iPROCEEDS-2

Project on targeting crime proceeds on the Internet and securing electronic evidence in South-eastern Europe and Turkey

Summary

Version 6 December 2019

Project title:	iPROCEEDS-2
Project area:	Albania, Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia, Turkey and Kosovo*[1]
Duration:	42 months (1 January 2020 – 30 June 2023)
Budget:	EURO 4, 945, 000
Funding:	European Union and Council of Europe
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

BACKGROUND AND JUSTIFICATION

The region faces common cybercrime threats and challenges. The Organised Crime Threat Assessment for Southeast Europe 2018 (OCTA SEE) notes that cybercrime is continuously growing in the region and that it has been converted into a "business-like concept". Cybercrime is committed both by individuals and organised criminal groups. According to the report, the region witnessed distributed denial-of-service (DDoS) attacks, attacks and malware against mobile devices, ATM malware, skimming, ransomware, cryptojacking or wallet address stealer, SIM BOX frauds, identity thefts, CEO frauds, various types of payment frauds, child online sexual exploitation, etc.

According to data submitted by countries, during 2018 and the first quarter of 2019 the biggest number of reported and investigated cases were related to computer fraud and forgery, data interference and misuse of personal data. Several companies have been scammed through phishing causing damages amounting to hundreds of thousands of Euros, as well as through Business Email Compromise/CEO frauds. The latter targeted business organisations, professionals, and individuals by compromising either business or personal email accounts to send (or cause to be sent) false payment instructions and other information used to conduct financial fraud. Payment by cards still remain a very popular payment method in the region and therefore a target for criminals. Debit and credit cards skimming still represents a major threat. Card-present and card-not-present fraud is widely spread with forged cards and compromised credit card details being used to commit high volume crime, with tens of thousands of victims.

These cybercrimes are driven mostly by financial gain and thus rapid detection and action on illegal money flows on the Internet remains a necessity in order to identify and minimize damages from the criminal activity.

At the same time, the development of new technologies provides criminals with new ways to pursue their illegal goals. Cybercriminals increasingly abuse cryptocurrencies to fund their activities. Bitcoin still remains the primary cryptocurrency encountered by law enforcement, including in the region. The project countries or areas have received extensive training under the current project on investigations related to virtual currencies and the Darknet. However, capacities and investigative tools remain limited in the region. Serbian national authorities are the only one who successfully

[1] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

seized bitcoins. There are several currency exchangers, cryptocurrency ATMs and wallet providers in the region, however these are highly unregulated. Thus, there is a risk that the money launderers would be increasingly lured to use their services.

Darknet continues to facilitate online criminal markets, where criminals sell and purchase illicit products and services in order to engage in other criminal activity and remain anonymous. The Cybercrime Sector of the Ministry of Interior of the North Macedonia is the only authority that created a task force, which monitors and gathers information on illegal activities on the Darknet.

Experience from the iPROCEEDS project shows that capacities of authorities in project countries/areas vary considerably. In some of them, more support is required to strengthen skills in view of increasing the number of cybercrime and parallel financial investigations to search, seize and confiscate proceeds from online crime.

This includes, for example, Montenegro's limited cybercrime and digital forensics investigative capacity; the need for specialised training of new staff of the Special Prosecutor's Office of Serbia and Cybercrime Department of the Ministry of Interior of Serbia; the use of electronic evidence in criminal proceedings in Turkey and the need for training of prosecutors and judges on e-evidence; the need to enhance inter-agency cooperation between prosecution, police forces at state, entities and district levels in Bosnia and Herzegovina, etc.

There is a good level of commitment and interest of relevant authorities in the region, which offers appropriate conditions for further action. Consolidating results achieved and targeted additional support will allow capitalising on the expertise, experience and commitment gained.

At the same time, there are several new areas that require attention.

Cybersecurity represents a high priority for the governments in the region. All the countries have completed the establishment of the Computer Security Incident Response Teams (CIRTs)/ Computer Emergency Response Teams (CERTs) or are in the process of expanding their operations. Often CIRTs have data on incidents that may be most valuable to criminal justice authorities for follow up investigation and prosecution of cyberattacks. To date, sharing of such data remains limited. It is therefore difficult to determine the scale and trends of cybercrime and threats to cybersecurity and thus to inform cybercrime and cybersecurity strategies in this region. Increasing information sharing between CIRTs/CERTs and criminal justice authorities could be considered for further support within this region.

Additionally, important legal initiatives are currently being developed both at the EU level and under the auspices of the Council of Europe. The EU e-evidence proposal[2] will put forward new rules for police and judicial authorities to obtain electronic evidence from service providers. The Cybercrime Convention Committee (T-CY) of the Council of Europe is currently drafting the 2nd Additional Protocol to the Budapest Convention on Cybercrime,[3] which aims at facilitating access to data in the cloud. The new Protocol will include provisions for more efficient MLA, direct cooperation with providers in other jurisdictions and a framework and safeguards for existing practices of extending searches transborder.

