



iPROCEEDS

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

Version 30 January 2017

General guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online

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

Contents

General guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online	4
Introduction.....	4
Relevant institutions	4
Principles	5
Interagency Cooperation	5
Cooperation during Criminal Investigations.....	5
General Forms of Cooperation.....	6
International Cooperation.....	6
Appendix: Explanatory Report	8
1. Introduction	9
1.1 Purpose and Background	9
1.3 Information/request exchange	9
1.4 Criminal investigation	10
1.5 Scope/Applicability	10
2. Measures.....	12
2.1 Domestic Measures.....	12
2.2 International Measures.....	12
3. Cooperation during Criminal Investigations	14
3.1 Pre-investigation	14
3.2 Commencement of investigation.....	14
3.3 Cooperation with respect to exchange of information	14
4. Exchange of Intelligence, Information and Evidence	15
5. Multi-Agency Groups	16
5.1 Establishment of a Multi-Agency Group	16
5.2 Multi-Agency Group Personnel.....	16
5.3 Strategic Decision-making	17
5.4 Collaboration of Technologies.....	17
5.5 Review and Reporting	17
5.6 Research	18
5.7 Joint Training	18
5.8 Informal Cooperation	18
5.9 Contact Points for Multi-Agency Groups.....	18
5.10 Publicity	19
5.11 Termination of Multi-Agency Groups	19
5.12 Expenses.....	19
6. Public-Private Sector Cooperation.....	20

7. International Cooperation	21
7.1 Joint Investigation Teams	21
7.2 International Standards.....	22
7.3 Evaluation of Application of International Instruments.....	26
8. Statistics	29
8.1 Gathering of statistics	29
8.2 Review of statistics	29
9. Recommendations for Drafting Protocols	30
9.1 General guidelines	30
9.2 Amendments and supplements to the Protocols.....	31

General guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online

Introduction

1. Domestic and international investigations involving cybercrime, electronic evidence, proceeds from crime online and money laundering cut across different institutions, and require the involvement, in particular, of cybercrime units, financial investigation units, Financial Intelligence Units and prosecution services. Effective interagency and international cooperation to identify and prosecute perpetrators, identify and trace proceeds of crime online with a view of confiscation and to prevent and prosecute money laundering are essential.
2. The purpose of the present document is to help institutions improve interagency and international cooperation, and – if appropriate – formalise such cooperation through protocols between them.
3. The basis for cooperation shall be the existing relevant legal framework, taking into account also existing Memoranda of Understanding between relevant institutions.
4. While recognising the importance of cooperation with each other, within their respective legal responsibilities, and the importance of timely information and data sharing in concrete criminal investigations, particularly in cases involving cybercrime, tracing online crime proceeds and online money laundering, the institutions shall identify and explore possible cooperation protocols to achieve coordinated, timely and effective cooperation.
5. The aims of a domestic protocol are to:
 - Bring together all relevant institutions to cooperate more effectively.
 - Eliminate practical obstacles encountered during investigations into online crime proceeds.
 - More effectively identify perpetrators of criminal acts, prosecute and bring criminals to justice and to lead to the seizure and confiscation of online crime proceeds.
 - Specify the possible avenues for international cooperation, related to the search, seizure and confiscation of online crime proceeds and to identify opportunities and obstacles.
6. The existence of domestic protocols tends also to engender trust and greater cooperation with international partners.

Relevant institutions

7. The institutions to which a protocol applies may include, for example:
 - The State Prosecutor's Office
 - The Ministry of Interior - Cybercrime Unit
 - The Ministry of Interior – Integrated Financial Investigations Unit
 - The Financial Intelligence Unit (FIU-K).

8. These institutions cooperate with each other on the basis of legally defined roles, responsibilities and powers. These institutions may invite observers from other public institutions to join their regular or operational meetings if the expertise or know-how is deemed relevant to cooperation.

Principles

9. Institutions agree to the following principles:
 - There is a need for **effective** interagency cooperation and **efficient** sharing of information is a key pillar of this cooperation.
 - Each institution obtains and/or controls information that may be useful to an investigation involving online crime proceeds.
 - The institutions will access data and share information in accordance with existing **legal provisions**, including **data protection requirements**.
 - Investigations involving online crime proceeds may require **timely** responses to requests from other organisations and all relevant institutions are prepared to make undertakings in this respect.
 - Investigations involving the joint action of multiple agencies will require **coordination**.
 - The processes for cooperation should be as efficient as possible in order that they are used in the greatest number of appropriate cases and, in particular, that the existence of these processes does not hinder existing interagency cooperation.
 - There is a need for a **joint training programme** on cybercrime, electronic evidence, financial investigations and online crime proceeds.
 - There is a need for **regular yearly meetings** between the institutions to discuss, identify and advocate for ways to improve cooperation.

Interagency Cooperation

Cooperation during Criminal Investigations

10. The institutions recognise the importance of cooperation and information sharing in concrete criminal investigation involving online crime proceeds (with elements of cybercrime, tracing online crime proceeds and money laundering).
11. The institutions will access data and share information in accordance with existing legal provisions and in line with data protection requirements.
12. Institutions will respond to urgent requests for information upon receipt of a request from another institution relating to a cybercrime investigation or online crime proceeds investigation. Urgent requests should be marked as such by the requesting institution and include the motivation for the indication of the urgency.
13. The Prosecution service (responsible prosecutor) will consider the need to involve relevant units/institutions when targeting online proceeds of crime.
14. During an investigation, the Prosecution service (responsible prosecutor) will consider the appropriate form of cooperation on a case-by-case basis, and this can include, for example, creation of a task force, regular meetings or other forms of cooperation.
15. Investigations involving joint action of multiple institutions might require operational coordination under the lead of the prosecutor, including coordination of the activities of multiple agencies. A

lead investigation unit will be responsible for the coordination of operational activity, with all actions conducted under the instruction of the prosecutor and with regular reports being provided to the prosecutor.

