Council of the European Union

Brussels, 9 June 2017
(OR. en)

9986/17

GENVAL 63
CYBER 92

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime" - Draft Final report

In line with Article 2 of Joint Action 97/827/JHA of 5 December 1997[1], the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European policies on prevention and combating cybercrime.

Delegations will find in the Annex the draft final report on the seventh round of mutual evaluations. This document encompasses the conclusions and recommendations contained in the previously prepared country specific reports.

[1] Joint Action 97/827/JHA of December 1997 adopted by the Council on the basis of article K.3 of the Treaty on European Union, establishing a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organised crime (OJ L 344, 15.12.1997).

The draft final report, prepared by the General Secretariat of the Council, will be presented to the GENVAL Working Party at its meeting of 13 June 2017, with a view to a preliminary exchange of views.

Delegations will be invited to submit written comments on the draft final report **by 3 July 2017** to the General Secretariat of the Council (secretariat.mutual-evaluation@consilium.europa.eu and giovanna.giglio@consilium.europa.eu).

The final version of the report will be submitted to COREPER and to Council for information on the results of the evaluation. It is recalled that, in accordance with the procedure laid down in Article 8(3) of Joint Action 97/827/JHA, the Council, if it sees fit, may address any recommendations to the Member State concerned, and may invite it to report back to the Council on the progress it has made by a deadline to be set by the Council.

In accordance with Article 8(4) of the above Joint Action, the final report should also be forwarded to the European Parliament for information.

ANNEX

Final report on the 7th round of mutual evaluations on "The practical implementation and operation of the European polices on prevention and combating cybercrime"

TABLE OF CONTENTS

I- INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997 establishing a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organized crime, this reports attempts to summarise the findings, and recommendations and to draw conclusions regarding the seventh mutual evaluation round.

In accordance with Article 2 of the above Joint Action, the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on prevention and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud and should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

[2] OJ L 335, 17.12.2011, p. 1.
[3] OJ L 218, 14.8.2013, p. 8.

The questionnaire for the seventh round of mutual evaluations was discussed by GENVAL on 27 November 2013 and on 22 January 2014 and subsequently adopted by silence procedure on 31 January 2014. The order of visits, subject to certain adjustments, and the composition of the evaluation teams in relation to the observers were approved by GENVAL on 1 April 2014.

In accordance with Article 3 of Joint Action 97/827/JHA, experts with substantial practical knowledge in the field were nominated by Member States pursuant to a written request to delegations made by the Head of Unit DGD 2B of the General Secretariat of the Council on 28 January 2014. On each mission, three national experts took part in the evaluation. Other experts, from the Commission, Eurojust Europol and ENISA participated in some evaluation missions as observers. The General Secretariat of the Council coordinated and participated in the missions with one or two staff for each evaluation, prepared the process and assisted the experts.

The first evaluation mission was conducted in France between 28 and 31 October 2014. The final evaluation mission took place in Sweden between 27 and 30 September 2016. All 28 evaluation missions have resulted in detailed reports on the individual Member States. These evaluation reports have subsequently been discussed and adopted in GENVAL[4]. Most of them are available on the Council's website and publicly accessible.

[4] France (7588/2/15 REV 1 DCL 1); Netherlands (7587/15 DCL 1); UK (10952/2/15 REV 2 DCL 1); Romania (13022/1/15 REV 1 DCL 1); Slovakia (9761/1/15 REV 1 DCL 1). Estonia (10953/15 DCL 1); Slovenia (14586/1/16 REV 1 DCL 1); Italy (9955/1/16 REV 1 DCL 1); Spain (6289/1/16 REV 1 DCL 1); Bulgaria (5156/1/16 REV 1 DCL 1); Lithuania (6520/1/16 REV 1 DCL 1); Malta (7696/1/16 REV 1 DCL 1); Greece (14584/1/16 REV 1 DCL 1); Croatia (5250/1/17 REV 1 DCL 1); Portugal (10905/1/16 REV 1 DCL 1); Cyprus (9892/1/16 REV 1 DCL 1); Poland (14585/1/16 REV 1 DCL 1); Czech Republic (13203/1/16 REV 1 DCL 1); Hungary (14583/1/16 REV 1 DCL 1); Latvia (5387/1/17 REV 1 DCL 1); Denmark (13204/1/16 REV 1 DCL 1 + COR 1); Belgium (8212/1/17 REV 1); Austria (8185/1/17 REV 1); Germany (7159/1/17 REV 1 DCL 1); Luxembourg (7162/1/17 REV 1 DCL 1); Ireland (7160/1/17 REV 1 DCL 1); Finland (8178/17); Sweden (8188/17 REV 1).

This document reflects the conclusions and recommendations contained in the previously prepared country specific reports[5]. It should be noted, however, that due to the long-lasting character of the evaluation, the country reports do not always reflect the current state of play.

[5] The country reports were produced right after the visit to the Member States. Changes, e.g. the completion of implementation of legislation, may have happened after that, which is not reflected in the country reports. The follow-up to the evaluation reports, due 18 months after the adoption, should reflect the amendments made. At the time of the discussion of the report in GENVAL, Member States often announced (future) changes to follow recommendations made in their individual report.

II- EXECUTIVE SUMMARY

- As a result of the more frequent use of the Internet, cybercrime is an expanding criminal phenomenon, and new trends, modus operandi and forms of crime are emerging, both cyber-related offences, which are legally defined as having a cybercriminal aspect, and cyber-enabled offences, which are ordinary offences committed using Information Technology. Therefore, in all countries moving forward in the fight against cybercrime requires a high level of political will, budgetary efforts and a major human and technical resources investment.

- The evaluation has shown that all the Member States take the fight against cybercrime seriously and have structures, resources and measures in place for this purpose. However, the degree of commitment and efficiency varies in the Member States and in some cases there is room for improvement in relation to certain aspects of the overall approach to tackle cybercrime. At the same time, some common problems and challenges have been identified in the 7th evaluation round that can be summarized as follows.

- At the time of the evaluation, the majority of the Member States had adopted a National Cyber Security Strategy, providing a framework to establish the national priorities as well as the key coordination structures at strategic and operational level in order to fight against cybercrime and ensure cyber resilience,whereas a few Member States were in the process of doing so. Some Member States had also adopted an Action Plan for the implementation of the National Cyber Security Strategy.

- At the time of the evaluation, most Member States had signed and ratified the 2001 Council of Europe Budapest Convention on Cybercrime and its additional Protocol on the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Member States who have not yet done so were invited to sign and ratify these instruments.

- One of the main shortcomings identified concerns the collection of separate statistics on cybercrime and cyber-security, as those available are insufficient, fragmented and incomparable in most Member States. Reliable statistics are needed to have an overview of, monitor and analyse trends and developments of cybercrime,with a view to taking appropriate action and assessing the effectiveness of the legal system in countering this form of crime. Member States have therefore been recommended to collect specific and comprehensive statistics for cybercrime in the different stages of the proceedings on the basis of a standardized approach.

- Due to the rapid development of IT with increasingly sophisticated methods, and the complexity of cybercrime, a high degree of specialisation of practitioners working in this area is extremely important. According to the findings of the evaluation, the level of specialization is generally sufficient or satisfactory for the Law Enforcement Authorities, whereas there is room for improvement as regards the judiciary, as in several Member States, cybercrime is dealt with by general Prosecution Offices and criminal Courts. It has therefore been recommended to Member States to increase the level of specialisation of their judiciary staff dealing with cybercrime cases.

- For the same reasons the evaluation has highlighted the importance of providing regular and continuous specialist training on cybercrime both for the Law Enforcement Authorities and for the judiciary, including by making best use of the training opportunities provided by EU bodies, such as EC3/Europol, ECTEG, Eurojust, OLAF and CEPOL.

- The evaluation has emphasised that close and effective inter-institutional coordination and cooperation based on a multi-agency approach at strategic and operational level between all relevant public and private stakeholders involved in cybercrime and cyber-security, is a key element to efficiently fight against cybercrime and to ensure a good level of resilience of the national cyber- security system against cyber threats. In some Member States such cooperation, however, has not been sufficiently developed yet or can be further improved.

- For this purpose, Member States have also been encouraged to consider the possible establishment of a central body/entity where both the public and the private sector are represented, to coordinate the activities in this area.

- Close cooperation between the public and the private sector - financial/ banking institutions, telecommunication companies, ISPs, NGOs, academy, business, professional associations, etc. - is crucial in this context, as their expertise is of great added value for the success of investigations and of actions to resolve cyber-incidents. The most advanced forms of cooperation with the private sector are institutionalised by the establishment of appropriate institutions/working groups. Public/Private Partnerships has been identified by the evaluators as an important tool for a good cooperation between the Law Enforcement Authorities and the private sector.

- Some Member States have direct contacts with ISPs located abroad, especially in the US, but cooperation with such companies is quite problematic because they do not answer every request or require MLA/letters rogatory or a court warrant in order to provide the requested information; therefore, the evaluation highlighted that the EU and its Member States should reflect on how to improve such cooperation.

- The growing use of encryption with more and more sophisticated techniques is increasingly becoming a problem in all the Member States as it makes it difficult or prevents completely getting access to relevant information regarding online crime or cybercrime. Decryption is possible only by using high capacities specialised hardware and software and the evaluation has shown that there is limited success in addressing, especially more complex cases, of encryption. Many Member States make use of Europol decryption platform EU Cyber Crime Centre (EC-3). According to the findings of the evaluation, the challenges posed by encryption could be partially offset by stepping up research and development and developing new methods, as well as with good cooperation among the various authorities involved. Member States and the EU institutions were also recommended to consider the elaboration of a decryption order.

- The nature of e-evidence, and the ease with which it can be manipulated or falsified, may create issues with regard to admissibility that do not arise with other types of evidence. For this reason, in some Member States there are specific requirements regarding the collection of e-evidence in order to be admissible in courts. However, the evaluation has shown that in most Member States, procedural law is mainly technology-neutral, which means that general rules and principles on gathering of evidence are applied and that the procedural system does not contain any specific formal rules on admissibility and assessment of e-evidence.

- In certain Member States the national legislation allows obtaining subscriber information directly from foreign providers, whereas in other Member States it is necessary to follow MLA procedures, should be faster and more effective. Member States have been invited to ensure that their national legislation is flexible enough to facilitate the admissibility of e-evidence, including when obtained from another country.

- The evaluation highlighted that cybercrime committed in the "cloud" generally raises problematic issues for investigation and prosecution as the information in the "cloud", are not easily located and accessed by the Law Enforcement Authorities. Depending on the type of cybercrime, the effect may be pinpointed to several States' jurisdictions, including outside the EU. Conflicts of jurisdiction can therefore arise where the assistance of Eurojust and EJN can be sought. The evaluation highlighted the importance to address these challenges at EU level.

