CyberSouth
Cooperation on cybercrime
in the Southern Neighbourhood

Project concept[1]

Version 9 December 2021

Project title / number (2017/DG1/JP/3692):	CyberSouth – Cooperation on cybercrime in the Southern Neighbourhood Region
Project area:	Southern Neighbourhood Region[2]
	Initial priority areas: Algeria, Jordan, Lebanon, Morocco and Tunisia
Duration:	78 months (June 2017 – December 2023)
Budget:	EURO 5,005,000
Funding:	European Union and Council of Europe
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

BACKGROUND AND JUSTIFICATION

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. Moreover, evidence in relation to any crime is now often stored on computer systems. Accessing and securing volatile evidence on computers domestically or on servers in the cloud is a complex matter.

This is also true for countries of the Southern Neighbourhood. Security, confidence and trust in ICT are needed to allow these societies to exploit the human development potential of ICT.

Governments increasingly consider cybercrime and cybersecurity matters of national security in particular in the light of terrorist use of the Internet, transnational organised crime in cyberspace and reports on attacks and computer intrusions by States or State-backed actors. In some countries, such threats may trigger repressive measures that in turn may threaten rule of law and human rights principles. It is necessary, therefore, to reconcile the positive obligation of governments to protect society and individuals against crime with rule of law, human rights and data protection requirements.

The approach of the Council of Europe on cybercrime addresses this challenge. It is built on the Budapest Convention on Cybercrime and related instruments, such as Data Protection Convention 108 and others. Joining the Budapest Convention entails membership in the Cybercrime Convention Committee (T-CY) and thus cooperation with currently 80 States. Furthermore, the Budapest Convention and the work of the T-CY is backed up by capacity building programmes.

The Budapest Convention is open for accession by any country ready to implement its provisions and to engage in cooperation. From among the States of the Southern Neighbourhood, Israel and Morocco are parties to this treaty. Morocco is a priority country of the GLACY+ joint project of the EU and the Council

[1] The present updated following the extension of the project, provided by the European Commission.

[2] The following ten countries participate in the European Neighbourhood Policy framework of the European Union: Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine*, Syria and Tunisia

(* This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue)

of Europe on Global Action on Cybercrime. Tunisia has also been invited to accede to the Budapest Convention. Morocco and Tunisia have furthermore acceded to the Data Protection Convention 108 of the Council of Europe.

Applying a phased approach, Algeria, Jordan, Lebanon, Morocco and Tunisia would be considered priority countries which may benefit from the full range of support under the present project, while cooperation with other countries would focus on the strengthening of legislation and rule of law conditions for cybercrime and electronic evidence followed by gradual involvement – if feasible – in other activities.

Morocco was a priority country under GLACY (2013-2016) and is a priority and hub country under the GLACY+ project (2016 – 2024). Under GLACY, the feasibility of capacity building activities on cybercrime legislation, training of judges on cybercrime and electronic evidence, law enforcement training, and public/private and international cooperation has already been demonstrated. The tools and materials applied there could be adapted for use in other countries of this region.

It is proposed that Morocco will not only participate in the CyberSouth project but will continue to participate in GLACY+. Morocco would thus serve as a link between the two projects and help share new tools and practices developed under GLACY+ with the countries participating in CyberSouth.

Furthermore, the project will benefit from the experience of joint EU/Council of Europe projects in the Eastern Partnership region (Cybercrime@EAP) and in South-Eastern Europe (iPROCEEDS under the Instrument of Pre-Accession) which are aimed at public/private cooperation and on the confiscation of proceeds from online crime.

OBJECTIVE, EXPECTED RESULTS AND ACTIVITIES

Overall objective	**To contribute to the prevention of and control of cybercrime and other offences involving electronic evidence, in line with international human rights and rule of law standards and good practices.**
Project objective	**To strengthen legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements** End of project target: – An additional two States will be Parties and a further two States will have been invited to accede to the Budapest Convention. – Criminal justice authorities are prosecuting cybercrime and cases involving e-evidence and engage in international cooperation.
Result 1	**Criminal law frameworks strengthened in line with the Budapest Convention on Cybercrime, including rule of law safeguards (Article 15)** End of project target: – At least three additional countries will have the legal framework in line with the Budapest Convention. Another two countries will have draft laws in line with the Budapest Convention. – Cybercrime related provisions are limited by appropriate conditions and safeguards. – Legislative reforms will be initiated in at least two countries for implementing the provisions of the Second Additional Protocol to the Budapest Convention into the national legislation.
Activities:	– Prepare an assessment (study) on the legislation on cybercrime and e-evidence in priority countries and other countries of the Southern Neighbourhood, including legal profiles. – Prepare an assessment (study) on data protection framework in priority countries. – Organise regional workshop on cybercrime and data protection legislation as well as on criminal justice statistics to determine the effectiveness of legislation. – Carry out desk reviews of draft laws and follow up with in-country workshop. – Document jurisprudence regarding cybercrime and e-evidence and publish on Octopus Community. – Support in-country workshops for judges, prosecutors and law enforcement on the application of cybercrime legislation, including rule of law safeguards and data protection requirements. – Support in-country workshops for developing guidelines on conditions and safeguards in cybercrime and e-evidence related investigation. – Support in-country activities in coordination with other EU funded projects for increasing the knowledge of the criminal justice authorities on the link between cybercrime investigations and data protection regulations – Regional and in-country initiatives for promotion of the Second Additional Protocol to the Budapest Convention and support its implementation into the domestic legislation. – In-country activities on cybercrime legislation targeting national policy makers (Parliamentarians and Governmental officials).
Result 2	**Specialised police services and interagency as well public/private cooperation strengthened with a sustainable approach**