16. An electronic platform for exchange of information between Police and Prosecutor service should be considered.

General Forms of Cooperation

17. A training programme/workshop will be held at least once per year, where representatives from each of the institutions shall exchange best practices and experiences related to investigations of online crime proceeds and discuss open questions and opportunities to improve cooperation. Where appropriate, the involvement of public sector observers or relevant private sector entities could be considered.

Presentations may include describing:

- a. The role and the powers of their institution when it comes to investigations involving online crime proceeds.
 - b. The nature of information available to that institution.
 - c. The process for engaging with that institution in matters requiring cooperation.
18. The training will be hosted each year by one of the institutions, in rotation.
 19. Each institution will consider the incorporation of interagency cooperation on targeting online proceeds of crime training into their annual training programmes.
 20. Regular yearly meetings of heads of relevant institutions or units will be held with the purpose to improve cooperation. The heads of relevant institutions may, by unanimous decision, determine further guidelines that govern aspects of their institutions cooperation.

International Cooperation

21. The increased cooperation of relevant institutions at national level reflects also the need for coordinated international cooperation by information exchange and mutual legal assistance. The relevant institutions shall identify and explore possible cooperation protocols to achieve coordinated, timely and effective international cooperation.
22. Institutions are aware of different options for international cooperation on the basis of national legislation (Law on International Cooperation in Criminal Matters), including on the basis of reciprocity, international legal instruments in the area of laundering, search, seizure and confiscation of proceeds of crime, cybercrime and money laundering (Council of Europe Strasbourg, Warsaw and Budapest conventions, European Convention on Mutual Assistance in Criminal Matters and additional protocols) and bilateral agreements.
23. The primary mechanism for police-to-police cooperation is the International Law Enforcement Coordination Unit (ILECU).
24. Prosecutor-to-prosecutor cooperation is carried out through direct coordination and through the use of mutual legal assistance treaties.

25. Court-to-court cooperation is carried out via direct requests sent to, and if agreed, signed by the Ministry of Justice.
26. FIU-to-FIU cooperation is carried out through the use of bilateral Memoranda of Understanding.
27. Central authority for mutual legal assistance is the Ministry of Justice.
28. The institutions recognise the opportunities of different options for international cooperation within their legal responsibilities in concrete criminal investigation involving online crime proceeds: with elements of cybercrime, tracing of proceeds of crime and money laundering.
29. The institutions will continue to provide information to the others on the nature and type of information that can be requested internationally, within their responsibility, as well as the process and timeframes involved.
30. The institutions will continue to consider and explore different possibilities for the use of the channels for international cooperation in a concrete case in accordance with the existing legal provisions.
31. The institutions understand that 24/7 Contact Point for international cooperation in the field of cybercrime is in the process of being established as envisaged by the Cyber Security Strategy and Action Plan for 2016-2019 and as provided the provisions of the Budapest Convention. The institutions further understand that requests for expedited preservation of electronic evidence can be expected through this single point of contact.
32. The institutions shall consider the benefits of using joint investigations and joint investigation teams in cross-border cases. When task force or joint team is created, the leading prosecutor or the leading unit should define tasks in order to avoid duplication of information requests through different networks.
33. The institutions shall consult good practices and guidance issued by relevant international institutions, such as the Council of Europe's Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC), the Cybercrime Convention Committee (T-CY), the Conference of Parties to Warsaw Convention, and others.
34. The institutions shall inform each other, at least on a yearly basis, on statistics on international cooperation related to online proceeds of crime as well as on best practice and other experience.

Appendix: Explanatory Report

Explanatory Report On the General guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online

1. Introduction

1.1 Purpose and Background

The purpose of this document is to provide a source of reference to agencies involved in the investigation and prosecution of cybercrime and the search, seizure and confiscation of online crime proceeds and to supplement the information in the General Guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online.

The document contains various aspects and options for interagency and international cooperation, as well as some considerations related to domestic protocols.

It is designed to assist prosecutors, investigators and other relevant entities to form a strategic framework on which to base an effective and collaborative exchange of information and investigation team when working in partnership with other public agencies and/or parts of the private sector to search, seize and confiscate online crime proceeds.

The common interest is to bring the criminals to justice and to deprive them of the criminal profit.

1.2 Explanatory note

Interagency cooperation depends on the legal framework defining the roles and responsibilities of the relevant institutions, including for the cases that bring together aspects of cyber investigation, financial investigation and prevention and investigation of online money laundering.

The intensity of cooperation among the relevant institutions might vary from simple (spontaneous) exchange of information or sending the requests for answers to another institution to the level of creation of more structured investigation teams on operational level (led by leading (police) unit) or on formalised level led by the prosecutor.

The interagency and international protocol documents should be reviewed and updated at regular times such as at annual meetings held between all of the relevant institutions mentioned within this document.

1.3 Information/request exchange

It is the understanding of the value of engagement between different institutions that drives the decision to cooperate. Thus consideration should be given as to whether communication between the institutions (Criminal Police, FIU and prosecution service) is centralised (by defined contact points and communication channels – for example in a memorandum of understanding) or if the mode of communication should be left for decision by heads of units in the relevant institutions on a case-by-case basis. There might be benefits of centralised exchange of information/requests, but with operational flexibility.

Such exchange of information/requests might occur even prior to formal start of criminal investigation, so the prosecutor might not be engaged in leading (yet). Should the prosecutor be informed on such communication depends on (legal and practical) arrangements.

1.4 Criminal investigation

According to the Criminal Procedure Code the prosecutor leads the investigation. He has the power to ask the police and other institutions to perform tasks necessary to investigate and collect evidence. The prosecutor has the legal competence to commence and direct criminal investigations with operational support from the police over whom the prosecutor has a directive and supervisory role.