- The evaluation has confirmed Member States' concerns in relation to the absence of a common legal framework on data retention at EU level. This has an impact on the effectiveness of criminal investigations and prosecutions, in particular in terms of reliability and admissibility of evidence to the courts, based on the collection of electronic communication data, as well as on cross-border judicial cooperation. A common reflection process involving the EU institutions and the Member States is currently ongoing to address the issue of data retention with a view to identifying legal and practical solutions to the challenges arising from the ECJ case law.

- Sexual child abuse on the Internet in its various forms has significantly increased in recent years. In order to effectively combat such forms of crime, a wide range of both preventive (i.a. training and information campaigns aimed at raising awareness) and of coercive measures (blocking access or removal of illegal content) involving both the public and the private sector are implemented to a various extent in the Member States. The evaluation has shown that only some Member States have a national database dedicated to victims' identification for combating the sexual abuse of children; the others Member States who only use Interpol's International Child Sexual Exploitation Database (ICSE-DB), have been recommended to develop such national database. Several Member States have measures to prevent re-victimisation, including in some cases to protect victims and witnesses of child sexual abuse during criminal proceedings. Good cooperation between all relevant stakeholders, namely the Law Enforcement Authorities, the hotlines, NGOs and ISPs has been identified as an essential element to tackle this forms of crime.

- As regards cyber-security, a crucial role in monitoring and responding to cyber incidents is played by the national CERTs that the majority of the Member States have already established. Moreover, it was recommended to Member States to introduce into their national law the obligation for the private sector to report without delay cyber-attack incidents having a significant impact on the continuity of essential services to the LEAs . Both issues are provided for by the NIS Directive and will have to be implemented by 9 May 2018.

- Since cybercrime, other cyber-related crimes and their investigation frequently involve more Member States, cooperation and sharing of information with EU Agencies - Europol/EC3, Eurojust, the EJN and ENISA - is a priority. For the same reason a more extensive use of the Joint investigation Teams (JITs) was recommended, as an effective instrument for conducting cross-border investigations.

- The Internet has no borders, and therefore smooth and well-functioning international cooperation is crucial for tackling cybercrime efficiently. However, as highlighted by the evaluation, MLA procedures are on the contrary slow, time-consuming and ineffective, with a negative impact on the investigations, as digital evidence is volatile and must be handled rapidly. There is consequently a need to speed up the handling of MLA requests in cybercrime investigations. In addition, Member States have been encouraged i.a. to make more frequent use of Eurojust, EJN and Europol tools and to develop informal contacts with the competent foreign authorities in order to obtain faster responses to MLA requests.

III - NATIONAL CYBER SECURITY STRATEGY

KEY FINDINGS AND CONCLUSIONS

- ENISA has developed a Practical Guide on the Development and Execution of National Cyber Security Strategies in 2012. According to its findings, a National Cyber Security Strategy is a tool to improve the security and resilience of national infrastructures and services.

- In general the purpose of a National Cyber Security Strategy is to provide a framework to establish the national priorities as well as the key coordination structures at strategic and operational level in order to fight against cybercrime and ensure cyber resilience.

- A comprehensive National Cyber Security Strategy should be targeted and contain specific and measurable objectives as well as clear delineation of responsibilities, so as to ensure coordination of the roles of the different stakeholders and to provide an estimation of the costs for relevant actions to be undertaken.

- At the time of the evaluation, the majority of the Member States had adopted a National Cyber Security Strategy, and some of them also an Action Plan for its implementation, whereas a few Member States were in the process of doing so.

- Following the development of a National Cyber Security Strategy and, where appropriate, of an Action Plan, it is essential to ensure a proper follow-up and to monitor the implementation of the National Strategy closely.

- Due to the rapid development both of Information Technology (IT) and of new types of cyber-related offences, there is also a need for constantly updating the measures and means put in place to fight cybercrime effectively, and therefore for ensuring, when necessary, the timely review of the National Cyber Security Strategy.

- The establishment of a single body with coordination functions for the implementation of the National Cyber Security Strategy, as in some Member States, can be considered as a good practice to be followed by other Member States.

- The adoption of a National Strategy on the security of network and information systems is foreseen in the newly adopted Directive 2016/1148/ (NIS Directive) in order to define the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintain a high level of security of the of networks and information systems (Article 7).

RECOMMENDATIONS

- ***Member States who have not yet adopted a National Cyber Security Strategy are encouraged to do so in the best possible timeframe and consider also the adoption of an Action plan; those who have adopted it, should ensure its proper implementation, and the possible attribution to a single body/entity with coordinating functions for this purpose.***

- ***Member States should update their National Cyber-Security Strategy whenever necessary, in line with relevant IT developments as well as with trends in the area of cybercrime.***

IV - BUDAPEST CONVENTION

KEY FINDINGS AND CONCLUSIONS

- The 2001 Council of Europe Budapest Convention on Cybercrime, is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It also foresees a series of powers and procedures such as the search of computer networks and lawful interception.

- Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

- Articles 16, 17, 29 and 30 of the Convention, in particular, govern the expedited preservation of stored computer data and traffic data and the partial disclosure of traffic data, whereas Article 35 establishes the international 24/7 network for emergencies, which enables data to be frozen, thus allowing digital evidence to be kept. The latter is an important instrument as it creates a fast possibility of preservation of digital evidence before sending an MLA.

- The Budapest Convention is supplemented by an additional Protocol on the criminalisation of acts of a racist and xenophobic nature committed through computer systems and, as regards the Protection of Children against Sexual Exploitation and Sexual Abuse, by the Lanzarote Convention.
- At the time of the evaluation, most Member States had signed and ratified these instruments, whereas a few Member States had not yet done so. The Council conclusions on improving criminal justice in cyberspace of 9 June 2016 reiterated the request to Member States to ratify and implement fully the Convention on Cybercrime of 23 November 2001.

RECOMMENDATIONS

- ***Member States who have not yet done so are invited to sign and ratify the 2001 Council of Europe Budapest Convention on Cybercrime and its additional Protocol and to fully implement these instruments.***

V- STATISTICS

KEY FINDINGS AND CONCLUSIONS

- The analysis of the EU legislation shows a clear need to collect statistics in the area of cyber-criminality. According to Article 14 para 1 of Directive 2013/40/EU on attacks against information systems, Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 7.

- According to Article 14 par. 2 of the same Directive the statistical data referred to in paragraph 1 shall, as a minimum, cover existing data on the number of offences referred to in Articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of the offences referred to in Articles 3 to 7.

- Furthermore, pursuant to recital 44 of Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, Member States are encouraged to create mechanisms for data collection or focal points, at the national or local levels and in collaboration with civil society, for the purpose of observing and evaluating the phenomenon of sexual abuse and sexual exploitation of children.

- Moreover, the need to collect statistics at the national level results *"in principio"* in the Member States from their national law or regulations.

- Statistics on cyber-criminality are extremely important. On the one hand, they make possible a detailed analysis and insight on the extent of the new emerging trends of this expanding form of crime, thus allowing to have an overview and to monitor its developments, with a view to taking appropriate action; on the other hand, they allow to assess the effectiveness of the legal system and the adequacy of legislation in countering cyber criminality and in protecting the private interests of citizens victimized.

- Furthermore, the collection of statistical data facilitates the work of the EU institutions (the Commission) and agencies (Europol, Eurojust or ENISA) involved in countering cybercrime. They allow to gain a more complete picture of the problem of cybercrime and network and information security at the EU level and thereby contribute to formulating a more effective response.

- The statistics are also important to have a realistic image about the rate of cybercrime. i.e. due to the underreporting of such offences, including serious ones, to the Law Enforcement Authorities by victims - both individuals or banks or companies.

- Comprehensive statistics should cover all the fields deemed important for this kind of crime at all stages of the proceedings: investigation, prosecution, trial, the specific criminal offence and the specific investigative measure, the number of reported offences, the number of investigations carried out and the decisions not to investigate certain types of cybercrime, the number of victims and of victim's complaints, the number of persons prosecuted and convicted for different kinds of cybercrime, the number of cross-border cases, the outcome of MLA requests and the duration of the procedure.

- However, one of the main shortcomings identified in the 7th evaluation round in the majority of the Member States concerns the collection of separate statistics on cybercrime, cyber-enabled crime (ordinary offences committed using Information and Communication Technology) and cyber-security incidents. Those available are insufficient, fragmented and incomparable in most Member States.

- Furthermore, many Member States do not have a common national definition of cybercrime and cyber-enabled crime for statistical purposes. In many Member States it is not possible to identify the share of cybercrime in the overall criminality picture, and other Member States who collect specific statistics on cybercrime generate them as a single figure; consequently, it is not possible to divide them into categories and to distinguish between the cases that concern cybercrimes "*stricto sensu"* and cyber-enabled offences. Not all Member States produce regular statistical reports on cybercrime.

- In most Member States judicial statistics are separated from the Law Enforcement Authorities' statistics. As statistical systems often vary significantly from one competent authority to another and each authority collects and from different sources with different methods and manages them with different criteria and/or using different databases with no interoperability among them, cybercrime cannot be tracked in one single statistical system.

- In many Member States cybercrime figures entered in the various systems are very low. In these cases questions may arise about the efficiency of detection, prosecution and punishment of cybercrime and about the accuracy of statistical records.

- Sharing statistics among Law Enforcement and judicial authorities could be of great value for a follow-up mechanism as well as for the prioritisation of goals in combating this phenomenon. Often, however, there is no or insufficient exchange of statistical data among the different national authorities involved in tackling cybercrime.

RECOMMENDATIONS

- ***Member States facing problems related to the lack of common definition or of common understanding of cybercrime are encouraged to develop a consistent national definition (or understanding) of cybercrime to be applied by all stakeholders involved in fighting cyber criminality and for the purpose of compiling statistics.***

- ***Member States should gather specific statistics for cybercrime allowing both to check the overall cybercrime figures and to identify the share of cybercrime in the global criminality picture.***

- ***Member States should develop a standardized approach to collect comprehensive statistics in the different stages of the proceedings, broken down into specific cybercrime areas, preferably those identified at the EU level, i.e. online child sexual abuse, online card fraud and cyber- attacks.***

- ***Member States should consider solutions allowing interoperability of the various databases containing cybercrime figures, with a view to quickly achieving cases comparison, criminal identification and cases quantification.***

VI - STRUCTURES – THE JUDICIARY

KEY FINDINGS AND CONCLUSIONS

- The structure and the organisation of the judiciary vary in the different Member States, including the attribution of competence for dealing with cybercrime cases.

- Due to the rapid development of ICT and the complexity and increasingly sophistication of cybercrime, successful investigations, prosecutions and convictions in cybercrime cases depend to a large extent on how skilful and experienced the authorities in charge of investigation and trial are. A good level of understanding and knowledge, and of specialisation of the judiciary in this area is therefore of utmost importance.

- However, according to the findings of the mutual evaluation, the degree of specialization of prosecutors and judges dealing with cybercrime matters and related offences is not always satisfactory.

- In a significant number of Member States cybercrime is dealt with by general Prosecution Offices and in all Member States there are no specialised courts or judges appointed for examining and adjudicating cybercrime cases. On the contrary, some Member States have specialised prosecutors or specialised structures within the Prosecution Services dealing with cybercrime offences.

