Council of the European Union

Brussels, 4 November 2016
(OR. en)

13982/16

EUROJUST 136
CYBER 123
COPEN 317
JAIEX 87
ENFOPOL 393
COSI 179

NOTE

From:	EUROJUST
To:	Delegations
Subject:	Strategic Seminar "Keys to Cyberspace" Eurojust, The Hague, 2 June 2016 Outcome Report

Delegations will find in Annex the Outcome Report of the Strategic Seminar "Keys to Cyberspace" held at Eurojust on 2 June 2016.

STRATEGIC SEMINAR "KEYS TO CYBERSPACE"

EUROJUST, THE HAGUE

2 JUNE 2016

OUTCOME REPORT

1. Introduction

The *Strategic Seminar "Keys to Cybercrime"* was held on 2 June in The Hague. The Seminar was jointly organised by the Netherlands Presidency of the EU and Eurojust.

This Outcome Report presents the summary of the main topics discussed by the participants in the Strategic Seminar, consisting mainly of national judicial authorities specialised in cybercrime, representatives from the European Commission and Council, the Council of Europe, Europol and the Eurojust Task Force on Cybercrime.

The Seminar also gave the opportunity to inform participants of the Netherlands Presidency's initiatives in the field of cybercrime, in particular the Council Conclusions setting up the European Judicial Cybercrime Network supported by Eurojust.

The main conclusions of the Seminar were presented the day after at the 11th Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union.

2. Session I: Jurisdiction in cyberspace in relation to the Cloud

Discussion on this topic was preceded by presentations of a German and a Dutch case on challenges in establishing jurisdiction in the Cloud. A representative of the Netherlands Presidency of the EU also reported on the outcome of the Amsterdam Conference of 7-8 March 2016 where this issue was also discussed.

Participants discussed the meaning and implications for investigating and prosecuting authorities of "Cloud computing". It was noted that, essentially, "Cloud" means loss of location: this has negative implications *in primis* because data is stored in different countries, data is also in permanent migration process, parts of data may be located in different countries at the same time.

The main challenge underlying investigations and prosecutions in the Cloud resides in the facts that legislation is not clear on this point, and most of all when available it refers to the traditional concept of territory of a country. Reference was made to the Council of Europe Convention on Cybercrime (the "Budapest Convention"), and in particular Articles 19 and 32 which are based on the assumption that the physical location of data is known. All participants convened that legislation is still too much linked to a "physical" concept of territory, which seems to become more and more obsolete in particular when investigating in the Cloud. Many advocated the need to change laws governing the assertion of jurisdiction in this respect, to make them more territory-neutral or in any event to evolve from the territoriality principle to identify and exercise jurisdiction and/or competence.

Some referred to national case law, where for instances searches can be authorised by a judge in those cases where the location is unknown and cannot be known based on reasonable efforts on the part of the investigating and prosecuting authorities. The question remains, however, how much effort can be recognised as "reasonable" before one can stop trying to identify a link with a territory. It was also indicated that in some Member States the legal framework has been recently amended to specifically allow adjudicating authorities to issue a court order authorising law enforcement to investigate in the country where access to a device is known. In these cases, accessibility of information seems to be the criterion used to initiate an investigation in cases where it is not possible to know where the data is stored.

Some participants also referred to the opportunity to amend Article 32 of the Budapest Convention so as to remove the requirement of voluntary consent of the suspect to access data. However, it was also said that a more "worldwide" solution should be found, as amending the said Article would assist only investigations and prosecutions carried out in the States parties to the Convention. Reference was also made to the possibility to amend Article 18 of the same Convention to facilitate national enforcement of a production order towards companies with a headquarter in a third State but providing services in a given Member State. Additionally, it was also suggested to consider adding a Protocol to the Budapest Convention elaborating on criteria to establish jurisdiction, including the location of the data controller. Some also suggested that the EU legislator should look into the possibility to proceed towards a "mutual recognition" of court orders issued towards service providers in a given State, that could be served to branches of that service providers located in other States, depending on where the data is stored.