[2] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[3] Terms of Reference for the preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime available here:
https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

Furthermore, the entrance into force of the EU General Data Protection Regulation (GDPR)[4], the EU Police Directive[5] and the modernisation of the Council of Europe Data Protection Convention[6] are reshaping the landscape with respect to collection and processing of personal data and transborder data flows. This directly impacts the way in which information is shared between criminal justice authorities, as well as public-private cooperation and access to data held by the private sector.

In addition to these legislative developments, a number of court decisions may also have an impact on how criminal justice authorities can obtain different types of data.[7]

Therefore, the countries of the IPA region require assistance in bringing respective legislation and practices in line with the EU and Council of Europe standards (current and future). The project will work towards ensuring that relevant rules to secure electronic evidence and obtain data from private sector service providers include strong safeguards and guarantee protection of fundamental rights, including the right to the protection of personal data. A swift alignment should be a priority for these countries, as crime investigation and prosecution call for common standards, including in data protection, when information is shared between law enforcement bodies of different countries in order to ensure full respect of fundamental rights and freedoms. This will enhance trust and be a condition for improved public-private and international cooperation.

This project will build on the results achieved during the implementation of the iPROCEEDS project and concentrate on targeted support under the following project areas:

- Legislation regarding securing electronic evidence and access to data in full respect of fundamental rights and freedoms, including privacy and personal data protection.
- Alignment with EU and Council of Europe personal data protection standards.
- Promotion of cybercrime and cybersecurity policies and strategies.
- Interagency and public/private cooperation for investigation of cybercrime and proceeds from crime online.
- Public reporting systems on online fraud and other cybercrime offences.
- Judicial training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures.
- International cooperation and information sharing for investigation of cybercrime and proceeds from crime online.

The bulk of activities will target the specific needs of individual project countries and areas and complement regional activities.

[4] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJEU of 23 May 2018.

[5] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. The directive entered into force on 5 May 2016 and EU countries had to transpose it into their national law by 6 May 2018.

[6] Albania, Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia and Turkey have signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108). The Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) was adopted on 18 May 2018. The Protocol was opened for signature in Strasbourg on 10 October 2018.

[7] See for example the decision of the European Court of Human Rights in Benedik versus Slovenia.

OBJECTIVE, EXPECTED RESULTS AND ACTIVITIES

Specific objective/ Intermediate outcome	To further strengthen the capacity of authorities in project countries and areas to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet and to secure electronic evidence.
Result/ Immediate outcome 1	Legislation strengthened regarding securing electronic evidence and access to data in line with data protection and rule of law requirements.
Activities:	– Advice and workshops to support authorities in drafting, revising or updating the relevant legal framework in line with applicable and emerging standards; – Support to participation of national project team members in relevant regional and international events on legal standards and international cooperation on cybercrime and electronic evidence, including those organised by the Council of Europe (plenaries of the T-CY).
Result/ Immediate Outcome 2	Coordinated cybercrime and cybersecurity policies and strategies developed and under implementation by the competent authorities.
Activities:	– Support countries in developing coordinated policies and strategies in cybercrime and/or cybersecurity areas; – Business analyses and development of agreed procedures for cybercrime/incident reporting and sharing of data by CERTs/CSIRTs with criminal justice authorities through beneficiary-specific workshops with regional conclusions. – Workshops and training sessions to follow up on assessment/business analyses to promote data sharing and integration of data from various sources by criminal justice authorities; – Simulation exercise on effective sharing of data between cybersecurity and cybercrime communities; – Support countries in the preparation of beneficiary reports on cybercrime and cybersecurity trends as well as for criminal justice statistics.
Result/ Immediate outcome 3	Specialised online public reporting systems on online fraud and other cybercrime offences fully operational in at least two project countries/areas.
Activities:	– Support the development and set-up of the online reporting platforms of cybercrime in North Macedonia[8] and Kosovo[9]; – Support raising awareness of the public on existent reporting mechanisms of cybercrime, on cybercrime threats and cyber resilience; – Design and delivery of revised first responder training course in all project countries/areas.[10]

[8] There is an effort underway on behalf of the Cybercrime and Digital Forensics Sector to create an online reporting system where reports of cybercrime are captured through a webpage. The system will use a dynamic web form and will allow citizens to report various types of cybercrime. The aim is to differentiate complaints along lines of the categories. Relevant reports will be shared with the CERT – if there is an online report about a possible government attack - and with banks – if the reported information is related to bank security or to a particular bank account, for example. This project, after the IC3 Internet Criminal Complaints Center of the US, has not yet been finalised. Although the interface for the reporting system is operational, the programming logic behind it needs more work and the current budget of the Ministry of Interior does not allow for its completion.