- In a few Member States there are Prosecution Offices/Sections whose competences include the offences committed or ordered by organized criminal groups or economic crime and corruption, among which cybercrimes offences.

- According to the internal practices of organisation of the judiciary, based on prosecutors' specialisations or on the concentration in judicial offices of cybercrime cases, in a few Member States the responsibility for dealing with such crimes usually lies "*de facto"* with specialised public prosecutors and judges, who have been trained or have experience in the area of cybercrime thus acquiring in practice a high degree of specialisation, which allows them to provide assistance to their colleagues.

- In some Member States, there are cyber-prosecutors' national networks specialized in cybercrime, which can be considered as a good practice, as they allow to exchange knowledge and experience and to facilitate the spreading of best practices among practitioners.

- The evaluators had recommended Member States to facilitate, with the support of Eurojust, the creation of a European network of judges specialising in the fight against cybercrime, aimed at improving and facilitating judicial cooperation in this field. In the meantime, this objective has been achieved with the establishment in June 2016 by Council conclusions of of the European Judicial Cybercrime Network (EJCN), which has already started to work.

RECOMMENDATIONS

- ***The Member States should increase the level of specialisation of their judiciary, with a view to efficiently prosecuting and sanctioning cyber-related and cyber-enabled offences. For this purpose, they should preferably establish specialised offices or internal structures/units and/or appoint specialised prosecutors and judges with a good level of understanding and knowledge of cybercrime, to deal with such cases.***

- ***The Member States should establish networks of prosecutors and judges specialized in cybercrime at national level as an additional tool for improving the efficiency of the fight against this type of crime.***

VII - STRUCTURES - THE LAW ENFORCEMENT AUTHORITIES (LEAs)

KEY FINDINGS AND CONCLUSIONS

- The structure and the organisation of the Law Enforcement Authorities (LEAs) vary significantly in the different Member States, including as regards the attribution of competence for cybercrime. In some Member States, specialized units work on the basis of a two-stranded approach involving strategic planning and operational activities, whereas in other Member States these functions are performed separately by different authorities and bodies.

- An effective organisation, international integration and professional competence of LEAs involved in cybercrime investigations are key elements in tackling this crime effectively. A good level of knowledge and specialisation of the LEAs, for the same reasons highlighted for the judiciary, is also essential to fight against this complex and sophisticated form of crime efficiently.

- Generally, the mutual evaluation showed that the degree of specialisation of the LEAs is higher than for the judiciary, but that in many cases it can be improved.

- In most Member States, there are specialised central cybercrime structures or units within the Ministry of Interior and/or the Police, in charge of preventing and fighting cybercrime at national level, thus ensuring the coordination of the investigation of cybercrime across the country with a great level of specialization in this area. This also facilitates the communication between the Police and prosecutors. In several Member States there are also decentralised specialized Units at local and or regional level dealing specifically with cybercrime investigations.

- Some Member States have been recommended to proceed with police reorganisation and make relevant steps in terms of increasing the number of human resources, providing more effective and intensive training of police, and sufficient technical equipment dedicated to the fight against cybercrime. Furthermore, LEAs' equipment and resources need to be constantly updated to cope with constant development and diversification of cybercrime modus operandi.

- The main obstacles to successful investigation of cybercrimes are, among others, the rapid development of technology, the increasing professionalism and level of expertise of cybercriminals, the fact that cybercrime can easily span over the jurisdiction of several countries, the difficulty in obtaining access to e-evidence in regard to cybercrime and the challenges related to the use of encryption, TOR and anonymisation.

- Currently there is no national network of police officers specialised in cybercrime in any Member States.

RECOMMENDATIONS

- ***Member States should maintain and, where appropriate, increase, the level of specialisation of LEAs dealing with cybercrime investigations. Member States who have not done so yet, should consider setting up specialised units within LEAs to combat cybercrime more effectively also at regional/local level.***

- ***Member States should consider creating a network of police officers specialized in cybercrime at national level that could also help maintaining a communication channel from public and private sector to the police.***

- ***Member States should consider strengthening non-technical police personnel across the district or regional structures and ensuring sufficient technical equipment catered for their needs.***

VIII - COOPERATION AND COORDINATION AT NATIONAL LEVEL

KEY FINDINGS AND CONCLUSIONS

- As cybercrime has a cross-cutting nature and the responsibility for the security of cyberspace at national level is generally shared among different actors, with different responsibilities and capabilities, whether public or private, military or civilian, collective or individual, a multidisciplinary approach is a key factor for preventing and combating efficiently cyber-criminality and ensuring cyber-resilience.

- In this context, close and effective inter-institutional coordination and cooperation between the different public authorities and bodies at operational and strategic level as well as between central and local/regional authorities in order to coordinate initiatives and strengthen data exchange, technical support and investigative techniques, is essential.

- A close cooperation in countering cybercrime is needed not only between the Police and the Prosecution services, but also with the national Intelligence Services to receive support from a technical point of view (interceptions, expertise, etc.) and with intelligence to the criminal investigations and prosecutions, in particular for obtaining and processing digital evidence.

- Cooperation between the public and private is also crucial for the successful investigation, prosecution and conviction of cybercrime and cyber enabled offences and for the response to cyber threats and attacks (for more details see following chapter).

- Together with the legal framework for inter-agency cooperation, where it is defined, usually the National Cyber Security Strategy and, where it exists, the Action plan for its implementation, set up the general framework for the coordination and cooperation among all the public institutions and authorities with responsibilities in the area of cyber-security, and with the private sector, in order to ensure the delineation of roles and responsibilities.

- The proper implementation of the National Cyber Security Strategy is therefore a key factor for providing synergies and maximizing readiness as well as reaction capabilities in countering cybercrime and strengthening cyber-security.

- According to the finding of the evaluations, forms, modalities and levels of cooperation and coordination among relevant stakeholders involved in the fight against cybercrime and in ensuring cyber-security vary in the different Member States, some of which have developed more advanced and efficient forms of interaction than others, that in individual reports have been identified as good practices.

- The best way to ensure the proper functioning of the system is a structured mechanism, especially where coordination functions for cyber security issues and for the policies against cybercrime are assigned to a single institutional authority (i.e. Ministries or offices in their organizational structure) or to an "ad hoc" single body or entity. Such single institution/body, providing an institutional framework for cooperation where both public and private stakeholders involved in fighting cybercrime and in cyber-security are represented, already exists in some Member States, and at the time of the evaluation other Member States were considering its establishment.

- In a few Member States there is no legal framework for inter-agency cooperation in cases concerning cybercrime and the authorities involved in investigating and prosecuting cybercrime cooperate in an informal manner, as they know their counterparts in the other authorities and therefore get in touch very easily; this works well, facilitating contacts and dialogue without unnecessary bureaucratic delays.

- Some Member States where shortcomings have been identified in the context of the mutual evaluation are making efforts to strengthen existing structures and processes of cooperation and coordination, with a view to preventing and combating cyber criminality more effectively.

RECOMMENDATIONS

- ***The Member States should prioritise institutional coordination and cooperation among all relevant stakeholders involved in the prevention and fight against cybercrime and in cyber-security, based on a multidisciplinary approach, with a view to providing synergies as well as maximizing readiness and reaction capabilities.***

- ***The Member States are in particular encouraged to introduce or strengthen a structured cooperation framework and to possibly establish a central body/entity where both public and private stakeholders involved in fighting in cybercrime and in cyber-security are represented, with coordinating functions and decision making powers.***

IX - COOPERATION BETWEEN THE PUBLIC AND THE PRIVATE SECTOR

KEY FINDINGS AND CONCLUSIONS

- Close cooperation between the public and the private sector is of fundamental importance, as countering cybercrime is very complex, which means that Law Enforcement Authorities cannot successfully fight against this crime without the cooperation of the private sector (financial/ banking institutions, telecommunication companies, ISPs, NGOs, academy, business, professional associations, etc.).

- Such cooperation could work to the benefit of both sectors, as it creates the opportunity to involve a wide range of entities working together, and to ensure synergies among them, thus contributing to increase the level of cyber-security.

- The contribution of the private stakeholders in terms of expertise, technical support and exchange of information on cyber-threats and cyber-security trends is of great added value for the success of investigations and of actions to resolve cyber-incidents. It is also useful to involve prosecutors in contacts with the private sector, so as to ensure that evidence is gathered in compliance with current legislation and is admissible in court proceedings.

- According to the findings of the evaluation, the level of cooperation between the public and the private sector varies in the Member States, and generally proves to be more developed and efficient where it is more structured and where there is an environment of confidence and trust. In some Member States the evaluation has identified good practices, whereas in others a need for improving such cooperation has been underlined.

- Some Member States in order to prevent and combat cybercrime and to ensure cyber-security, make an extensive use of public/private partnerships, which in some cases is foreseen in the National Cyber-security Strategy, whereas in others its use is limited to some specific areas or not yet implemented. It may be defined in various forms, including on the basis of Memoranda of Understanding or similar formal agreements.

- According to the findings of the evaluation, Public/Private Partnerships, has been identified by the evaluators as an important tool for a good cooperation between the Law Enforcement Authorities and the private sector, especially with Internet Service providers, and the financial sector, in particular banks, but also with NGOs, CERTs and critical infrastructure.

- As stated in some individual reports, regulation of the Public-Private Partnership with a framework establishing duties and rules, helps information flow and management, as it enables informal processing, instead of using more traditional methods based on an official exchange of documentation at the formal request of the Law Enforcement Authorities.

- The most advanced forms of cooperation with the private sector have been identified in some Member States where such cooperation is institutionalised by the establishment of appropriate institutions/working groups for cooperation between the private sector and the public administration/law enforcement bodies. This is more frequent as regards cooperation with the banking sector (see below), but, as recommended in some individual reports, it is useful to extend such form of cooperation to other areas and stakeholders in the private sector.

- Not all Member States have however developed a formal framework for Public/Private Partnerships, and in some of them cooperation, meetings and exchange of information on incidents, trends and developments with the private sector take place informally, rather than on a legal or contractual basis.

- Cooperation with Internet Service Providers (ISPs) or cloud service providers and with providers of electronic communications services is extremely useful both to benefit from their expertise and for accessing subscriber information pertaining to cybercrime. By conducting risk assessments, taking the appropriate security measures and applying a structured security policy, providers of electronic communications networks and services may not only prevent the occurrence of certain types of cybercrime, but also assist the LEAs with the provision of substantial evidence, under the condition that it is acquired through the procedures prescribed by law.

- According to the findings of the evaluation, there is a need to identify solutions for a clear and appropriate framework regulating the relations of the judicial authorities with ISPs across the EU. For this purpose, having procedures that could enable authorities to receive answers to their requests in a timely manner, and putting in place a system of penalties for non-compliance/cooperation/failure (administrative or procedural fine) could improve such cooperation.