Some participants also flagged the need to have a clear understanding at least at EU level of reactions from service providers whenever a request for data from national authorities is served. This would be needed to facilitate investigations and prosecutions, as many times the same providers provide different replies to analogous questions, including that the provider is not aware of where the data sought is stored. Others suggested that service providers should be obliged by law to provide information without having the possibility to rely on the fact that data might be stored in different locations. Another possibility discussed was to oblige these providers having business interests in the EU to store information within EU.

Overall, many also convened that a circle of trust should be established among investigating and prosecuting authorities as a principle to start investigations and prosecutions or to continue them, especially when exerting jurisdiction becomes challenging and time consuming. As an example, it was mentioned that it should not be an issue to allow a colleague from a Member State X to gather evidence in the territory of Member State Y without adopting a formalistic approach. This however should always be done after careful consideration about all possible implications to human rights and in any event if full respect of the Charter of Fundamental Rights of the European Union.

In terms of strategy of the investigation, it was also observed that consideration should be given to all factors possibly pointing to links to other (Member) States (e.g. nationality of victims or suspects, headquarters of service providers, where providers have economic interests, type of data requested and its possible location) before starting an investigation. Some participants also stressed that if there are reasons to believe that a search would implicate links to other States it has proved useful to first informally discuss with authorities of that State how to better proceed. The involvement of Eurojust and Europol in this and other circumstances revolving around cooperation among authorities if different (Member) States are involved was also suggested.

Lastly, participants convened that relevant national case law touching upon this and other challenges practitioners face in the investigations and prosecutions of cybercrime cases should be shared among the members of the European Judicial Cybercrime Network.

3. Session II: Cooperation with Service Providers located in the USA

Following presentations from Eurojust and USA authorities, participants discussed cooperation with service providers located in third States, in particular the USA. Many convened that direct cooperation with service providers varies greatly within the EU. Some practitioners defined it as "dark", some others described as good, others indicated that it depends very much on whether the service provider is located in the Member State of the authority carrying the investigation: when this is the case, cooperation seems to be usually productive.

Many participants noted that in fact it seems that service providers have a large marge de manoeuvre when it comes to execute requests from law enforcement or even judicial authorities aiming at obtaining data. Some participants also discussed why these companies set up compliance teams assessing requests for data from national authorities as there appear to be no apparent business reason. In any event, such marge de manoeuvre seems to greatly affect investigating authorities when examining all the criteria to exert jurisdiction.

Nearly all participants called for the intervention of the EU legislator: these companies are present in the territory of the Member States and certain obligations should be imposed on them for this same fact. Discussion should be held at EU level to ascertain whether some kind of cooperation obligation should and could be imposed on these companies, including requiring them to answer direct requests from national authorities. If so, the EU legislator should aim at harmonising at least minimum requirements and standards for such requests.

The basic consideration made was that if these companies are entitled to access a market in a Member State, they should also comply with certain standards including those regulating cooperation with law enforcement: information should be accessible to law enforcement agencies when needed for legitimate purposes. As an example, reference was made to the regime applicable to financial branches of certain service providers that are subject to certain obligations provided for in the Member States they are located in.

In terms of tools that could improve cooperation with service providers, the general permission letters that some Member States use and that are released by the USA Department of Justice are seen as useful. However, some participants also pointed out that in order to use the information so gathered in court, a formal MLA request would still be needed.

Some Member States adopted a more “pragmatic” approach, by establishing frequent contacts including via regular meetings between the Prosecution Service and representatives from relevant service providers, particularly when technical aspects are at stake.

Liaison officers and magistrates in third States where the headquarters of these companies are located can also be extremely useful to draft complete and correct requests to service providers. It was also noted that prosecutors with an expertise on cybercrime and in particular on technical matters are also extremely useful to define better the type of information requested, thereby avoind rejection of the request.

