**Lesson 2.2 Informal Methods of International Cooperation**

|  |  |  |
| --- | --- | --- |
| Lesson 2.2 Informal Methods of International Cooperation | | Duration: 60 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Internet access (if available) * PowerPoint or other presentation software | | |
| **Session Aim:**  Session is aimed towards a presentation and discussion about informal ways of the cooperation through use of established channels of communication on the police, prosecution, and court level. Number of examples of international organizations and their cooperation networks are at disposal and some of the most successful are presented here.  Expert should present possibilities of using these networks, procedures and contact points for fast communication and exchange of not only if information but evidence, if possible and admissible, as well.  Main point of the session should be that mechanisms at disposal should be used in most efficient way for reaction in suppression of the cyber crime. | | |
| **Objectives:**   * to understand differences between formal and informal mutual legal assistance in criminal matters * to get additional information and knowledge about International Organizations and Networks for Cybercrime organization, setup, and competencies * to additionally analyse and understand implementation of the Council of Europe Cybercrime Convention Article 35 * to raise awareness about some of the local national solutions for suppression of the cybercrime and mutual legal assistance with that regards | | |
| **Trainer Guidance**  During the session following topics should be considered:   * Formal versus informal mutual legal assistance in criminal matters, examples of it, and key considerations and recommendations * International organizations and networks specialized in informal and formal cybercrime cooperation experience and possibilities (INTERPOL NCB and NCRP, EU mechanisms, EUROPOL, EC3, EUROJUST, EJCN, EJN) * Council of Europe Convention on Cybercrime 24/7 Contact Point Network for fast cybercrime reaction setups and experiences in exchanging information * Country specific experience on the international response to cybercrime (can be adjusted) | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The opening slides are the introduction to the session and include the Agenda and the session objectives together with some refresher subtopics from Introductory training. | |
| 4 to 6 | These slides are giving insight in the differences between formal and, so called, informal mutual legal assistance in criminal matters.  Prosecutors or judges making a formal request should always assert the international obligation of a requested state to assist where such an obligation exists by way of international instrument. Equally, the authority upon which the letter of request is written should also be spelt out.  Administrative assistance can, and should, also be used when making evidence-gathering requests to a state where no coercive power (e.g. a warrant or court order) is required to be exercised to obtain the evidence. Such an approach reduces the risk of delay and will be welcomed by most states. | |
| 7 to 8 | These slides are giving some examples for formal and informal assistance.  It should be remembered that the regime of mutual legal assistance is one for the obtaining of evidence; thus, the obtaining of intelligence and the locating of suspects or fugitives should usually only be sought by way of administrative assistance to which, of course, agreement may or may not be forthcoming.  Although no definitive list can be made of the type of enquiries that may be dealt with informally, some general observations might be useful.  However, variations from state to state must always be borne in mind. | |
| 9 to 12 | These slides are exploring admissibility of evidence acquired through informal assistance and some key considerations and recommendations.  Any consideration of administrative assistance should not overlook the use to which such assistance can be put to pave the way for a later, formal, request.  The potential difficultly in failing to heed these elements might be that (in States with an exclusionary principle in relation to evidence) such evidence will be excluded; in addition, but of no less importance, inappropriate actions by way of informal request may well irritate the authorities of the foreign State, who might therefore be less inclined to assist with any future request. | |
| 13 - 15 | These slides are explaining setup and possibilities for use of INTERPOL as an informal information network exchange.  Each of member countries hosts an INTERPOL National Central Bureau (NCB). This connects their national law enforcement with other countries and with the General Secretariat via our secure global police communications network called I-24/7.  NCBs contribute national crime data to our global databases, in accordance with their respective national laws. This ensures that accurate data is in the right place at the right time to allow police to identify a trend, prevent a crime, or arrest a criminal. For example, our Red Notices alert police in all countries to wanted persons.  NCBs cooperate on cross-border investigations, operations and arrests. To take investigations beyond national borders, they can seek cooperation from any other NCB. | |
| 16 to 18 | These slides are explaining European Union instruments regarding MLA. EU Convention from 2000 to encourage and facilitate mutual assistance between judicial, police and customs authorities on criminal matters and to improve the speed and efficiency of judicial cooperation. It supplements the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its 1978 Protocol.  These slides are presenting the scope of the work of EUROPOL and its EC3 centre with this regard.  Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses, and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds on-the-spot operational-support deployments resulting in hundreds of arrests, and has analysed hundreds of thousands of files , the vast majority of which have proven to be malicious. | |
| 19 to 22 | These slides are presenting the scope of the work of EUROJUST with this regard. To reinforce the fight against serious organised crime, the European Council, in its Conclusion 46, agreed that a unit (Eurojust) should be set up, composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to its own legal system.  In July 2013, the European Commission submitted a proposal to the European Parliament and the Council for a new regulation on Eurojust to provide a ‘single and renovated legal framework for a new Agency for Criminal Justice Cooperation (Eurojust)’, the legal successor of Eurojust as established in 2002.  European Judicial Cybercrime Network(EJCN) was established in 2016, during the Dutch EU Presidency, to foster contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase efficiency of investigations and prosecutions.  The EJCN facilitates and enhances cooperation between competent judicial authorities by enabling the exchange of expertise, best practice and other relevant knowledge regarding the investigation and prosecution of cybercrime. The network also fosters dialogue among different actors and stakeholders that play a role in ensuring the rule of law in cyberspace. | |
| 23 to 28 | These slides are covering Council of Europe 24/7 Contact Point Cybercrime Network.  Under Article 35 of the Convention each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of this Chapter, in particular as defined under Article 35, paragraph 1, litteraea) – c). It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime.  Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer- or computer-related crime, yet other choices may be appropriate for a particular Party, given its governmental structure and legal system. | |
| 29 to 36 | These slides are presenting the capacity building efforts under one of the projects of the Council of Europe specifically aimed at improving international cooperation. The findings of regional Reports produced by Cybercrime@EaP projects can be used as a resource for discussing more practical, down-to-earth approaches to improving cooperation. | |
| 37 to 39 | The final slides allow the trainer to review the learning objectives with the audience so that they may be sure that they have been achieved. It is also an opportunity for the delegates to raise any issues that may be outstanding or where they have not fully understood the subjects presented.  In addition, the trainer may use the session to check the knowledge learned by asking questions of the participants. This is important as there is no formal assessment for the course. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No knowledge check or assessment has been requested for this session. | | |