Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

CyberSouth+ project on enhanced cooperation on cybercrime and electronic evidence in the Southern Neighbourhood Region

Project title:	CyberSouth+: Enhanced Cooperation on cybercrime and electronic evidence in the Southern Neighbourhood Region
Project area:	Priority countries: Algeria, Egypt, Jordan, Lebanon, Libya, Morocco, Palestine*[1] and Tunisia
Duration proposed:	36 months (1 January 2024 – 31 December 2026)
Budget proposed:	EUR 3.890.000 million
Funding:	European Union (90%) and Council of Europe (10%)
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

Background and justification

Countries of the Southern Mediterranean region – as societies all over the world – increasingly rely on information and communication technologies (ICT) but with this they are also vulnerable to threats such as cybercrime. Cybercrime – that is offences against computer systems and by means of computers – affects individuals, institutions and organisations as well as States. Increasing ransomware and other types of attacks against critical information infrastructure underline the need for synergies between criminal justice responses to cybercrime and measures to enhance cybersecurity.

Moreover, evidence in relation to any crime is now often stored on computer systems. Any criminal justice response to the challenges of cybercrime and e-evidence is needed that is both effective and meeting human rights and rule of law requirements. With the Convention on Cybercrime (Budapest Convention) and its Protocols a framework for such a criminal justice response is available. Morocco is a Party to the Convention; Tunisia has been invited to accede and expected to become a Party in February 2024. Algeria, Jordan and Lebanon have adapted or are in the process of adaption their domestic criminal law to the requirements of the Convention.

The new Second Additional Protocol to this treaty on enhanced cooperation and disclosure of electronic evidence that was opened for signature in May 2022 provides new and innovative tools.[2] Morocco was among the signatories in May 2022.

The Council of Europe and the European Union have been working with Algeria, Jordan, Lebanon, Morocco and Tunisia since 2017 through the joint project CyberSouth aimed at strengthening of "legislation and institutional capacities on cybercrime and electronic evidence

[1] * This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of Council of Europe and European Union member States on this issue.

[2] The tools of this Protocol include: direct cooperation with service providers in other Parties for the disclosure of subscriber information and with registrars for domain name registration information; government-to-government cooperation for the production of subscriber information and traffic data; expedited disclosure of data and cooperation in emergencies; joint investigation teams and joint investigations; video conferencing. These tools are backed up by data protection and other safeguards that need to be implemented by Parties.

in the region of the Southern Neighbourhood in line with human rights and rule of law requirements".

With CyberSouth coming to an end in December 2023, a follow up joint project CyberSouth+ is proposed to commence on 1 January 2024.

CyberSouth+ will be aimed at strengthening criminal justice capacities for enhanced cooperation on cybercrime and disclosure of electronic evidence through a combination of regional and country-specific actions that will be tailored to the needs and capacities of each project country. While CyberSouth+ will build upon or further consolidate achievements of the CyberSouth project, the following themes will be added or receive stronger emphasis:

- Legal framework: Support to the reform of domestic legislation not only in line with the Convention on Cybercrime but also its Second Additional Protocol on electronic evidence, including its rule of law and data protection standards.

- Capacities for investigation, prosecution and adjudication of criminal offences: Support to sustainable training programmes on cybercrime and electronic evidence and specialised training courses, including on digital forensics.

- International co-operation: Support the development of practical guides, procedures and templates, and domestic and regional training activities for government-to-government and government-to-private cooperation across borders based on the tools of the Second Additional Protocol.

- Synergies between criminal justice and cybersecurity responses to cyberthreats: Mechanisms for trusted cooperation and reporting between cybersecurity institutions and criminal justice authorities. This component will focus on the links between measures on cybercrime and cybersecurity. Moreover, the project area will be extended. While Algeria, Jordan, Lebanon, Morocco and Tunisia will remain priority countries, CyberSouth+ will also co-operate with Egypt, Libya and Palestine* in project activities and thus share the experience gained so far under CyberSouth through regional and – to the extent feasible – country-specific activities.

The project management structure may be adjusted. While part of the CyberSouth+ management team will again be based at the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, some staff may be located in the Council of Europe office in Tunisia to ensure coordination with the Programme South V of the Council of Europe and the European Union. Tunisia may thus also serve as a hub for the delivery of project activities.

Outcome and expected Outputs

Impact	**To reduce the vulnerability of Southern Mediterranean countries against cyber threats.**
Outcome	**Better prevention and response to cybercrime by State Institutions of the Southern Mediterranean countries in cooperation with the private sector and in line with the Budapest Convention.**
Output 1	**Increased capacities of the competent authorities to introduce regulatory and technical reforms in the areas of cybercrime, electronic evidence and criminal justice response.**
Output 2	**Improved knowledge and specialisation of criminal justice professionals to prevent and fight cybercrime.**
Output 3	**Increased opportunities for international cooperation in the framework of the Budapest Convention and its Second Additional Protocol.**
Output 4	**Improved procedures and tools connecting criminal justice authorities and cybersecurity organisations.**

Contact

Alexander Seger
Head of Cybercrime Division
Council of Europe

alexander.seger@coe.int
+33-3-9021-4506