- Some Member States have direct contacts with ISPs located abroad, especially in the US, but cooperation with such companies is quite problematic because they do not answer every request or very often reply that without MLA/letters rogatory or court warrant, they are not able to provide the requested information. These situations have a strong impact on investigations and sometimes can even lead to a specific case being closed as the lack of information can make it harder to identify the perpetrator, the time and the location of the offence, and the instrument by which the offence was committed.

- According to the findings of the evaluation, a dialogue with the main Internet operators, hosting companies and Internet access and/or service providers at both the EU and the international level, could strengthen their cooperation in the context of judicial investigations.

- Effective cooperation between the Law Enforcement Authorities on the one part, and financial institutions and commercial banks on the other part, is also essential in the fight against online card fraud and other frauds related to Internet banking (and use of banking malware), with a view to identifying such frauds, updating the private sector with regard to new tendencies and identify precautionary measures.

- In certain Member States such cooperation is facilitated by dedicated banking associations or inter-banking Committees created for countering fraud in the payment systems and means of payment, which held regular meetings, with the participation of the Police. In one Member State, the participation of the Police in the advisory body of the national bank association was considered by the evaluators as a good practice.

- In other Member States cooperation between the Law Enforcement Authorities and the banking and financial institutions is less structured and limited to contacts and/or meetings to ensure collaboration and exchange of information on cybercrime related issues.

- In some Member States there is a reporting obligation for the private sector on cybercrime, whereas in other Member States such reporting is not mandatory or limited to specific branches of the private sector or to certain type of cyber-offences.

- In certain cases reporting of cybercrime occurs on a voluntary basis. However, according to the finding of the evaluations, in some Member States financial and credit institutions and Internet Service Providers are reluctant in reporting and supporting a criminal procedure with the aim of determining the criminal liability of the perpetrator. They are more interested in rebuilding as soon as possible the damage, that could result from publication and media coverage which is not good for their credibility and reputation.

- According to certain individual reports when the private sector is the victim or the injured party, cooperation with the Law Enforcement Authorities is usually good, since it takes care of the preservation of evidence, its interpretation and its delivery to the Law Enforcement Authorities.

- The private sector plays also an important role on the protection of children and in prevention and awareness-raising activities in this respect; private associations and NGOs operating in this field cooperate with the Law Enforcement Authorities involved in combating online sexual exploitation make a key contribution by channelling reports of abuses.

- According to the conclusions of the evaluation, a dialogue with the private sector beyond the mandatory reporting requirements would in any case facilitate better results in combating cybercrime offences.

- Public authorities should also cooperate, as in several Member States, with the academia, educational institutions, social services, business, professional associations, media and other organisations and companies in order to prevent and neutralise the negative impact of computer crime and computer-related crime on the computer information security in the country. In particular, cooperation with academia is very important for awareness-raising, training and Research and Development (R&D).

RECOMMENDATIONS

- ***The Member States should maintain and enhance regular cooperation between the public and the private sector, (banks, telecommunications companies and ISPs), including involving prosecutors and possibly judges, to discuss methodologies to ensure that the gathering of e-evidence takes place pursuant to current legislation, so as to allow its admissibility in court proceedings.***

- ***Member States should make use of structured Public/Private Partnerships, with a view to ensuring a clear framework for cooperation between the public and the private sector with clear rules and duties.***

- ***Member States should encourage the private sector to share information with the public authorities and, where appropriate, provide in the national law a reporting obligation for the private sector of cyber-related offences, in particular for the credit institutions to report without delay cyber-attack incidents that target both the credit institutions and/or their customers.***

- ***The European Union and its Member States should reflect on how to improve the cooperation between Member States' LEAs and international telecommunication companies and Internet access and/or service providers, including the possibility for the EU to conclude agreements with big foreign private companies to facilitate cooperation in criminal matters.***

X - INVESTIGATIVE TECHNIQUES

KEY FINDINGS AND CONCLUSIONS

- Given the wide range of cyber-offences, there cannot be any generally tried and tested procedures or methods for investigating such offences. Each investigation and approach depends on the specific circumstances and the investigative procedures and methods must be tailored to the particular case.

- Especially in the field of cybercrime, the modus operandi, the software and tools that are used change constantly and at short intervals. The investigating measures need therefore to be constantly updated (e.g. with special investigating computer software), in line with the developments of cyber-criminality.

- In addition to the ordinary investigative techniques, special techniques are used for the investigation of cybercrime cases. There are a number of possibilities: the most commonly used special investigative techniques, which are particularly effective working tools in especially when dealing with cases involving child sexual exploitation, are the interception of communications, the preservation of data and the undercover investigation.

- The latter, especially useful if the investigation cannot be carried out using technical means, is conducted by deploying undercover officers to carry out investigations on forums and boards. However, investigations of this kind are only likely to yield satisfactory results if they are carried out over the long term.

- Other special investigative techniques are based on new technical possibilities in tackling computer crime on-line, such as on-line monitoring, or other techniques like hardware access blocks and special bit copiers, remote search and seizure (e.g. in the case of LEAs hacking online of a suspected computer instead of physically obtaining it), IP tracking (e.g. Skype and other messaging services), open-source searches on the Internet, backing up data from data carriers and from the Internet (websites, log files). Special techniques are also used for mobile devices (e.g. UFED).

- However, not always the national legislation of the Member States provides for the use of special investigative techniques. In some Member States a judicial order is needed for this purpose.

RECOMMENDATIONS

- ***Member States who have not yet done so are encouraged to provide in their national legislation the possibility of using special investigative techniques in order to facilitate investigations in cybercrime cases.***

XI - ENCRYPTION

KEY FINDINGS AND CONCLUSIONS

- The increasing availability and use of secure and trustworthy encryption technologies ensures the security, safe transmission and confidentiality of computer data, and consequently the protection of citizens' privacy and effective data protection in the cyberspace.

- However, the growing use of encryption both in data storage and in Internet communications with more and more sophisticated techniques is making harder and harder to get through the encryption, that is increasingly becoming a problem in all the Member States.

- Encryption is often deployed deliberately by criminals to protect the illegal material in their possession and makes both the fight against and the prevention of cybercrime more difficult. Since encryption is default in many applications, and is used across a wide spectrum of offences, the Law Enforcement Authorities often encounter problems with encrypted data.

- The encryption makes it difficult or prevents completely getting access to relevant information regarding online crime or cybercrime, in particular for the identification of communications or computer data in possession of suspects or offenders, not only in forensic examinations but also in all other types of investigations. In addition, the use of end-to-end encryption by an increasing number of service providers makes the interception or interpretation of material difficult.

- There is no standard solution either for encrypted data or for encrypted communications. After examination of the individual case, targeted measures such as special telecommunications surveillance measures or decryption measures can be deployed.

- In this context, the first challenge is to detect the encrypted content, that is not always indicated as such, and the form of encryption using the necessary equipment. The most significant problem is, however, the decryption itself, which is possible only by using high capacities specialised hardware and software requiring high level investments and significant costs.

- In tackling these problems there is a need for familiarity with the present state of the art in encryption technology and to study weaknesses in algorithms and implementations, including in order to take advantage of possible errors.

- The evaluation has shown that some success is usually achieved when very simple forms of encryption methods are used, and that is possible to ascertain or back-calculate keys using appropriate software (such as PRTK via the FTK Platform) that makes decryption possible. Simple passwords can be 'cracked' using the appropriate hardware and tools.

- The investigative authorities may contribute significantly to the success of password cracking if they can provide information relevant to the password itself (possible passphrases, phrase fragments, character set, password length, etc.), and all digital evidence (storage devices) to the computer forensic experts. However, this is not always effective.

- According to the findings of the evaluation, in certain cases more complex content encryption has been successfully bypassed as a result of a brute force - i.e. trying out all possible codes -or dictionary attacks - i.e. using terms devised for password mining - or where the suspect has provided the password or phrase needed to bypass the encryption, to the extent that he/she accepts to cooperate that or has good faith.

- However, not always the data subjects are willing to cooperate with the authorities and there are no means to oblige data subjects to cooperate. As indicated in one individual report, a way for increasing the effectiveness of investigations could be the introduction of the concept of decryption order which could also be elaborated at the European level.

- However, generally speaking, the evaluation has shown that there is limited success in addressing the issue of decryption in all areas, including access, content data and end-to-end encryption, as the algorithms used by criminals and their implementation are often technologically solid.

- The main problems encountered with encryption concern files protected with strong encryption (AES-256 encrypted archives) and whole disk encryption (TrueCrypt, BitLocker, FileVault2, WinRar or PGP). In these cases decryption using brute-force or dictionary attacks can be extremely time-consuming (months, even years in some cases), requires a great amount of computational capacity (specialised commercial software and network cluster infrastructure) to try to break cryptographic protection in cases when the perpetrators use long and complicated passwords in order to find the encryption key.

- According to the findings of the evaluation, in many cases it is therefore not possible to solve the problem of encryption effectively and decryption attempts are not always successful, especially if the password is technically advanced and cannot be retrieved in a reasonable period of time; in certain cases the decryption process is ceased.

- In some Member States, decryption is carried out in cooperation with private companies, whose expertise proves useful especially where the encryption methods are very sophisticated. In several Member States, on the contrary, private companies are not involved in decryption in the context of criminal investigations, which is reserved to the National Forensic Institutes.

- Europol's resources and services, in particular the EU Cyber Crime Centre (EC-3) offer the possibility of using its sophisticated decryption platform and some Member States make use of this facility.

- According to the findings of the evaluation, the challenges posed by encryption can be partially offset with a view to more successful investigations, by stepping up research and development and developing new methods, including for more intelligent analysis of a suspect's pattern(s) of password creation and dynamic aggregation of computer power.

- Good cooperation among the various authorities involved, in particular Law Enforcement Authorities, IT forensics and prosecutors is also indispensable, including because not every department or authority can afford to purchase password recovery hardware and software due to the costs resulting therefrom.

- Cooperation between Member States in the area of decryption is ensured by sharing resources and experience and participating in joint operations. If there is a need to forward evidence to other authorities for decryption, this can be done via the Europol and Interpol channels.

RECOMMENDATIONS

- ***Member States should invest in specialised hardware and software with adequate computational capacity and in staff adequately trained in order to ensure decryption also in complex cases of encrypted files and communications.***

- ***Member States should ensure cooperation among all relevant stakeholders , including, where appropriate with private companies, with a view to increasing the decryption abilities of the competent authorities.***

- ***Member States should step up research and development with a view to developing new and more efficient decryption methods, and make use of Europol facilities, namely of the decryption platform EU Cyber Crime Centre (EC-3) for more sophisticated cases of encryption.***

- ***Member States and the EU institutions should consider the elaboration of a decryption order.***

XII - E-EVIDENCE

KEY FINDINGS AND CONCLUSIONS

- A significant number of Member States does not have a definition of the concept of electronic evidence in their national legislation. The terms used in the Convention on Cybercrime of the Council of Europe (hereinafter referred to as the Budapest Convention), and in Directive 2013/40/EU of 12 August 2013 on attacks against information systems serve as a reference.