The prosecutor has the power to establish investigation teams, constructed by representatives of relevant institutions for the purpose of a concrete case investigation.

The conditions to create such team depend on legislation and the decision of the prosecutor (and consent of heads of relevant institutions). It would be advisable to determine the working methods, intensity of the meetings or even (temporarily) joint office. A work plan is particularly important to avoid duplication of tasks, and especially to avoid multiple international requests through different channels of cooperation/information sharing.

In complex cases also the operational lead should be considered (especially when several police units are involved).

It might be useful to define general guidelines (by the Prosecutor General) for creation of an investigation team. This could include concrete conditions when such teams would be considered and the possibility for police to propose its creation to the prosecutor. Available personnel and financial resources might affect such forms.

1.5 Scope/Applicability

Relevant institutions include:

- State Prosecutor's Office
- Ministry of Interior - Cybercrime Unit
- Ministry of Interior - Integrated Financial Investigations Unit
- Ministry of Finance - Financial Intelligence Unit (FIU-K)
- Ministry of Justice - central authority for international cooperation.

The mandate of each institution:

- **State Prosecutor's Office** holds a variety of roles when dealing with cybercrime and similar crimes generating proceeds. The prosecutors take the lead in all criminal investigations and direct the relevant law enforcement agency on what tasks they need to complete. Investigations into money laundering and organised crime are conducted by the Special Prosecution. Prosecutor is also empowered to have its own investigation team that it can directly task and control. This is providing a heightened level of cooperation with Law Enforcement Officers.
- **Ministry of Interior - Cybercrime Unit** leads the investigations into cybercrime offences according to the Law on Prevention and Combating Cybercrime, which was drafted as to comply with the Budapest Convention on Cybercrime. Currently, the officers in the Cybercrime Unit concentrate their investigative activities on four main areas related to unlawful access to computers and networks (hacking), credit card offences, indecent images of children and the

provision of forensic and other expertise in supporting the Police and Prosecution in matters where technology is a significant factor to a crime or related evidence.

- **Ministry of Interior – Integrated Financial Investigations Unit** primarily concentrates its activities on preventing and combating of economic crimes, financial and corruption investigations. The unit is seeing a significant increase in the use of technology and the reliance upon electronic evidence in its investigations. The unit has a number of existing partnerships, which support its day-to-day activities. These partners include other Government departments, such as Customs, Financial Intelligence Unit, Public Revenue, Agency for Employment as well as the private sector businesses such as financial institutions and banks.
- **Ministry of Finance – Financial Intelligence Unit (FIU-K)** derives its powers from the Law on the Prevention of Money Laundering and Combating Terrorist Financing. The FIU-K is a central independent national institution operating within the Ministry of Finance and is responsible for requesting, receiving, analysing and disseminating to the competent authorities disclosures of information which concern possible money laundering and terrorist financing. The FIU-K is empowered to suspend suspicious transactions for up to 48 hours to allow the completion of investigations or to apply for restraint or similar by the provision of another legal instrument, normally in collaboration with a prosecutor.
- **Ministry of Justice** is the designated central authority for mutual legal assistance in criminal matters.

2. Measures

2.1 Domestic Measures

Every country has legislation under which it prosecutes offenders and through which authorities are authorised to investigate crime (and criminals).

Practice might show the need for more detailed arrangements for cooperation between the institutions in applying some particular measures (for example special investigative means, freezing order, expedited preservation etc.). A special provision of protocol/Memorandum of Understanding could be considered.

The following domestic matters will require legislation and due process. Consequently they should be considered in investigations involving cybercrime and related investigation into the proceeds of such crimes. As such, the following matters should be conducted in a manner provided for under domestic legislation:

- Issuance of warrants
- Arrests
- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production orders
- Search and seizure
- Real-time collection of traffic data
- Interception of content data
- Require reporting of suspicious transactions
- Require identification/disclosure of transaction trails
- Require maintaining or disclosure of transaction information
- Prohibition of disclosure of any ongoing money laundering enquiry or investigation
- Temporarily suspend or withhold transactions that have been reported as suspicious transactions
- Attachment/confiscation of bank accounts and other assets (virtual currency etc.)
- Measures for temporary freezing the property, measures to confiscate proceeds of crime
- Investigative tools (access to bank account data, use of SIMS).

2.2 International Measures

When cooperating with international partners, there is a general expectation that nations will have sufficient measures in place to support the agreements made under the Budapest and Warsaw conventions.

The most relevant international measures are highlighted in this section in order to provide reference in the making and receiving of international requests:

- Expedited preservation of stored computer data (Article 29 Budapest Convention)
- Expedited disclosure of preserved traffic data (Article 30 Budapest Convention)
- Mutual assistance regarding accessing of stored computer data (Article 31 Budapest Convention)
- Mutual assistance regarding real-time collection of traffic data (Article 33 Budapest Convention)
- Mutual assistance regarding interception of content data (Article 34 Budapest Convention)
- Request for information on bank accounts (Article 17 Warsaw Convention)

- Requests for information on banking transactions (Article 18 Warsaw Convention)
- Requests for monitoring of banking transactions (Article 19 Warsaw Convention)
- Confiscation of instrumentalities/proceeds/property of corresponding value (Article 23 - 26 Warsaw Convention):
 - Execution of requests for confiscation
 - Dealing with confiscated assets
 - Conditions on confiscation orders

The requests referred to above are transmitted in the manner provided for in the conventions, Article 25 Budapest Convention, where there is an existing legal basis for cooperation or Article 27 (if accepted by the state party), where there is not such a basis, and Articles 33 and 34 of the Warsaw Convention, subject to confidentiality and limitation provisions where applicable and in the absence of existing relevant agreement (Article 28 Budapest Convention and Article 43 Warsaw Convention).

