5.1.5 Organise exercises to validate the technical trainings and test the incident response.

Expected Result (2): Strengthened capacity of Albania, Montenegro and North Macedonia to coordinate responses to large-scale cybersecurity incidents and crises.

Activities (indicative):

5.2.1 Facilitate the establishment of a system to collect network data in a standardised open format across selected government organisations that have agreed to participate in this pilot to aid in the cyber incident analysis;

5.2.2 Strengthen capacity to detect whether cyber incidents have impacted networks of other government entities or critical service providers regionally;

5.2.3 Assist in building in-country preparedness and incident response capabilities in line with the NIS2 Directive.

Expected Result (3): Strengthened resilience of democratic institutions and processes to cyber-threats.

Activities (indicative):

5.3.1 Raise awareness and facilitate preparedness for cyber-risks in the context of democratic processes;

5.3.2 Promote inter-institutional cooperation and among stakeholders (e.g. political parties) to protect the integrity of election results;

5.3.3 Assist with operational capacity and harmonisation of procedures to ensure the security of infrastructure used in democratic processes (i.a. elections, referenda, census).

6. IMPLEMENTATION

6.1 IMPLEMENTATION MODALITIES

The Commission will ensure that the appropriate EU rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures[1].

6.1.1 Indirect management with a pillar assessed entity

This action may be implemented in indirect management with an entity which will be selected by the Commission's services using the following criteria: knowledge of the cybersecurity legal and institutional framework in the Western Balkans region, including expertise in providing support to state agencies and ministries and the relevant regulatory actors. The implementation by this entity entails the strengthening of cybersecurity capacities in Albania, North Macedonia and Montenegro, and will thereby contribute towards the achievement of objectives and results set out in section 4 and 5.

6.1.2 Changes from indirect to direct management mode due to exceptional circumstances

In the unlikely event that exceptional circumstances beyond the Commission's control should make it necessary to change the implementation modality for the described objectives, from indirect to direct management, it would be implemented with a grant (direct award), for the entire EUR 1.8 million envelope. The type of applicants targeted would be non-profit organisations and private companies.

Under the responsibility of the Commission's authorising officer responsible, the recourse to an award of a grant without a call for proposals is justified because the action entails crisis

[1] www.sanctionsmap.eu Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website, it is the OJ version that prevails.

management aid as referred to in Article 195(a) and as defined in Article 2(21) of the Financial Regulation at the date of the Financing Decision.

6.2 INDICATIVE BUDGET

The total European Union contribution under this Financing Decision **will not exceed EUR 1 800 000**. A breakdown among components is provided hereunder, and is indicative.

Indicative budget breakdown

Components	EU contribution (amount in EUR)	Indicative third party contribution, in currency identified
Component 1: Cyber Resilience, composed of		
6.1.1. – Indirect management with a pillar assessed entity	1 800 000	N/A
Total	1 800 000	N/A

6.3 ORGANISATIONAL SET-UP AND RESPONSIBILITIES

The action shall be implemented under indirect management. It will be managed by the Commission, with the support of the European Union Delegations for the monitoring of the action.

6.4 PERFORMANCE AND RESULTS MONITORING AND REPORTING

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process and part of the implementing partner's responsibilities. To this aim, 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 report. Each 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 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 Commission may undertake additional project monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

6.5 EVALUATION

Having regard to the nature of the action, an evaluation will not be carried out for this action or its components.

The 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 financing of the evaluation shall be covered by another measure constituting a financing decision.

6.6 AUDIT

Without prejudice to the obligations applicable to contracts concluded for the implementation of this action, the Commission may, on the basis of a risk assessment, contract independent audits or expenditure verification assignments for one or several contracts or agreements.

The financing of the audit shall be covered by another measure constituting a financing decision.

6.7 COMMUNICATION AND VISIBILITY

The 2021-2027 programming cycle has adopted a new approach to pooling, programming and deploying strategic communication and public diplomacy resources.

It will remain a contractual obligation for all entities implementing EU-funded external actions to inform the relevant audiences of the Union's support for their work by displaying the EU emblem and a short funding statement as appropriate on all communication materials related to the actions concerned. This obligation will continue to apply equally, regardless of whether the actions concerned are implemented by the Commission, partner countries, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU member states.

The 2022 "Communicating and Raising EU Visibility: Guidance for external actions" reference document shall be used to establish the appropriate contractual obligations.

7. COMPLEMENTARITY, COORDINATION AND FOLLOW-UP

Complementarity and coordination will be sought with previous and ongoing crisis response projects, as well as the EU's ongoing development cooperation and humanitarian efforts in the Western Balkans. Particular emphasis will be put on ensuring transitioning into upcoming EU support to strengthen cybersecurity and a more resilient information environment in the region. Given the high level of international interest in supporting the Western Balkans in the response to the ongoing crisis-situation, particular emphasis will also be given to ensuring effective coordination with other donors, particularly EU Member States.