- In practice, e-evidence is generally understood as any information generated, stored or transmitted by the use of electronic equipment and capable to ascertain the existence or non-existence of an offence, to identify the person who committed such an offence and to determine the circumstances necessary for the settlement of a case.

- It consists of, but is not limited to, registry information, Internet traffic history, content data, images, IP addresses, emails, electronic documents, digital video files, audio files and images, databases, spreadsheet data, cookies, print outputs, electronic book-keeping, data geo-location from GPS, logs of banking operations performed, etc.

- The collection, analysis and usage of e- evidence can be relevant in criminal proceedings not only in relation to crimes against and by means of computers but also in relation to any other offence that may involve electronic evidence.

- The nature of e-evidence, and the ease with which it can be manipulated or falsified, may create issues with regard to admissibility that do not arise with other types of evidence; for example more evidential material may be needed, such as forensic tool analysis or expert evidence by forensic investigators.

- For this reason, in some Member States there are specific requirements regarding the collection of e-evidence in order to be admissible in courts. This may i.a. involve the collection to be made by an expert with technical knowledge in order to preserve the integrity of e-evidence or good documentation of the evidence chain, as regards how the evidence was originally obtained, who has handled it and how it was handled, including whether it was altered in any way.

- Some Member States for the purpose of collecting e-evidence follow the best practices on digital forensics established in the Council of Europe Convention on Cybercrime or international guidelines as ACPO guidelines, which also apply to storage and transfer of e-evidence.

- However, the evaluation has shown that in most Member States, procedural law is mainly technology-neutral, which means that general rules and principles on gathering of evidence are applied and that the procedural system does not contain any specific formal rules on the admissibility and assessment of e-evidence; the latter is subject to the same conditions of evidence as any other piece of evidence and is evaluated by the judges in accordance with the general criminal rules of procedure.

- Therefore, generally speaking, electronic evidence becomes admissible in criminal proceedings if it is obtained in a lawful manner and is relevant to the trial. This also applies to e- evidence collected from outside the State through cooperation with Member States or through international MLA.

- The absence of regulation on the methodology of collection and presentation of e-evidence before the court, however, as indicated in one individual report, should in principle not hinder the effective prosecution of cybercrime cases, since the admissibility of e-evidence falls within the general evidence regulations.

- In a few Member States, e-evidence, like most traditional evidence, is admissible in court and is evaluated by the judge in accordance with the principle of free assessment of evidence. This means that anything that may be of value as evidence in a case may, in principle, be brought before a court that will decide on a case-by-case basis how much value to put on each piece of evidence. According to the conclusions of the evaluation, this may be considered as a good practice.

- When on the contrary the rules on the admissibility of evidence are rather strict, this can create obstacles for electronic evidence, notably when obtained from another country, e.g. through MLA requests.

- The police may access data stored at the location of the search, as well as remote data or data located abroad, in compliance with international agreements. If the clarification of facts relevant for criminal proceedings requires the preservation of stored computer data to be entered into criminal files, including operational data saved through the computer system, or on any data carrier, (e.g. CD, DVD carriers, mobile phones), objects in question are usually seized pursuant to relevant Criminal Procedure rules of the Member States.

- If an electronic evidence is on the Internet, or it is owned by the providers of electronic services, cooperation with information society service providers or providers of electronic communications services is essential to provide the necessary data and to take measures aimed at preventing the destruction or modification of data.

- The borderless nature of cyberspace gives rise to special challenges for Law Enforcement and judicial authorities. Electronic evidence, which nowadays is crucial to investigations and for judicial authorities, can be stored, changed and deleted in seconds from anywhere in the world.

- Consequently electronic evidence may also be moved, deleted and controlled or fragmented in several jurisdictions globally within seconds. However, in not all Member States it is possible to have direct access to e-evidence located in other country or in the cloud and MLA procedures should be followed.

- According to the conclusions of the evaluation, in order to tackle these problems, the current procedures for mutual legal assistance (MLA) need to be faster and more effective and the authorities investigating must very speedily be able to send requests to many different countries.

- In certain Member States the national legislation allows obtaining subscriber information directly from foreign providers, subject to being also allowed by the law of the State of the provider's seat. In one Member State some practitioners expressed a wish for a harmonised mechanism for exchanging subscriber data and new approaches at EU level on establishing jurisdiction.

- Practices and forms for making available the e-evidence secured in the investigation as a part of the case file in a format that allows scrutiny by the prosecutors and judges, vary in the Member States.

- Seizure of computer hardware containing e-evidence seems not to be the preferable option as it may be cumbersome for a victim of cybercrime to accept the loss of his or her digital equipment seized for the duration of the investigation.

- Alternatively, in order to secure digital material, stored data may be copied (mirrored) on to another storage medium (e.g. DVD, hard disk) and made available in this form and/or, in particular readable data, (e.g. text messages) or image files may be printed out and made available in paper form as well.

- Usually the same procedure is used for electronic evidence procured abroad. However, if special conditions are set by the country that helped acquiring the evidence, the police and prosecutors will have respect those conditions.

- When the prosecutor and judges who have to handle e-evidence in court proceedings receive it in a form that can be accessed and evaluated only using IT equipment, and specific knowledge is therefore requested, including for analysing the authenticity of the electronic evidence, a forensic expert can be asked for advice.

- According to the findings of the evaluation, specific high-tech hardware and software for the better identification and extraction of e-evidence would enable the Member States' authorities to work and cooperate with comparable e-evidence.

RECOMMENDATIONS

- ***Member States should dispose of adequate high-tech hardware and software for the identification and extraction of e-evidence enabling the Member States' authorities to work and cooperate with comparable e-evidence.***

- ***Member States should ensure that their national procedural legislation is flexible enough to facilitate the admissibility of e-evidence, including when obtained from another country, e.g. through MLA requests.***

- ***Member States should consider engaging in, and maintaining, a constant dialogue with the private sector and discuss methodologies to ensure that the gathering of e-evidence takes place in a way to allow its admissibility in courts.***

XIII - 'CLOUD' COMPUTING

KEY FINDINGS AND CONCLUSIONS

- Cybercrime committed in the "cloud" was highlighted by a significant number of Member States as an area raising problematic issues for investigation and prosecution.

- Some Member States, at the time of the evaluation, had no experience of investigation of cybercrime of this type and consequently the issue of jurisdiction in terms of "cloud storage" had not yet been challenged before their national courts, which could mean that a number of cybercrimes remains in practice unknown; it was however acknowledged that they would inevitably have to face such situations.

- This phenomenon may lead to serious problems in the future, as "cloud" solutions are becoming more and more popular and the use of "cloud-based" storage and services is increasingly becoming a common practice not only for legal entities and natural persons, but also for offenders who wish to hide the storage of illegal content; in particular, offenders who sexually abuse children via the Internet are increasingly 'hidden', as they are making greater use of on-line 'cloud storage".

- Because of the technologies used, and because of the storage capacity in servers and economies of scale, data move around the globe constantly and may be fragmented in pieces to be put together only upon retrieval. A specific problem when dealing with offences relating to the "cloud" is therefore to retrieve the actual physical location where the offence is actually committed, which may be difficult to establish, very complicated and lengthy.

- Therefore, information and the computers that process it in the "cloud", which can store data important for the investigation of criminal offences, are not easily located and accessed by the Law Enforcement Authorities.

- The lack of information can make it harder to identify the perpetrator, the time of the offence, the location of the offence and the instrument the offence was committed with, and this results in cases where cybercrime may go unpunished, and situations in which people will be victimised over and over again.

- Also "cloud" storage providers may have troubles in locating the actual (territorial) location of data; even the owners of data often do not know where it is located.

- Crimes committed "in the cloud" can often be pinpointed both to where the perpetrator was when he or she committed the crime and to where the effect occurred. Depending on the type of cybercrime, the effect may be pinpointed to several Member States' jurisdiction or also outside other EU Member States' jurisdiction.

- Consequently, the method of "cloud computing" creates problems not only with regard to national law, but also to international legislation, which is based on the acknowledgement of States' independence and on the principle of territoriality.

- Even if the location has been established, domestic legislation in some Member States does not allow for extra-territorial jurisdiction, or cybercrime offences committed in the 'cloud' may be prosecuted only if such data is accessible from the Member States concerned.

- Conflicts of jurisdiction as regards the competence to issue an order to obtain respective electronic evidence can arise when two or more Member States can establish jurisdiction over the crime; in these cases, Member States can make use of Eurojust services and of Joint Investigation Teams to overcome such conflicts.

- There are two main possibilities for obtaining data stored in the "cloud": either direct access to the content of such profiles and storage facilities is obtained by way of the consent of the user/owner of the profile or account, or the location of the information has to be identified and MLA procedures which are lengthy and inefficient should be used.

- The further option to order directly providers to supply certain data, often turns out to be very difficult in practice as there are providers who do not cooperate with the foreign police forces and do not answer every request.

- With a view to overcoming these difficulties, the evaluation highlighted that special arrangements with the most important "cloud" providers (e.g. Google, Yahoo, etc.) could be put in place to reduce delays and to obtain information in formats admissible in courts.

- The Council of Europe has concluded conventional law agreements relating to such matters (including with third States, such as the United States of America, Canada, Australia, and Japan). However, pursuant to the Convention on Cybercrime, cross-border action is only possible in a very limited number of cases, i.e. with the lawful consent of the person who has the lawful authority to disclose the data, in a case where the jurisdiction is known. In cases where the location of data is not known, these provisions are inadequate.

- In the light of the above, it has not been possible yet to solve the problem of "cloud" storage adequately. The various possibilities provided by international law for acting independently or in mutual cooperation (legal assistance), have proven limited for investigations of Cybercrime committed via the "cloud".

- According to the conclusions of the evaluation, these situations should be envisaged and consideration should be given as to how to improve the practice with a view to ensuring effective investigation and prosecution while also avoiding positive conflicts of jurisdiction.

- For this purpose, it could be useful to consider addressing the existing relevant legal frameworks in place and/or investigative issues in order to have clear rules and procedures in relation to cybercrime committed in the "cloud".

- Member States' participation as observers in international fora e.g. Cybercrime Convention Committee (T-CY) in which solutions to these issues are discussed has also been highlighted as useful in the context of the evaluation.

- One Member State put forward suggestions to access data held in the cloud such as providing the possibility to make virtual searches in data centres located in other countries without having to first identify the physical location of the server and/or to mandate the data service providers to provide passwords to LEAs to enable them to access the data.

