



CyberSEE

Project on enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye

PROJECT SUMMARY

Version 10 January 2024

Project title/number:	CyberSEE: Enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye (3530)
Project area:	Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Türkiye and Kosovo*
Duration:	42 months (1 January 2024 – 30 June 2027)
Budget:	EUR 5,550,000
Funding:	Joint project of the European Union (DG NEAR) and the Council of Europe
Implementation:	Cybercrime Programme Office of the Council of Europe (C-PROC)

BACKGROUND AND RATIONALE

The CyberSEE project on “Enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye”, launched in January 2024, is a joint project of the European Union (Directorate General for Neighbourhood and Enlargement Negotiations) and the Council of Europe, financed by the European Union under the IPA III instrument (90%), and the Council of Europe (10%), and is implemented by the Cybercrime Programme Office of the Council of Europe (C-PROC).

The overall objective of CyberSEE is to strengthen the rule of law, security and regional co-operation in the South-East-Europe and Türkiye through a more effective response to the challenges of cybercrime and electronic evidence. Under this overall objective, the Project implements activities in the region with the specific objective to reach strengthened and more effective criminal justice response of Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Türkiye and Kosovo to cybercrime and electronic evidence, in line with the provisions of the Budapest Convention on Cybercrime, its Second Protocol and European Union objectives.

The expected results are (1) legislation and policy frameworks on cybercrime and electronic evidence improved in line with the Budapest Convention, its Second Protocol and related instruments, (2) capacities of criminal justice authorities strengthened for investigation, prosecution and adjudication of cybercrime offences, as well as for the use of electronic evidence, and (3) capacities of criminal justice authorities enhanced on information exchange with cybersecurity institutions, as well as on international co-operation and co-operation with the private sector, on the basis of the Second Protocol to the Budapest Convention.

CyberSEE builds upon the achievements of the iPROCEEDS projects with stronger emphasis on: investigation of ransomware attacks and the search, seizure and confiscation of virtual currencies that are the proceeds of such crime; the investigation of online child sexual exploitation and abuse (OCSEA); capacities to secure evidence on computer systems; and cooperation between cybersecurity institutions and criminal justice authorities.

** This designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.*

Co-funded
by the European Union



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of Europe

OBJECTIVES AND EXPECTED RESULTS

Project specific objective	Strengthened and more effective criminal justice response of Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Türkiye and Kosovo to cybercrime and electronic evidence, in line with the provisions of the Budapest Convention on Cybercrime, its Second Protocol and European Union objectives.
Immediate Outcome 1	Legislation and policy frameworks on cybercrime and electronic evidence improved in line with the Budapest Convention, its Second Protocol and related instruments.
Output 1.1	The rule of law institutions are better equipped to improve the regulatory frameworks for cybercrime investigation and international co-operation in line with the Budapest Convention and its Second Protocol.
Output 1.2	The rule of law institutions are better equipped to improve or update cybercrime policies or strategies.
Immediate Outcome 2	Capacities of criminal justice authorities strengthened for investigation, prosecution and adjudication of cybercrime offences, as well as for the use of electronic evidence.
Output 2.1	Criminal justice authorities equipped with knowledge and skills for investigation of cybercrime and handling of electronic evidence.
Output 2.2	Criminal justice authorities equipped with knowledge and skills for investigation of ransomware attacks and related proceeds.
Output 2.3	Criminal justice authorities equipped with knowledge, skills and access to specialised tools for the investigation of OCSEA and related electronic evidence.
Immediate Outcome 3	Capacities of criminal justice authorities enhanced on information exchange with cybersecurity institutions, as well as on international co-operation and co-operation with the private sector, on the basis of the Second Protocol to the Budapest Convention.
Output 3.1	Criminal justice authorities equipped with mechanisms trusted co-operation between cybersecurity institutions and criminal justice authorities.
Output 3.2	Competent criminal justice authorities and 24/7 points of contact equipped to apply the tools of the Budapest Convention and its Second Protocol.
Output 3.3	Initiatives for domestic and international public/private co-operation launched on the basis of the Budapest Convention and SAP.

CONTACTS

Daniel CUCIURIANU
 Programme Manager CyberSEE
 Council of Europe
daniel.cuciurianu@coe.int

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