Additional provisions relevant to international cooperation include:

- Provision of spontaneous information (Article 26 Budapest Convention, Article 20 Warsaw Convention),
- Trans-border access to stored computer data subject to consent/where data is publicly available (Article 32 Budapest Convention). This is an extra-territorial measure available to investigators engaged in investigating the offence in their territorial jurisdiction of competence applicable in certain defined, limited circumstances,
- The establishment of a 24/7 Network POC (Article 35 Budapest Convention),
- Exchange of information between FIUs spontaneously or on request (Article 26 Warsaw Convention),
- Cooperation between FIUs related to postponement of suspicious transactions (Article 47 Warsaw Convention).

3. Cooperation during Criminal Investigations

The establishment of a Multi-Agency Group, a Joint Investigation Team in cross-border cases or sharing of resources requires planning, sharing of information, agreement and collaboration. Below are some of the considerations that Prosecutors, Senior Police Officers and Agency managers will need to consider in support of agency cooperation during criminal investigations.

3.1 Pre-investigation

- Notice at pre-investigation stage.
 - Where cooperation is required by two or more agencies, early indications of the type of support, length of time and the resources required should be discussed as soon as possible.
 - Anticipation and early notice of the likelihood of investigations requiring agencies to cooperate will allow managers and alike to plan their response in a planned and methodical way.
 - Means by which pre-investigation notices and requests are to be confidential should be clearly identified.
 - Prosecutors and senior investigators can review the requirements of the establishment of a Multi-Agency Group or Joint Investigation Team and put necessary plans in place. Further details are outlined in this document below.

3.2 Commencement of investigation

- How is notice to be given?
- At what stage is notice to be given?
- What should notice include?
 - Name of parties
 - Court, if any, where proceedings have been or are to be initiated
 - Nature of the action/proceedings
 - Alleged facts that serve as basis for the action/proceedings
 - Anticipated date of initiation of actions/proceedings
- Is there a requirement for parties to keep notices regarding commencement of investigations confidential if required?
- Cooperation with respect to certain measures (see Measures below).

3.3 Cooperation with respect to exchange of information

See Exchange of Intelligence, Information and Evidence below.

4. Exchange of Intelligence, Information and Evidence

Law enforcement, intelligence organisations and governments recognise the need to collaborate, share and exchange information. The effective exchange of intelligence, information and evidence requires process, trust and security.

By considering the following requirements, Prosecutors and Law Enforcement agencies will provide a system that balances legal requirements and considerations of privacy as well as identify exactly how information, intelligence and evidence may be used in respective processes.

- Preconditions for exchange of intelligence, information and evidence
- Procedure for requesting intelligence, information and evidence:
 - How will requests for information be made, received and processed by each party?
 - Which persons within each agency will requests be sent to?
- Confidentiality of requests
- Limitations to confidentiality of requests
- Penalties for breach of confidentiality of requests
- Spontaneous information
- Upper time limit to process requests:
 - Exceptions
 - Urgent requests
 - No exception for holidays/weekends/office hours
- Data protection
- Confidentiality of information – level of classification
 - Requirement that no notice be given to parties (e.g. no notice to be given to bank account holder regarding freezing of bank accounts)
 - Security measures to be implemented
 - Physically securing premises
 - Securing IT systems
 - Penalties for disclosure of information exchanged
 - Exceptions to confidentiality:
 - Where disclosure is required by law
 - Where there is consent to disclose
 - Adequate instructions given to contact points/other staff involved about confidentiality requirement
- Conditional exchanges of evidence
- Integrity of information, intelligence and evidence exchanged:
 - Ownership
 - Processes to maintain integrity/chain of custody
 - Making officials available to testify to authenticity of data in courts
- Means through which electronic data will be shared (cloud/physical discs etc.).

5. Multi-Agency Groups

The creation of a Multi-Agency Group for a criminal investigation may be required for a number of reasons, which include sharing of resources, the size of the operation, the legal requirement for different agency involvements, expediency and many other needs.

There are a number of issues to consider during the establishment of a Multi-Agency Group, which includes leadership, resources, responsibility and legal framework. This set of guidelines lays down some considerations that should be undertaken in the creation of such a Multi-Agency Group and should be reviewed throughout the investigation. National legislation and directives will take priority over the recommendations detailed below.

5.1 Establishment of a Multi-Agency Group

During the establishment of a Multi-Agency Group, the following should be considered and recorded for later review:

- Permanent or temporary Multi-Agency Group:
 - If temporary, term of Multi-Agency Group
- Any process undertaken for identifying and mapping agencies involved
- Development of structure:
 - Leadership and governance for the Multi-Agency Group
 - Planning resources and ensuring hub management
 - Provisions for changes in leadership or structure
- Levels of Multi-Agency Groups:
 - Existing forms of practice and coordination
 - Virtual links between agencies:
 - Co-located hub of agencies/ride-along.

5.2 Multi-Agency Group Personnel

Once a decision has been made to create a Multi-Agency Group, the resourcing should be considered and agreed by relevant managers from the agencies involved in the creation of such a group. The resourcing should continually be monitored by the hub management. The following provides a guideline to those considerations:

- Assignment of personnel by agencies:
 - Number of personnel
 - Duties of personnel
 - Duration of assignment
 - Schedule of personnel
- Specific personnel to be assigned:
 - Interagency collaborator positions (designation of individual in an agency to collaborate with/between agencies and departments)
 - Liaison positions (person employed by one agency designated to work with another agency)

- Personnel details (specialist or professional employed by to perform tasks for another agency).