RECOMMENDATIONS

- ***Member States should consider to conclude special arrangements with the most important "cloud" providers (e.g. Google, Yahoo, etc.) in order to reduce delays and to obtain information in formats admissible in courts.***

- ***Member States should, where appropriate, consider a review of their existing legal frameworks in order to have clear rules and procedures in relation to cybercrime committed in the "cloud", including allowing for extra-territorial jurisdiction for related offences.***

- ***The EU institutions should address the global challenges raised by "cloud computing" with a view to identifying solutions that could increase the capacity to detect cybercrime committed in the "cloud" and to locate and access evidence of criminal liability to be used in criminal proceedings.***

XIV - RETENTION OF ELECTRONIC COMMUNICATION DATA

KEY FINDINGS AND CONCLUSIONS

- The invalidation of the Directive 2006/24/EC (Data Retention Directive), has created a situation of legal uncertainty, in particular as regards the legal status of national transposition legislation and the availability of electronic communication data collected for access by the Law Enforcement Authorities and their use as evidence in criminal proceedings.

- Member States who no longer have an obligation deriving from a specific Union legal instrument to introduce or maintain a national data retention regime providing for the mandatory storage of electronic communication data by providers have had different approaches to the judgment, maintaining, amending, replacing or repealing of the transposing legislation or its invalidation by national courts.

- The evaluation has confirmed Member States' concerns in relation to the absence of a common legal framework on data retention at Union's level and the consequent fragmentation of the data retention regimes throughout the Union, which raises significant challenges within the Union and in the international cooperation with third States.

- Several Member States have underlined the negative consequences of the above mentioned judgement on the effectiveness of criminal investigations and prosecutions at national level, in particular in terms of reliability and admissibility of evidence to the courts based on the collection of electronic communication data, as well as on cross-border judicial cooperation between Member States and internationally (limited capacity to provide obtain evidence).

- The non-preservation of some data or in their retention only for a limited short period of time, makes difficult or even impossible to secure e-evidence in the EU Member States through the application of the standard procedures.

- It was in particular stressed that this development has had a serious negative impact on the ability of the competent national authorities to investigate and prosecute efficiently cybercrime and other crime where e-evidence and Internet or telecommunications data would greatly contribute to the successful identification of the perpetrators.

- Several Member States emphasised that there would be an added value in having a common approach at EU level, including the possibility of a new a legislative framework that could harmonise data retention conditions and periods in the Member States.

- In the meantime, in its judgment in the two Joined Cases C-203/15 and C-698/15 of 21 December 2016 on "Tele 2 and Watson", the Court stated that national legislation which imposes the general and indiscriminate retention of all traffic and location data exceeds the limits of what is necessary and clarified the criteria and conditions to be fulfilled by the national data retention schemes of the Member States.

- A common reflection process involving the EU institutions and the Member States is currently ongoing to address the issue of data retention with a view to identifying legal and practical solutions to the related challenges arising from the ECJ case law.

RECOMMENDATIONS

- ***Member States and the EU institutions should pursue the common reflection with a view to identifying legal and practical solutions to address the issue of the retention of electronic communication data at national and at EU level, taking into account the principles enshrined in the recent ECJ case/law.***

XV - ACTIONS AGAINST CHILD PORNOGRAPHY AND SEXUAL ABUSE ONLINE

KEY FINDINGS AND CONCLUSIONS

- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, at the time of the evaluation had been transposed by the majority of the Member States. The current state of play regarding transposition into national measures of this Directive can be consulted using the following link : http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093
- Due to developments in society and technology, which have increased both opportunities for communication and information dissemination and the possibility of committing criminal acts on-line, sexual child abuse on the Internet (grooming, sexting, cyber bullying, etc.) has significantly increased in recent years. In order to effectively combat such forms of crime, a wide range of both preventive and coercive measures involving both the public and the private sector are implemented in the Member States.
- In some Member States a national database dedicated to victims' identification for combating the sexual abuse of children exists, or at the time of the evaluation was in the process of being established. In the majority of the Member States such national database is however missing, or at the time of the evaluation had not been sufficiently developed. In these cases, the Law Enforcement Authorities only use international databases and tools, in particular, Interpol's International Child Sexual Exploitation Database (ICSE-DB), which proves to be a powerful intelligence and investigative tool for identifying victims and perpetrators, as it allows specialized investigators to share data around the world.

- In one Member State, if the police cannot identify the victim using the database, but have reasonable suspicions about the possible identity of a child, they share one or more pictures of the victim with schools for identification, which can be considered a good practice.

- In order to avoid re-victimization, there are different approaches in the Member States: in addition to blocking and/or removal of child sexual abuse material (CSAM), other measures include: the listing of dangerous media deemed harmful for minors in an index, the limitation of the contacts with the offender, guidance and counselling provided for victims by NGOs, as well as specific measures to protect victims and witnesses of child sexual abuse against negative impacts during criminal proceedings.

- In a few Member States, there are no specific measures in place to avoid re-victimisation, but there is cooperation for this purpose with NGOs, with specialised non-police bodies and institutions with responsibilities in the area of the protection of minors or with the EMPACT sub-priority on cybercrime 'Online Child Abuse'.

- Various legal, technical, organizational and information measures are in place in the Member States to address sexual exploitation/abuse online, sexting, cyber bulling and child sex tourism. Several Member States have specialised units or dedicated officers working exclusively with child sexual abuse for the purpose of identifying children and perpetrators and conduct investigations. A good practice in one Member States is the assessment upon recruitment and the annual psychological examinations of specialised police officers working in this field.

- All Member States implemented to a various extent preventive measures aimed at promoting the safe use of the Internet by minors, often developed under the aegis of their governmental authorities and in collaboration with the specialised units and with the NGOs working with children. Some projects in this field are co- financed by the EU, like the European Safer Internet Network (INSAFE), under the European Commission's Safer Internet Programme.

- Preventive measures include i.a. training projects and information campaigns aimed at raising awareness and training target audiences (students, parents, educators and other groups) on the main potential risks that minors face when using the Internet, and to develop its responsible use. The modern techniques, involving children teaching children, used in one Member State, was considered a good practice. In some Member States, the police also organises or participates in these activities.

- Media education is also a powerful tool for the prevention of child sexual abuse, especially for children and adolescents and in some Member States information on safe online behavior for children is published in dedicated websites. Other Member States have elaborate brochures or handbooks or "school guide" to safe and efficient Internet use, cyberbulling, etc.

- The majority of the Member States has a Hotline service that can be used anonymously to report child sexual abuse content, which often also functions as a Helpline intended for children, teenagers and parents, providing them with anonymous and free assistance by telephone and online (websites or platforms), also e.g. how to file a report to the police. A European online platform - www.reportchildsextourism.eu - includes all the national alert lines in Europe.

- Most Member States have criminal provisions providing for offences and sanctions for travelling child sex offenders, or apply other measures including against advertising abuse opportunities and child sex tourism, as foreseen by Article 21 of Directive 2011/93/EU. Measures aimed at improving detection of this specific form of crime include monitoring or notification systems on travelling of sex offenders, actions involving the tourism and travel industry and the foreign service, the posting of liaisons' officers abroad, the confiscation of the passport of a convicted child abuser, etc.

- General measures for early detection of child sexual abuse on the Internet, include i.a. patrolling the Internet and undercover investigations, which proves to be an effective tool to counter real time web-based child sexual exploitation, as well as filtering tools, which however are not applied in all Member States or are often not compulsory for ISPs.

- Coercive measures in cases of sex child abuse on the Internet, which include blocking of access, removal of content, and taking down of web pages, are not applied in the same way in the Member States, including in procedural terms as regards whether or not a court order is required in advance or to confirm these measures taken by the police.

- In the majority of the Member States legal and practical measures are taken to remove permanently from the web online audio-visual child sexual abuse material (CSAM). The "deletion approach" can be considered an effective measure, as it makes possible to prevent images/videos of minors from continuing to be shown on the Internet. Other Member States use also or only the "access-blocking approach", that consists in blocking access to the web sites containing child pornography materials, by rendering such material temporarily inaccessible.

- If the material is hosted on servers located abroad, usually international channels, namely Europol, and its secure information exchange system SIENA, or Interpol and its Access Blocking initiative, are used; it is also possible for the Hotlines to report simultaneously to INHOPE, (International Association of Internet Hotlines), which ensures that child pornographic content directed to one State, but stored abroad, can be removed from the Internet.

- In a few Member States, websites with child pornographic content are blocked and made inaccessible regardless of whether the site is located within or outside the EU, which was considered as a good practice.

- For the implementation of the above coercive measures, it is essential to have good cooperation between all relevant stakeholders, name the Law Enforcement Authorities, the hotlines, NGOs and Internet service providers (ISPs). In some Member States the latter have an obligation to take appropriate action to interrupt the possibility to use such material, by blocking access or removing content from the Internet, whereas in other Member States the national legislation does not stipulate such an obligation, though the above measures may be taken in individual cases on the grounds of a judicial order.

- Cooperation in the Member States between the police and the domestic ISPs is generally good, and they often remove illegal content which is child pornography promptly and voluntarily when notified by the police, even where they are not obliged to do so. A tool used in one Member State, which uses the same interface icon for all providers with a reporting button that can be clicked to report that a given Web site contains child pornography material, was mentioned as an example of good practice.

RECOMMENDATIONS

- ***Member States who have not yet done so, should develop a national database dedicated to victims' identification for combating the sexual abuse of children.***

- ***Member States who have not yet done so, should consider developing specific measures to avoid re-victimisation, including measures to protect victims and witnesses of child sexual abuse against negative impacts during criminal proceedings.***

- ***Member States should ensure well-functioning cooperation between all relevant stakeholders, name the Law Enforcement Authorities, with a view to efficiently combat crimes targeting children on the Internet, and consider introducing an obligation for Internet service providers (ISPs) to take appropriate actions such as blocking of access, removal of content, and taking down of web page.***

XVI -MECHANISM TO RESPOND TO CYBER-ATTACKS

KEY FINDINGS AND CONCLUSIONS

- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems at the time of the evaluation had been transposed by the majority of the Member States. The current state of play regarding transposition into national measures of this Directive can be consulted using the following link : http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093.

- Cyber-attacks are an evolving threat, the methods and tools used to carry out such attacks are increasingly sophisticated, and the spectrum of cyber-attacks threatening the cyber-space is very wide. The evaluation has in particular shown that there has been a significant increase in ransomware attacks - a type of malicious software that blocks access to data until a ransom is paid - across the European Union.

- When cyber-attacks occur there is a need for a technical assessment (digital analysis of materials that are seized during the operations, like searching viruses, recovering deleted data, etc.), that in some Member States is requested to the private sector, as it has a good expertise and works with better equipment and less costs. Furthermore, there is a need for assessing the consequences of possible attacks for the infrastructures and for creating a comprehensive situational awareness and assessment of the attack, including methods and tools used.

- Appropriate countermeasures, with a view to ensuring the coordination of the emergency response and subsequent recovery of the information systems, and mitigation measures to mitigate the effects of a cyber-attacks shall be taken. In order to guarantee a proper level of cyberspace security, preventive measures (systematic cooperation and exchange of information among all public and private actors of the global, awareness-raising measures, involvement in security research, technical analyses and situation reports) are also extremely important.