[9] Kosovo has established an online platform for reporting cybercrime, however further development of certain features is required (preventive function, processing of received reports, collation of statistics, etc.). It is not fully operational.

[10] Public reporting is still significantly dependent on administrative (written) reports filed with the police in

Result/ Immediate outcome 4	Capacities of specialised investigative units and inter-agency cooperation between cybercrime, financial investigators, prosecutors, representatives of FIUs and cybersecurity experts in the search, seizure and confiscation of online crime proceeds, combating cybercrime and securing electronic evidence further strengthened.
Activities:	– Specialised workshops and trainings on cybercrime and parallel financial investigations in cooperation with the European Cybercrime Training and Education Group (ECTEG);[11] – Support the creation of national guidelines and best practices for investigation and collection/handling of electronic evidence based on international standards; – Simulation exercises on effective information sharing and inter-agency cooperation for the search, seizure and confiscation of online crime proceeds; – National cyber exercises involving cybercrime/cybersecurity institutions; – Case simulation exercises and mock trials on cybercrime investigations (specific topics, such as virtual currencies/Darknet, etc.) and digital forensics for relevant agencies/entities; – Training programme on effective access to data: training section on open-source incident and crime reporting systems that can be set up between industry, CERT/CSIRT and law enforcement (including incident handling on the basis of the EU NIS Directive); training on open-source image creation and copying toolkits that would ensure less intrusion into the regular business process; training on basic parameters and use of hardware/software for retention and access to traffic data, including ideas for shared management for distributed storage systems and public configuration protocols; – Support participation in cooperation forums and meetings for networking between cybercrime and cybersecurity professional communities; – Support participation in long-distance specialised master programme.
Result/ Immediate outcome 5	Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced with a focus on cooperation between service providers and criminal justice authorities.
Activities:	– Regional and domestic meetings to support existing public/private initiatives at domestic and regional levels; – Support to organisation of regional and international Internet industry and technology events with focus on increasing trust between the public, the state and the private sector in ensuring security of cyberspace; – Regional and international case simulation exercises developing skills for cooperation on cybercrime and electronic evidence for judicial and police cooperation authorities with multinational service providers (MSPs), using and testing their platforms for cooperation; – Update and maintain the online resource on law enforcement/Internet service provider cooperation.
Result/ Immediate outcome 6	Judicial training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures with a focus on data protection and rule of law safeguards is provided.

person, in writing or on the phone. Regional units may not have the personnel that understand the requirements for cybercrime investigations, nor the types of cases and evidence sources involved. First responder training is crucial in the area of cybercrime and fraud. Especially vulnerable groups (including special needs persons, disabled, elderly or children) cannot be expected to use web reporting for financial crime, and yet they are often targeted by criminals.

[11] A formal cooperation agreement was signed between the Cybercrime Programme Office of the Council of Europe and ECTEG in September 2017.

Activities:	– Review and update the current state of national judicial training and agree on project approach; – Regional training of trainers on the delivery of the training course on cybercrime and electronic evidence for judges and prosecutors based on the Electronic Evidence Guide of the Council of Europe and Council of Europe training materials; – National delivery of the training course on cybercrime and electronic evidence for judges and prosecutors in Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia and Kosovo in co-operation with judicial training institution; – Specific judicial training programme for Turkey: trainings/joint workshops on obtaining and use of electronic evidence in criminal proceedings (in-country trainings on electronic evidence for judges and prosecutors; joint workshops on electronic evidence for judges, prosecutors, police and digital forensics specialists); – Support the set-up and participation in the international network for national judicial trainers on cybercrime and electronic evidence; – Update, translation and dissemination of the Electronic Evidence Guide of the Council of Europe in each project area.
Result/Immediate outcome 7	International cooperation and information sharing between cybercrime units, financial investigation units and financial intelligence units (FIUs) as well as between competent authorities for judicial cooperation is more efficient.
Activities:	– Trainings and table top exercises to enhance mutual legal assistance and other forms of international cooperation on cybercrime, electronic evidence and search, seizure and confiscation of online crime proceeds for cybercrime units, financial investigation units, FIUs and other national authorities;[12] – Integration of templates for international cooperation at the national level (24/7 points of contact and MLA authorities); – Development of standard step-by-step guidelines for drafting and processing of mutual legal assistance requests for criminal cases involving cybercrime and electronic evidence; – National, regional and international workshops, trainings and hands-on simulations for improvement of the skills, set-up and competencies of 24/7 points of contact; – Support project countries in building partnerships with their counterparts in the region, with other countries and international organisations (participation in meetings, conferences and international events).

CONTACT

Cybercrime Programme Office of the Council of Europe
Alexander.seger@coe.int

www.coe.int/cybercrime

[12] Interventions will be based on the relevant recommendations of the Cybercrime Convention Committee (T-CY) Assessment of the functioning of the international cooperation provisions, December 2014 and Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers, November 2017.