5.3 Strategic Decision-making

The effective delivery of an efficient Multi-Agency Group will rely upon clear leadership, transparent decision-making and good strategic planning. By setting out a strategic decision-making process at the inception of such a group, the collaborative processes should be much more effective. The following provides some considerations:

- Leading agencies
- Particular roles
- Choosing jurisdictions
- Choosing forums
- Coordinated interventions:
 - With respect to already-existing information/intelligence/information
 - With respect to conducting arrests, searches and seizures
 - With respect to freezing of assets.

5.4 Collaboration of Technologies

- Agree on establishment of real-time information database
- Requirement for agencies to maintain and update interconnected databases in real-time to allow:
 - Real-time information sharing between agencies
 - Real-time decision making between agencies
 - Real-time communication between agencies
 - Data protection measures
 - Security/encryption standards
- Access to information database to use at pre-investigation and investigation stages.

5.5 Review and Reporting

Measurement of achievement and development of procedures is a continual requirement in the development of any investigative process. This enables best practice to be identified, blockages to be removed and risks to be mitigated. Some considerations that can best achieve this objective are recorded below:

Retention of records:

- Period of retention required
- Mode of retention
- Kind of data to be retained by agencies

Accountability:

- Measure of achievement of short-term/long-term outcomes
- Means by which progress is to be tracked

Meetings/Reports:

- Development of timetable schedule for meetings
- Annual meetings & extraordinary meetings
- Notice for meetings
- Agendas for meetings
- Results of meetings.

Required reviews:

- Review of on-going law enforcement activities
- Review of effectiveness of coordination
- Future law enforcement activities
- Review of statistics to identify problems in cooperation etc.
- Risk analysis
- Review of work action plans/work programs of each agency.

5.6 Research

- Exchange information on upcoming research activities of mutual concern
- Invite each other to relevant expert meetings and collaborate in research activities
- Exchange information on issues with respect to law enforcement.

5.7 Joint Training

Training is a method of sharing best practice and breaking down some of the misunderstandings across different organisations. It is a vital part of pre-planning for Multi-Agency Groups. The following list is a baseline standard of what training activities should consider in their delivery:

- Sharing of existing training materials
- Design and evaluation of training activities/workshops/tools/methodologies for different agencies
- Development of joint training materials
- Procedures for holding joint training
- Inviting each other to training activities/workshops
- Frequency of training
- Funding for joint trainings
- Responsibility for joint trainings.

5.8 Informal Cooperation

- Authorisation of informal/innovative means of cooperation
- Explore all legal avenues/possibilities for cooperation
- Continuing to respect personal data rules, privacy and other rules
- Consideration of what value a court may view informal cooperation and therefore exclude evidence.

5.9 Contact Points for Multi-Agency Groups

- Designation of contact point in each agency

- Means by which contact point can be contacted
 - Urgent matters
 - Non-urgent matters
- Contact points permanently staffed by individuals with appropriate security clearance to an agreed upon standard
- Staff of designated point of contacts to have full authority to respond to cases (no further authorisations required).

5.10 Publicity

- Restrictions on making statements to press regarding activities of Multi-Agency Groups without consent of all parties.

5.11 Termination of Multi-Agency Groups

- Can an agency unilaterally terminate the Multi-Agency Groups?
- Under what circumstances can a Multi-Agency Groups be terminated?
- What is the effect of termination on obligation of parties?
- What is the effect of termination on cooperation/information exchanged previously?
- How is notice of termination to be given?

5.12 Expenses

- Who will bear expenses that arise in course of implementation of Multi-Agency Groups?

6. Public-Private Sector Cooperation

The investigation of cybercrime and/or targeting online proceeds of crime and money laundering requires robust and efficient public-private sector cooperation. Such cooperation will be based upon domestic and international measures (specified elsewhere in this document), which need to be enacted within each nation.

The effective delivery of these laws and treaties relies upon relevant protocols and standard operating procedures being agreed and implemented between public and private sectors.

Requirements to support public-private sector cooperation should consider the following points:

- Developing system whereby appropriate agency will obtain data from private sector persons that it has legal mandate to regulate/seek cooperation/information from:
 - Allocation of roles based on efficiency and legal mandates
 - Make it dependent on an issue-wise basis or case-to-case basis
- Mechanisms by which cooperation with private sector will take place
- Establishment of permanent Multi-Agency Groups with different private sector bodies (e.g. CERTs, ccTLDs, ISPs etc.).

The success of public-private sector cooperation is often based upon succinct and relevant Memoranda of Understanding. It is important that these documents are reviewed regularly and updated as necessary.

Public-private cooperation protocols are a separate issue.¹

¹ See Council of Europe Guidelines for cooperation between law enforcement and internet service providers against cybercrime, 2008:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba>

Also available in Albanian:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fe152>

7. International Cooperation

Kosovo* is not a Party to the Council of Europe conventions such as the European Convention on Mutual Assistance in Criminal Matters and its Protocols, the Budapest Convention on Cybercrime (ETS No.185), the Strasbourg Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No.141), and the Warsaw Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism Convention (CETS No.198). However, its relevant legislation was drafted in line with international standards. International cooperation is realised on the basis of relevant bilateral or regional cooperation frameworks.

Although responsibilities for mutual legal assistance may be divided between the judges, prosecutors (the drafting and executing of requests) and central authorities (for *inter alia* the translation, transmission, receipt and execution of requests), it is also important to be aware of other cooperation channels (and their limitations) at police level. In all cases but especially in complex cases, the most efficient information gathering method should be identified by those involved at the outset with a view to avoiding simultaneous use of more than one channel for the same purposes as this can lead to the duplication of requests.

Cyber Security Strategy and Action Plan for 2016-2019 envisage the establishment of a permanent 24/7 Contact Point for international cooperation in the field of cybercrime.

7.1 Joint Investigation Teams

If approached to form part of a JIT by European Union (EU) Member State useful information on EU practice on JITs is available at the Europol² and EUROJUST³ websites.