	End of project target: – Specialised police units in priority countries are operational and report a 40% increase in investigations. – Use of Standard Operating Procedures for cybercrime investigations and handling of e-evidence.
Activities:	– Prepare an assessment (study) on specialised cybercrime and computer forensic units (police and prosecution) in the Southern Neighbourhood region. – Translate the E-evidence Guide and the Standard Operating Procedures Guide to French and Arabic and Standard Operating Procedures for first responders to cybercrime investigations, Guide on Seizing Cryptocurrencies, Guide on LEA training strategy and Guide on cybercrime criminal justice statistics to Arabic. – Organise a regional workshop on specialised cybercrime and computer forensic units and specialised prosecutors to share experience. – Organise a regional workshop on cybercrime training strategies and access to training materials. – Organise a regional workshop on standard operating procedures for police and prosecutors on e-evidence based on the SOP guide developed under the project. – Organise in-country workshops or otherwise provide advice on the development of domestic SOPs for e-evidence and on the strengthening of cybercrime units. – Hold regional workshops on law enforcement/service provider cooperation with the participation of multi-national service providers. – Hold in-country activities on LEA/ISP cooperation in support of cooperation arrangements. – Organise regional and in-country workshops on interagency cooperation between cybercrime units, financial investigators, financial intelligence units and prosecutors in the search, seizure and confiscation of online crime proceeds. – Organise regional and in-country training events in coordination with other EU funded projects on Darknet, Open-Source Intelligence, Ransomware, and virtual currency investigations. Support the development of the domestic Standard Operating Procedures for the collection, analysis and presentation of electronic evidence – Prepare a Guide for first responders to cybercrime investigations and support the development of a domestic toolkit for First responders/cybercrime investigators. – Support the organisation of a study visit to a country or international organisation for enhancing the international cooperation and sharing of best practices. – Prepare a Guide on Law Enforcement training strategy on cybercrime and e-evidence and provide advice on developing national strategies.
Result 3	**Judicial training on cybercrime and electronic evidence mainstreamed** End of project target: – Modules on cybercrime and electronic evidence are included in the curricula of judicial training institutions and delivered in the five priority countries. – Share of reference magistrates having received basic and advanced training delivered by local trainers. – Pool of national trainers established.
Activities:	– Prepare an assessment (study) on judicial training systems and capabilities in the Southern Neighbourhood region. – Organise a regional workshop for representatives of judicial training institutions to reach agreement on the approach to follow. – Organise in-country training of trainers workshops (in five countries).

	– Support the adaptation of training materials (basic and advanced course). – Support the delivery of the domestic course developed under the project in cooperation with the Judicial Training Institutes. – Support the delivery of TOT training to reference magistrates. – Organise regional conference on the progress made and on the integration of training on cybercrime and e-evidence in the curricula of training institutions. – Support the delivery of the specialised training on cybercrime and e-evidence and facilitate the access to the on-line training platform developed by the Council of Europe.
Result 4	**Criminal justice authorities have better skills and tools for more effective international cooperation on cybercrime and e-evidence** End of project target: – Role and performance of 24/7 points of contact through availability of operating procedures for 24/7 points of contact. By the end of the project, contact points established in the countries that became Parties to the Budapest Convention The other countries will make use of the G7 and Interpol Networks for international cooperation on cybercrime and e-evidence. – Regional (CyberSouth) Judicial Network established in priority countries.
Activities:	– Prepare an assessment (study) on competent authorities and on the functioning of international cooperation in the Southern Neighbourhood region. – Organise a regional/international conference on roles and responsibilities in international police-to-police and judicial cooperation on cybercrime and e-evidence. – Conduct advisory missions on the establishment of 24/7 points of contact. – Organise regional training workshops on international cooperation and the role of 24/7 points of contact (focus on issues such as sextortion and other high interest issues). – Support the participation of representatives of Southern Neighbourhood countries in the Cybercrime Convention Committee, the annual EUROPOL/INTERPOL conferences, and other relevant international meetings and training events. – Regional workshops to support the activities of the CyberSouth Judicial Network. – Regional workshops on the functioning of different networks and their use such as on Budapest 24/7 network, G7 and i24/7 Interpol and the elaboration of operating procedures for 24/7 points of contact. – Support in-country workshops for enhancing the international cooperation through the 24/7 points of contact.
Result 5	**Strategic priorities on cybercrime and electronic evidence identified** End of project target: – Strategic priorities agreed by in priority countries based on analyses of the challenges of cybercrime and electronic evidence and of legislation and institutional capacities to meet these challenges.
Activities:	– Prepare an assessment (study) on current cyber security and cybercrime policies or strategies in the Southern Neighbourhood region. – Organise a project launching conference on cybercrime policies/strategies with the participation of senior officials from the Southern Neighbourhood region. – Support the preparation of (annual) cybercrime and e-evidence situation reports, the development of criminal justice statistics and reinforcement of the dedicated reporting mechanism in five priority countries. – Organise a national cybercrime conference in five priority countries.

	– Prepare an assessment (study) on the progress made with respect to legislation and institutional capacities since the start of the project in the Southern Neighbourhood region. – Organise a regional project closing conference to review progress made and to adopt a set of strategic priorities.

CONTACT

Alexander Seger
Head of Cybercrime Division, Council of Europe
alexander.seger@coe.int

www.coe.int/cybercrime

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