- The responsibility for performing these tasks in order to guarantee the security of the global cyberspace at national level is generally shared among different actors. Consequently, in order to ensure a good level of resilience of the national cyber- security system against cyber threats, there is a need for an appropriate legal and institutional framework and for an integrated multidisciplinary mechanism; this involves a good coordination both at the strategic level and at the operational level (particularly in the critical infrastructure and public administration sectors), including the need for an appropriate crisis management system to coordinate response and recovery operations.

- In some Member States a structured multi-agency approach already exists, in certain cases based on Public-Private Partnership, whereas in other Member States such an approach has not been sufficiently developed or is missing and the coordination mechanism for reacting to cyber-attacks functions mainly on the basis of informal cooperation.

- At the time of the evaluation, the majority of the Member States had already established a national CERT, or were in the process of establishing it, whereas a few Member States had not yet done so.

- The main tasks of CERTs consist in monitoring and responding to cyber incidents, provide early warnings, alerts and risk and incidents analysis, as well as in establishing cooperation with the private sector.

- In certain Member States, national CERTs' role goes even beyond these tasks, as they manage databases on threats and incidents, support the exchange of information between various entities, provide advise and assistance for the protection of the computer systems of the public and the private sector, undertake proactive activities for diminishing the risks of incidents in computer security, carry out awareness raising and training activities, act as an intermediary between the private sector, academia and the police, and represent the national contact point for international cooperation.

- Governmental CERTs mainly manage crisis and provide response to cyber threats and incidents concerning the public sector, but in many cases also the critical infrastructures, and in limited cases also the private domain, which however is usually within the remits of other CERTs in the private sector.

- In some Member States, governmental CERT's have coordinating and supervision functions for other relevant stakeholders, which proves to be a useful practice, especially in those Member States where the response mechanism to cyber- attacks is quite complex, and/or a significant number of different CERTs both in the public and the private sector co-exist in parallel.

- CERTs do not have the powers of Law Enforcement Authorities vis-à-vis private subjects, but as regards attacks of a criminal nature (not all the IT incidents are criminal acts), have an important role in supporting the investigations, as they can help to provide information and to secure evidence. It is therefore very important for this purpose that CERTs have a good cooperation with the Law Enforcement Authorities, as obtaining attack-related information and evidence effectively is essential for the investigation of cyber-attacks, considering that electronic data are very dynamic and can be lost easily. Where necessary, other criminal intelligence entities and/or intelligence institutions may be involved in cyber-incidents investigations.

- According to Directive EU 2016/1148 (NIS Directive), to be transposed into national law by 9 May 2018, Member States should have well-functioning CSIRTs, also known as Computer Emergency Response Teams (CERTs), complying with certain requirements in order to guarantee effective capability to deal with incidents and risks and to ensure efficient cooperation at Union level.

- Digital resilience cannot be achieved by the government alone; there is an important role to play also for the private sector, in particular for operators of critical infrastructure, information systems and network operators, which are directly involved in managing the risks and safeguard the security of their networks and services.

- According to the NIS Directive, Member States shall ensure that operators of essential services protect the security of their networks and information systems and notify the competent authority or the CSIRTs without undue delay of any incident having a substantial impact on the provision of a service. Once the NIS Directive would be fully implemented, critical infrastructure entities will therefore be legally obliged to report cybercrime attacks.

- At the time of the evaluation, in some Member States there was already an obligation for the private sector to notify electronic attacks incidents to cyberspace to the Law Enforcement Authorities. In certain cases, however, this obligation was limited to certain branches of the private sector or to certain types of incidents or there were no sanctions for non- compliance with the reporting obligation.

- In certain cases, though in the absence of a formal obligation, reporting occurs on a voluntary basis; however, as highlighted in some reports, underreporting is frequent due to service providers' reluctance for the damage that can result to their reputation from criminal proceedings (for more details see chapter on cooperation). As highlighted in one individual country report, in order to encourage reporting, police authorities can highlight the fact that the investigations can be secret and good results can be achieved without affecting their reputation.

- According to the findings of the evaluation, without a reporting obligation, there is a real danger that most of the cases of cyber-incidents remain outside the notice of the authorities, thus making prosecution and sanctioning for related cyber- offences dependent on interests of the private sector and not the public's.

- A mandatory reporting system, particularly for serious crimes, is important not only for law enforcement purposes, namely to facilitate a quick and complete situation assessment and faster implementation of targeted countermeasures, but is also useful to provide the authorities with a better overview of the threats, to compile comprehensive statistics on the number of cyber-security incidents, and to take the right precautionary measures. Therefore, establishing a more binding legal framework to govern companies' reporting of cyber-attacks, e.g. by making such reporting mandatory, as in some Member States, has been considered by the evaluators a good practice.

- In order to ensure a high level of cyber security, security-conscious behaviour among leaders, system developers and users, safety improvements are needed, and therefore raising awareness at all levels, as done in certain Member States, is an important component of an effective approach to cyber-security.

- As sometimes cyber threats and attacks have a cross-border dimension, EMPACT Cyber-attacks proves to be a useful platform to improve cooperation between Member States, relevant institutions and agencies and partners from the private sector for the production and dissemination of antimalware and defence against network attacks on infrastructure.

- It is worth mentioning the close cooperation between the CERTs of the three Baltic States, which in November 2015, signed a memorandum of understanding, pledging to step up cooperation on cyber-security and the protection of IT systems and networks.

- When dealing with cyber- attacks outside the Union, the formal channels for mutual legal assistance are used. However, as time in cyber-related crimes can be of crucial importance (because of the data volatility), direct cooperation and information exchange between police forces directly or via Europol and Interpol , are also used for faster and more efficient cooperation. Some Member States also use the G7-24/7 network of contact points.

- The Digital agenda for Europe incentivises Member States to establish by 2012 a well-functioning network of CERTs at national level covering all of Europe. The European Commission invited Member States to strengthen cooperation between the existing National CERTs and to expand existing cooperation mechanisms like the European Governmental CERTs Group.

- There is communication and cooperation also at international level through the CERT networks that have been formed worldwide, such as the International Watch and Warning Network (IWWN), FIRST, the European Government Cert network, and TF-CSIRT with the aim of cooperating on cyber incidents, including mutual support for the management of IT situations and IT crisis management, since they carry out regular exercises. CERT networks may have partly similar focuses, e.g. government/authorities' CERTs, and partly different, e.g. with teams from business, science and the authorities.

RECOMMENDATIONS

- ***In order to guarantee an appropriate level of protection and security of national cyberspace, Member States should ensure an efficient institutional framework, based on multi-agency approach, and involving well -functioning cooperation between all relevant stakeholders involved in cyber-security, including the private sector.***

- ***In line with the NIS Directive, Member States who have not yet done so, should establish a national CERT. In order to ensure a high level of cyber security, Member States should consider vesting governmental CERTs with functions allowing them to act as central points of coordination of other CERTs and stakeholders involved in the prevention of cyber threats and in the response to cyber-security incidents.***

- ***For this purpose, Member States should also consider tasking governmental CERTs with the collection and analysis of cyber incidents, develop their ability to respond to threats and early-warning software systems and provide dedicated training on cybercrime and cybersecurity.***

- ***In line with the NIS Directive, Member States who have not yet done so should introduce into their national law the obligation for the entire private sector to report without delay cyber-attack incidents having a significant impact on the continuity of essential services to the LEAs.***

- ***Member States are encouraged to participate in the EMPACT Cyber-attacks platform as well as in European and worldwide networks of CERTs.***

XVII - COOPERATION WITH EU AGENCIES

KEY FINDINGS AND CONCLUSIONS

- Since cybercrime, other cyber-related crimes and their investigation frequently involve more Member States, cooperation and sharing of information with EU Agencies is a priority.

- Europol/EC3, Eurojust, the EJN and ENISA play a vital role with a wide-ranging activities, which include producing analyses of cybercrime trends, coordination of investigations, mutual exchange of information and intelligence, data analysis and training on a EU-wide basis. Their expertise and facilities enable mutual cooperation between Member States and their respective LEAs and prosecutorial services.

- Eurojust plays a crucial role in the coordination of criminal investigations and in offering judicial assistance regarding cross-border cooperation between Member States, which proves particularly useful in complex cases of cyber-related offences. It also contributes to facilitating and accelerating cooperation with the competent authorities of Member States and third States in the field of cybercrime.

- Eurojust also collects and disseminates case studies and best practices, provides training activities in the field of cybercrime and promotes exchanges of experiences between specialised judges in the field of cybercrime.

- Europol facilitates the cooperation and exchange of information among Member States, distributes operational products and services to investigation services, provides forensic and operational training and awareness-raising material. EC3 functions as a European service specialised in the fight against cybercrime, carries out analysis of the phenomenon of cybercrime as a whole, coordinates the activities of all those involved, and is proving very useful to investigations being carried out in several countries at once. Europol disposes of several tools to allow the exchange of knowledge and intelligence in this field between LEAs of Member States and with Europol, such as the EMPACT initiative on cybercrime, the SIENA system and J-CAT. Operational experience shows that any well-designed efforts to fight cybercrime should include a J-CAT liaison officers of the Member States with the necessary specialist knowledge.

- There is general appreciation among the Member States for the support and coordination provided by Europol/EC3, Eurojust, and the EJN with the assistance of its contact points, and consider their role essential for increasing mutual trust between investigating authorities and prosecutors and for facilitating international cooperation also with third States.

- ENISA's role in collecting cyber-alerts and transmitting them by automated systems is also crucial with a view to strengthening the technical security of information systems.

- However, not always the powers and the services of Eurojust, Europol, the EJN and ENISA with regard to cybercrime are entirely known and their products and services are not used by relevant practitioners in the Member States at their full potential.

RECOMMENDATIONS

- ***Member States should make the best possible use of the services offered by Eurojust , the EJN and Europol with regard to cybercrime, and provide close cooperation between their national CERTs and ENISA.***

- ***Eurojust, Europol and ENISA should consider raising awareness of their services and the existing possibilities for cooperation and specialised training that they offer in the area of cybercrime and actively supporting events that strengthen international cooperation with regard to combating cybercrime.***

- ***Europol should also capitalise on the deployment of the SIENA system in the investigation services, heighten the visibility of EMPACT projects, explore best use of J-CAT, consider proposing to Member States a standard approach on structural elements for criminal intelligence databases in cybercrime, and facilitate the adoption of a common taxonomy on cybercrime.***

- ***ENISA should explore how to standardise the concept of cyber-alerts collected and transmitted by automated systems, which would allow the statistics on these alerts to be comparable and harmonised throughout Member States.***

XVIII - JOINT INVESTIGATION TEAMS (JITs)

KEY FINDINGS AND CONCLUSIONS

- Due to the often cross-border dimension of cybercrime, the participation in internationally coordinated investigations can be of benefit in effectively prosecuting cyber related offences.

- Within the EU framework, the Joint investigations Teams (JITs) are a tool of international cooperation in transnational crime cases, based on an agreement between competent authorities of two or more Member States - both judicial and law enforcement - in order to carry out jointly criminal investigations.