In the EU, a JIT is set up for a fixed period and for a specific purpose, based on an agreement between two or more competent authorities in the member states. Competent authorities from countries outside the EU may participate in a JIT dependent upon the agreement of all other participating parties and the existence of appropriate underlying international legal base.

Generally, each JIT is set up to investigate a specific case. Once the investigation has concluded, the JIT comes to an end, thus there are no permanent or on-going JITs. The terms in accordance with which a JIT operates varies somewhat with each case, however, the terms are usually based on a model agreement appended to the Council Resolution of 26 February 2010 on a Model Agreement for setting up a Joint Investigation Team (JIT) (2010/C 70/01), which encourages the competent authorities in Member States "to agree upon the modalities for the joint investigation team."

As most EU Member States have signed and ratified both the Budapest and Warsaw conventions the expectation is that members of the JIT will be able to comply with the provisions of these treaties.

Law on International Cooperation in Criminal Matters refers in article 98 to JIT.

Establishment of a JIT

The following considerations should be undertaken during the creation of a JIT:

² <https://www.europol.europa.eu/activities-services/services-support/joint-investigation-teams>

³ <http://www.eurojust.europa.eu/doclibrary/JITs/joint-investigation-teams/Pages/jits-framework.aspx>

- Notice of establishment
- Structure/leadership
- Standard Operating Protocols
 - Standard Operating Procedures with financial institutions to ensure that where necessary, the flow of illegal money transfers can be delayed until necessary intelligence and/or further legal instruments can be utilised
 - Agreement that each of the relevant institutions will contact a nominated representative in the partner relevant institutions to expedite requests
- Conducting investigations
 - Maintaining chain of custody of exhibits.
 - Proper initiation of investigations
 - Current contact list of Police departments that are on call
 - Retention of up-to-date contact lists of financial institutions by relevant institutions
- Necessary funding (albeit some funding may be provided by Europol)
- Resources and staffing
 - Appropriate leadership
 - Appropriate resources including skill levels.
 - Appropriate allocation of roles and responsibilities
- Common agreement at which stage to terminate a JIT
- Cooperation following termination of JIT.

7.2 International Standards

Consider relevant provisions of Warsaw Convention (for financial investigation and FIU cooperation) and Budapest Convention (for cybercrime investigation), Recommendations of the Financial Action Task Force (FATF) (for investigation of money laundering, associated predicate offence and terrorist financing) and EU legal instruments as listed below.

EU legal instruments

EU legal instruments are applicable within the European Union. It may be useful to understand the standards, methods and practice of the most relevant instruments targeting proceeds of crime and cybercrime in areas of mutual legal assistance, when cooperating with an EU Member State.

- Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union;
- Framework Decision 2001/500/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime;
- Framework Decision 2005/212/JHA on confiscation of crime-related proceeds, instrumentalities and property;
- The principle of mutual recognition, as opposed to mutual assistance, has been introduced within the EU:
 - Framework Decision 2003/577/JHA for the execution of freezing orders
 - Framework Decision 2006/783/JHA for the confiscation orders
 - Council Decision 2007/845/JHA introduced the obligation to set up Asset Recovery Office(s) (ARO)

- Directive 2013/40/EU on attacks against information system (24/7)
- Directive 2014/41/EU on the European Investigation Order in criminal matters.

General Principles applicable to International Cooperation

- Warsaw Convention, Article 15
 - The Parties shall mutually co-operate with each other to the widest extent possible for the purposes of investigations and proceedings aiming at the confiscation of instrumentalities and proceeds.
 - The parties shall comply with requests for confiscation of specific items of property representing proceeds or instrumentalities, as well as for confiscation of proceeds in a requirement to pay a sum of money corresponding to the value of proceeds, and for investigative assistance and provisional measures with a view to either form of confiscation.
- Budapest Convention, Articles 23 and 25
 - The Parties shall mutually afford each other the widest possible mutual assistance for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
- FATF, Recommendation 37
 - Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings.

Communication and transmission of requests

Parties to both Warsaw and Budapest conventions are required to designate central authorities which communicate directly with one another (Warsaw Convention - Articles 33 and 34; Budapest Convention - Article 25 applies where there is an existing basis for cooperation, and Article 27 may apply if accepted by the party where there is no such existing arrangement or central authority designated). However,

- Warsaw Convention, Article 34 provides that urgent requests may be transmitted directly between the judicial authorities, including prosecutors, with a copy to be sent through central authorities or through INTERPOL.
- Warsaw Convention, Article 34/5 provides that non-coercive requests (i.e. where execution of a request does not require the use of a coercive measure) may be directly transmitted between competent authorities.
- Warsaw Convention, Article 34/6 provides for the possibility of direct exchange of draft requests in order to facilitate cooperation prior to a formal request being made.
- Budapest Convention, Articles 29-31 provide for requests to be dealt with in an expedited manner.
- Transmission via INTERPOL is available to all parties to the Council of Europe Convention on Mutual Assistance in Criminal Matters.
- Article 27/9 provides a similar provision (applicable if accepted by a party and if not covered by an existing arrangement).

Provisional Measures

- Warsaw Convention, Articles 21-22
 - Parties shall take provisional measures, such as freezing or seizing, to prevent any dealing in, transfer or disposal of property subject to confiscation and provide spontaneously all information relevant for the execution of such provisional measure.
- Budapest Convention, Articles 29-30 provide for the following measures:
 - Expedited preservation of stored computer data
 - Expedited disclosure of preserved traffic data.
- FATF, Recommendation 38⁴
 - Countries should have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering, predicate offences and terrorist financing, instrumentalities, or property of corresponding value.