Harmonisation of requests to these providers was also called for, in particular by means of a standardised form possibly electronic.

In addition, it was noted that one of the main challenges regards the lengthy MLA procedure, which should be streamlined and sped up. The role of Eurojust in speeding up MLA to third States was also emphasised.

A number of practitioners also referred to the need to draft practitioners’ guides that could raise awareness among prosecutors about how to properly address requests for data to service providers. Some Member States are already using them.

In general, practitioners seemed to agree on the need to improve awareness and knowledge on how to properly draft a request to service providers also in view to avoid lengthy processes if re-drafting is needed. The fact that service providers have different requirements and apply different evaluation standards to requests is also considered a challenge. Specialised points of contacts within law enforcement who are familiar with practices to be followed when requesting a particular service provider might be considered a good practice.

4. Session III: Encryption of data

Participants listened to two presentations on a USA and a Norwegian case, with focus on access to locked mobile devices and encryption of data.

Discussion focussed mainly on access to locked mobile devices and in particular on the opportunity to use a suspect's fingerprints previously collected to open a locked device in order to access data. National case law on this point was presented, pointing to different outcomes from different courts in a given State. Reactions on this practice varied and triggered a discussion on the application of the privilege against self-incrimination as interpreted by the European Court of Human Rights. Reference was made to this Court's case law on the topic, and practitioners discussed whether the EU legislator should intervene in this sense. The vast majority of the participants convened that there should not be any concern regarding the infringement of such privilege.

The possibility to compel a suspect to provide passwords was also discussed, as this is a possibility provided for in some Member States. However, participants also discussed whether this measure is really efficient considering that the penalty for not revealing the password is in many instances considerably lower than the one foreseen for the crime the suspect is accused of. In addition, consideration was also given to the fact that in some cases it may very well be that the password was forgotten. The possibility that many passwords might be used for different sets of data was also referred to.

Reference was also made to the production order as provided for in Article 18 of the Budapest Convention, in the sense that it could be used to order a non-suspect to provide information. Still, the result could be that information is given but encrypted which would make it in practice useless.

Participants overall agreed on the need to protect privacy of citizens including by means of encryption, but a careful balance should be struck between this need and the need to fight against crime thereby ensuring a higher level of security of all citizens.

5. Session IV: The European Judicial Cybercrime Network

The developments regarding the establishment of the European Judicial Cybercrime Network were presented. The Netherlands prioritized this theme under their Presidency, as over the past few years, practitioners, national authorities as well as relevant players at EU level repeatedly called for a practical network of prosecutors. This network would speed up cooperation, and facilitate the exchange of expertise and best practices among cyber prosecutors and judges. Reference was also made to the need to ensure synergies with all other existing networks and bodies already established that can contribute to effectively combat cybercrime. The Council Conclusions formalising the network were prepared and submitted to the JHA Council for adoption.[1]

Eurojust will be entrusted with the support to the network. In this context, it has developed a restricted web platform where practitioners can find useful information on cyberrelated subjects, such as national and EU legislation and case law. The website allows for sharing of expertise and best practices and should serve as a tool to facilitate contacts between the experts.

Next to the website, Eurojust produced a sample of a possible future reporting tool, the *Cybercrime Judicial Monitor*, which was distributed to the participants at the meeting. This report gives an overview of legislative developments in EU countries in relation to cybercrime, and includes judicial analysis of court decisions. A topic of interest is also elaborated, selected on the basis of current trends or emerging issues.

Eurojust is also compiling brief overviews of country-specific information in so-called *country fiches.* These fiches inform practitioners about important contact information, general information about the organisation of law enforcement and judicial authorities and information about the acquisition of certain types of electronic evidence.

Practitioners attending were invited to send comments and suggestions on these products.

---

[1] Council Conclusions on the European Judicial Cybercrime Network, Doc. 10025/16 of 9 June 2016.