- At the time of the evaluation, several Member States had participated in JITs regarding cybercrime cases, some of which more frequently than others, whereas other Member States had never done so.

- Participation in JITs is generally indicated as a positive experience by the participating Member States, who consider JITs as an effective instrument for conducting cross-border investigations, enabling direct exchange of information between investigators and timely cross-collection of evidence without having to submit separate formal requests for mutual legal assistance (MLA).

- Due to the lengthy procedures for MLA, the use of JITs contributes to the shortening of the time for the investigations and also contributes to enhancing trust among national authorities.

- Although the participation of Europol and Eurojust in the setting up and operation of JITs is not mandatory, as indicated by some Member States, the two organizations can play an important role in ensuring the efficiency and operational capacity of JITs. The possibility for JITs to be financed by Eurojust and Europol is considered by some Member States to be crucial.

RECOMMENDATIONS

- ***Member States are encouraged to use JITs more often in cybercrime regarding cross-border cases in order to make investigations more effective and for this purpose to raise awareness of practitioners about the possibilities and advantages of JITs.***

- ***The European institutions, in particular Eurojust and Europol, should continue to support and facilitate the setting up of JITs and make available adequate funding to help Member States to use JITs more frequently.***

XIX - MUTUAL LEGAL ASSISTANCE

KEY FINDINGS AND CONCLUSIONS

- Cyber-criminality being frequently of a transnational character, as often cyber-related or cyber-enabled offences are committed by foreign nationals or involve the use of foreign IT infrastructure, smooth and well-functioning international cooperation is crucial for tackling cybercrime efficiently.

- Mutual Legal Assistance (MLA) from a foreign State can be necessary at all stages of the proceedings and for all investigative or procedural measures, depending on the type of cyber offence that constitutes the illegal conduct.

- Among the most frequent MLA requests in this field from and to the Member States, as outlined in many individual reports, there are internet-related crimes, like computer-related fraud and forgery, attacks to computer, as well as credit-card offences; therefore, many of the MLA requests with respect to cybercrime refer to obtaining specific evidential material held by service providers (the tracing of telecommunications and identification of IP users), to the search and seizure of computer systems as well as to obtaining bank information.

- In all the Member States, the national legislation does not contain any specific provision regarding MLA in connection with cybercrime, and consequently general procedures and conditions for MLA requests are applicable to cybercrime cases.

- Mutual legal assistance, including in the area of cybercrime, may be provided on the basis of multilateral treaties, bilateral agreements or reciprocity. The national authorities responsible for receiving or sending MLA requests vary depending on the applicable international instrument.

- The majority of the EU Member States are parties to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 (MLA Convention), concluded in accordance with Article 34 of the Treaty on European Union, and to its 2001 Additional Protocol. The majority of the EU Member States also participate in and apply the Schengen acquis, that makes related provisions on judicial cooperation in the Schengen Convention also applicable, which is relevant in particular for Member States which are not party to the MLA Convention.

- These instruments enable direct communication between the judicial authorities (courts and prosecution offices) of the Member States regardless of the stage at which the request is issued (investigation, prosecution, trial or execution); therefore, MLA requests are sent directly from the competent judicial authorities of the issuing Member State to the competent judicial authorities of the executing Member State, who is competent for making decisions on the requests.

- Between Member States who do not apply the above instruments or in case of requests for assistance to and from third States, depending on the provisions of the applicable bilateral or multilateral agreements, MLA requests are transmitted directly (between competent or central national judicial authorities) or through the diplomatic channel (through the Ministry of Foreign Affairs).

- When the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and its Additional Protocols of 1978 and 2001, are applicable, letters rogatory are to be addressed by the Ministry of Justice of the requesting State to the Ministry of Justice of the requested State and shall be returned through the same channels. However, during investigations, or in cases of urgency, a request may be directly forwarded by the national judicial authority of the requesting Member State (active MLA) to the national judicial authority of the executing Member State (passive MLA).

- Judicial requests for mutual legal assistance are generally preceded by requests for expedited preservation of digital evidence stored computer data provided for by Article 29 of the Budapest Convention on Cybercrime of 22 November 2001.

- With regard to States which are neither party to the abovementioned multilateral conventions, nor of relevant bilateral conventions, mutual legal assistance can take place on the basis of the principle of reciprocity.

- The average timeframe for answering an MLA request is usually of some months but varies depending on whether the MLA is provided on the basis of an international agreement or of reciprocity; in the latter case, the response time is even longer because it is necessary first to receive/grant an assurance of reciprocity.

- In the fast-moving area of cybercrime, the lengthy of MLA proceedings makes MLA formal channels rather ineffective, with a negative consequence for the conduct and success of the investigations, as digital evidence is volatile and must be handled rapidly and efficiently, as delays can result in data being lost. There is consequently a general need to speed up the handling of MLA requests in cybercrime investigations. The improvement of the quality of MLA requests may significantly affect the acceleration of their execution in other countries.

- As an alternative to the formal MLA channels, some Member States use Europol, Eurojust and EJN channels, such as J-CAT at EC3, or Interpol, G7 network of contact points, networks of liaisons' officers or bilateral contacts, to obtain faster responses; however, it has to be considered that the validity of the data would have to be verified if these less formal channels are used.

- The support provided by Eurojust in facilitating communication and in accelerating the execution of urgent requests not only to or from EU Member States, but also with third countries, is considered by several Member States very useful, considering also the physical presence of liaison public prosecutors from the USA, Norway, and Switzerland at Eurojust.

- As regards non-EU countries, mutual legal assistance in criminal matters involving cybercrime is primarily requested to and sought from the United States, with whom a smooth cooperation is a key factor, as many popular Internet Service Providers are situated in its jurisdiction.

- However, many Member States encounter obstacles in this respect, especially in the field of data retention and the disclosure of the IP addresses of Facebook and other social networks' accounts holders. As stated by the evaluators in some individual reports, the issue of database accessibility of the Internet social networks originating in the US is a constant problem that affects all Member States.

- The United States generally attaches strong formal and content-related requirements to such requests, particularly as regards the link between the criminal offence and the specific element of proof that is the subject of the request for transmission.

- According to the findings of the evaluation, it would be useful to work on an international solutions to improve MLA procedures with third States such as, as in one Member State, using a form for requests of expedited production order agreed upon by executing authorities in a given state, that may be considered as a best practice.

- Pursuant to the relevant US law on searching for a location or obtaining email data and any content from a communication stored with an ISP, a court order known as a 'search warrant' is required. The amount of proof required to obtain a search warrant is known as 'probable cause'. This means that, in relation to a MLA request for obtaining disclosure of stored communication content from an ISP, the US authorities will require supplementary information. This procedure is very time-consuming, and in many cases does not lead to the execution of the request.

- Often MLA requests sent to the US have not been executed even though in certain cases the importance of the case was underlined and the need for the evidence being sought was emphasised in the requests.

- As regards some Member States, the development of informal and personal contacts with the competent authorities of third States prior to the sending of a MLA request has proven to be useful with a view to ensuring a better and faster cooperation in the execution of such requests.

- The establishment of a MLA registration system and a MLA management system making it possible to follow a case from registration to the answer being sent to the requesting country may be considered as a good practice.

RECOMMENDATIONS

- ***Member States should improve the quality of the MLA requests they send to other countries, in particular to ensure they are sufficiently completed and examine methods of speeding up and enhancing the quality of responses to MLA requests.***

- ***Member States are recommended to strengthen the effectiveness of the communication process with other Member States and third countries by establishing a MLA registration system and a MLA management system making it possible to follow a case from registration to the answer being sent to the requesting country.***

- ***Member States are encouraged to make more frequent use of Eurojust, EJN and Europol tools and to develop informal contacts with the competent foreign authorities in order to obtain faster responses to MLA requests from third countries.***

- ***The EU should consider coordinating efforts to establish an effective way of communicating and executing MLA requests from its Member States to non-EU countries, or establishing a framework for direct cooperation with relevant non-EU ISPs***.

- ***The EU should work on solutions to improve and speed up the communication process between Member States and third countries, in particular the United States, specifically with regard to the exchange of operational information and to MLA requests and their execution.***

XX - TRAINING

KEY FINDINGS AND CONCLUSIONS

- Taking into account the rapid technological progress and the evolving nature of cybercrime, and consequently the need to adjust to new trends and more sophisticated modus operandi, specialised, regular and continuous training on cybercrime and cyber-security for practitioners at all levels, including at the beginning of their careers, is of crucial importance for the purpose of successful investigations and prosecutions of cyber-related and cyber-enabled offences.

- In most Member States significant efforts, means and people are invested in specialised training in the area of cybercrime for the Law Enforcement Authorities, whereas not all Member States have the same level of training for the judiciary and courses for magistrates in some Member States are not mandatory.

- Nevertheless, given the technical specificities of cybercrime in the context of the investigations and taking into account that perpetrators of cybercrime should end up in a court, a high degree of understanding from the judges presiding over the cases is also required, and specialised training including as regards how to collect, analyse and use electronic evidence, is therefore fundamental for prosecutors and judges dealing with cybercrime.

- In some Member States in addition to the training provided by public bodies (police or judicial academias or institutes, etc.), cybercrime-related training is also provided by external entities such as universities and private companies operating in the sector, whose expertise proves very useful for a good quality training or also ONG. Some Member States have established highly specialised centres of excellence to provide training on cybercrime to the public and the private sector.

- In some Member States training is also provided in the form of distance learning sessions, of e-learning or also of podcasts that can be considered as a good practice and an effective training method.

- In addition to training provided at national level, also relevant EU bodies - EC3/Europol, ECTEG *(European Cybercrime Training and Education Group)*, Eurojust, OLAF, CEPOL and ENISA - provide specialised training in the area of cybercrime; however, this possibility is generally not used by Member States at its full potential.

- Some Member States have a specific budget allocated to cybercrime training. In some Member States further efforts should be made to improve specialized cybercrime training for all categories of officials involved in cybercrime cases.

- According to the findings of the evaluation, an integrated approach for common training of judges, prosecutors and representatives of LEAs can help to spread knowledge of cybercrime and function as a platform for the exchange of experiences and best practices with regard to cybercrime and for discussing obstacles relating to admissibility of evidence. However, the mutual evaluation showed that just a few Member States already provide this type of joint training.

RECOMMENDATIONS

- ***Member States should ensure a comprehensive programme of training covering the whole life-cycle of cybercrime cases for all stakeholders and practitioners involved in combating cybercrime, and in particular more regular training for the judiciary, and consider setting up a dedicated budget for cybercrime training.***

- ***Member States should consider organising joint cybercrime training for police officers, prosecutors and judges as well as the use of the e-learning approach.***

- ***Member States should make best use of the training opportunities both provided by EU bodies such as EC3/Europol, ECTEG, Eurojust, OLAF, CEPOL and ENISA and those offered by academic institutions and private companies, and consider the establishment of highly specialized centres of excellence to provide specialized training on cybercrime.***

- ***The EU institutions should increase the EU funding to help Member States to organize more specialised training for national practitioners on cybercrime.***