Investigative Assistance

- Warsaw Convention, Articles 16-19
 - Parties shall assist each other in the identification and tracing of instrumentalities, proceeds and other property liable to confiscation, which includes securing evidence as to the existence, location or movement, nature, legal status or value of the aforementioned property.
 - Such assistance comprises also of requests for information on bank accounts, on banking transactions and monitoring of banking transactions)
- Budapest Convention, Articles 31-34 - Mutual assistance regarding investigative powers:
 - Accessing/seizing or similarly securing/disclosing of stored computer data,
 - Mutual assistance regarding the real-time collection of traffic data,
 - Mutual assistance regarding the interception of content data subject to Domestic law.
- FATF, Recommendation 37
 - Countries should ensure that all powers and investigative techniques available to their competent authorities, including those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of the witness statements, are also available for use in response to requests for MLA.

Confiscation

- Warsaw Convention, Articles 23-25
 - Parties are requested either to enforce a confiscation order or to submit the request to its competent authorities for the purpose of obtaining an order of confiscation and enforce it.

⁴ See also the Interpretative Note to FATF Recommendation 38.

- This includes a request to pay a sum of money corresponding to the value of proceeds, or confiscation of specific item of property (value confiscation is not yet available in Albania, however a pending Criminal Code amendment is due to bring this into effect).
 - Article 23/5 provides for the execution of a judicial request for measures equivalent to confiscation leading to the deprivation of property, which are not criminal sanctions (non-conviction based confiscation).
 - Article 25 determines the rules of asset sharing: property is primarily disposed of by executing Party, unless requested to give priority consideration to returning it to the requesting Party so that it can compensate the victims or return property to their legitimate owners.
- FATF Recommendation 38 (see above).

Cooperation between FIUs

- Warsaw Convention, Chapter V, Articles 46 and 47
- FIUs shall exchange, spontaneously or on request and either in accordance with this Convention or in accordance with existing or future memoranda of understanding compatible with this Convention, any accessible information that may be relevant to the processing or analysis of information, or, if appropriate, to investigation by the FIU information regarding financial transactions related to money laundering and the natural or legal persons involved.
 - Countries should adopt measures to permit urgent action to be initiated by a FIU, at the request of a foreign FIU, to suspend or withhold consent to a transaction going ahead (postponement of suspicious transactions).
- FATF Recommendation 40
- FIUs should exchange information with foreign FIUs regardless of their status. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.
 - FIUs should have the power to exchange: a) all information that they can obtain from reporting entities as well as financial, administrative and law enforcement information that they have access to; and b) any other information which they have the power to obtain or access at the domestic level, subject to the principle of reciprocity.

24/7 Network

- Budapest Convention, Article 35
- Each Party shall designate a point of contact available on 24/7 basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
 - Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
 - the provision of technical advice,
 - the preservation of data pursuant to Articles 29 and 30,
 - the collection of evidence, the provision of legal information,
 - the locating of suspects.

Other methods of cooperation

The establishment of JITs pursuant to Council of Europe and EU instruments is discussed above.

Multi-disciplinary groups specialised in financial and asset investigations:

- FATF Recommendation 30
 - Countries should make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial and asset investigations and ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

Spontaneous Information

- Warsaw Convention, Article 20 and Budapest Convention, Article 26
 - Parties may, within the limits of its domestic law and without prior request, forward to another party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

Exchange of Information between Non-counterparts

- FATF Recommendation 40 and related Interpretative Note
 - Countries should permit their competent authorities to exchange information indirectly with non-counterparts. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country.
 - Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

7.3 Evaluation of Application of International Instruments

a. Targeting crime proceeds

PC-OC

The Council of Europe's Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC) focused its attention on the area of targeting crime proceeds in 2014. The replies to the PC-OC questionnaire⁵ showed, among other, that there are differences in

⁵ Questionnaire on the use and efficiency of Council of Europe instruments as regards international co-operation in the field of seizure and confiscation of proceeds of crime, including the management of confiscated goods and asset sharing. PC-OC Mod (2015) 06Rev4,

application of the provisions of Strasbourg and Warsaw conventions, relevant to international cooperation.

MONEYVAL

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL is a monitoring body of the Council of Europe, assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as making recommendations to national authorities in respect of necessary improvements to their systems.

MONEYVAL mutual evaluations are assessing the countries' compliance with the FATF 40 Recommendations⁶ and follow the practices and procedures used by the FATF. FATF Recommendations are international standards on combating money laundering and financing of terrorism as well as the financing of proliferation of weapons of mass destruction.

In relation to domestic interagency cooperation the following FATF standards are of particular relevance: on national cooperation and coordination (Rec 2), on FIU (Rec 29), on responsibilities of law enforcement and investigative authorities (Rec 30) and on their powers (Rec 31), and on statistics (Rec 33).

Recommendations on international cooperation *inter alia* emphasize the need to ratify and implement international instruments, including Budapest and Warsaw conventions (Rec 36), lay down requirements for mutual legal assistance (Rec 37), freezing and confiscation (Rec 38), extradition (Rec 39) and to other forms of international cooperation (Rec 40).

b. Cybercrime

The Council of Europe Cybercrime Convention Committee (T-CY) is monitoring implementation of Budapest Convention and developing further standards and guidance notes. It is useful to consult some recent work of the T-CY, related also to the (efficiency of) mutual legal assistance:

- T-CY Emergency requests: Preliminary observations on replies⁷
- T-CY Assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime⁸
- Final report of the T-CY Cloud Evidence Group on Criminal (CEG) justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY⁹.

T-CY adopted in December 2014 a set of recommendations to make the mutual legal assistance (MLA) process regarding investigation of cybercrime and electronic evidence more efficient through more effective use of existing provisions of the Budapest Convention and other agreements but also by

19.5.2016. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>

⁶ http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

⁷ T-CY(2016)13, 25.7.2016, [Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers: Compilation of replies.](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c)

⁸ T-CY(2013)17rev, 3 December 2014, <http://www.coe.int/en/web/cybercrime/t-cy-reports>.

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

⁹ T-CY (2016)5, 16 September 2016.

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

proposing additional solutions¹⁰, such as: parties should fully implement the preservation powers of the Budapest Convention (Recommendation 1), monitor the effectiveness of the MLA process (Rec 2), allocate more and better trained staff and more resources for MLA (Rec 3 and 4), strengthen the role and capacities of 24/7 points of contact (Rec 5), establish procedures for emergency situations (Rec 8), etc.

Also, parties should consider – possibly through a Protocol to the Budapest Convention – allowing for the expedited disclosure of subscriber information (Rec 19), the possibility of international production orders (Rec 20), direct cooperation between judicial authorities (Rec 21), addressing the practice of directly obtaining information from foreign service providers (Rec 22), joint investigations and/or joint investigative teams between Parties (Rec 23), allowing for requests to be sent in English language (Rec 24).

CEG in its recommendations concluded that mutual legal assistance remains the main means to obtain electronic evidence from foreign jurisdictions for use in domestic criminal proceedings. This is particularly true for content data. It also highlighted that access to subscriber data is less intrusive and should be lightened. Article 18 of the Budapest Convention could be used for requesting subscriber information from multinational ISPs operating in the territory of a state – a draft Guidance note nr. 10 on Production orders for subscriber information has been prepared¹¹.

CEG proposed to consider drafting an additional protocol in order to address some existing challenges, which will include provisions for more effective mutual legal assistance (such as a simplified regime for mutual legal assistance requests for subscriber Information; international production orders; direct cooperation between judicial authorities in mutual legal assistance requests; joint investigations and joint investigation teams; requests in English language; audio/video hearing of witnesses, victims and experts; emergency MLA procedures); provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests; clearer framework and stronger safeguards for existing practices of transborder access to data; safeguards, including data protection requirements.

¹⁰ See page 125 to 127 of the report at

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

¹¹ Draft T-CY Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention), presented at T-CY meeting in November 2016.

8. Statistics

Official statistics should provide quantitative or qualitative information on all major areas of Government Agencies or other public bodies. This includes prosecution and law enforcement.

Statistics should supply decision-makers and other users with information that they can develop their knowledge about the subject, assess performance of the agencies and identify improvements to strategy and systems. This improves accountability of official agencies or other public bodies.

8.1 Gathering of statistics

- Minimum level of statistics required with respect to domestic and international cooperation - for example: data on number of financial investigations and related criminal offences, number and value of freezing orders, number and value of confiscation orders, number and value of executed confiscations; number of money laundering investigations/prosecutions/judgements; FIU statistics; international cooperation: number of incoming and outgoing requests segregated by articles of Warsaw and Budapest conventions and national provisions.
- Ensure that statistics are prepared in a method so that they can be compared between different units and that annual totals can be accurately reported.
- Designate body (unit) to gather statistics from different institutions (police (Ministry of Interior and Ministry of Finance), prosecution, courts/judiciary, Ministry of Justice) and their commitment to send such data. Take into account different reporting obligations (Council of Europe: e.g. MONEYVAL, GRECO, OECD) or
- Designate or constitute body to collect statistics:
 - Mandate of the body
 - Powers to call for information from relevant institutions
 - Funding
- Development of common classifications to harmonize work being done by different agencies.

8.2 Review of statistics

- Incidence monitoring based on statistics gathered
- Review of statistics by Multi-Agency Groups to evaluate and enhance effectiveness.

9. Recommendations for Drafting Protocols

9.1 General guidelines

Below are some general guidelines, which should be referred to when seeking to create, review and implement domestic protocols. These guidelines are not exhaustive and other national procedures and legislation should take priority over these generic recommendations:

- Ensure that the powers/mandates of different agencies are enunciated in the protocol
- Ensure that the objectives of the protocol are clearly defined within the protocol
- Ensure that the request form for cooperation/information exchange is simple and not confusing and time-consuming
- Ensure that agencies have specified a single point of contact with authority to cooperate with other agencies
- Ensure that agencies that have powers to conduct certain kinds of investigations/information-gathering can easily share such information with other agencies
- Ensure that the measures with respect to which there shall be interagency cooperation under the protocol are clearly defined, both with respect to domestic and international cooperation
- Ensure that there are specific provisions regarding the development, establishment and maintenance of integrated database of information
- Ensure that there are strong confidentiality, security and data protection safeguards built into the protocol
- Ensure that there are clearly defined standard operating procedures for Multi-Agency Groups.
- Ensure that Multi-Agency Groups under the protocol have a defined leadership structure
- Ensure that the protocol provides for joint training
- Ensure that there is a comprehensive accountability and monitoring mechanism, including regular meetings, statistics gathering etc.
- Ensure that private sector operators are encouraged to cooperate on an informal basis
- Resolution of disputes:
 - Ensure that there is a procedure to resolve disputes that are within and outside the scope of the protocol
 - Ensure relevant time periods are in place to assure the expedient resolution of such dispute
 - Ensure that there is a mechanism to prevent hindrance to ongoing and new investigations as a result of disputes between agencies
- Termination of protocol
 - Ensure that there is a method to revoke or terminate any protocol, if required
 - Place a notice period for the termination of such protocol
 - Ensure that the effect of termination of the protocol is clearly stated, including impact on JITs, MAGs, ongoing investigations and cooperation
- Term or period of the protocol
- Identify the date on which protocol becomes effective
- Specify the term of protocol
- Provide an option for renewal, where necessary.

9.2 Amendments and supplements to the Protocols

- Specify a procedure for making amendments
- Identify how amendments can be made to the agreed protocol including the level of consensus required.