Council of the European Union

Brussels, 6 March 2017
(OR. en)

6890/17

LIMITE

JAI 183
CATS 17
CYBER 26
COPEN 64
ENFOPOL 97
CT 13
TELECOM 52
RELEX 201
SERVICES 3

NOTE

From:	Presidency
To:	CATS
No. prev. doc.:	14369/15; 14812/15
Subject:	Criminal justice in cyberspace - improving collaboration and coordination

1. IMPROVING COLLABORATION AND COORDINATION IN ADDRESSING THE CHALLENGES

The European Council in its Conclusions of 26-27 June 2014 [1] set prevention and combatting crime, including cybercrime, as one of the Union priorities for the next five years "while guaranteeing fundamental rights and values, including the protection of personal data". Since then, both the challenges and the policy responses continue to become increasingly complex, in particular as regards cyber-related issues.

[1] Doc. 11936/14.

The key challenges in combatting cybercrime listed by Europol and Eurojust in 2015 [2] provide a good framework for defining the different areas that need to be addressed, including from the perspective of criminal justice in cyberspace more generally: loss of data, loss of location, legal framework, public-private partnership, international cooperation and the evolving threat landscape and expertise gap.

Using these headings, the current paper briefly presents the on-going files and new elements in this area with a view to **raising awareness of the complexity** of the issues and the need to **address** them in a **multi-disciplinary and coordinated** way.

In this context, the Presidency invites delegations:

– **to use this as a basis for discussions on the appropriate coordination and collaboration at national level;**

– **to share good (national) practices of such coordination and collaboration, in particular in ensuring the right technical expertise into the policy and political processes;**

– **to discuss the requirements for a coordinated EU approach that takes due consideration of the different stakeholders involved, the varying degrees of progress and maturity of the files and the wide range of needs (law enforcement, judicial, data protection, human rights, digital single market, trade, international relations, etc.).**

2. CHALLENGES IN FIGHTING CRIME IN CYBERSPACE

a) Loss of data

In an ever more digitalised world, access to and use of data has become an essential or sometimes sole means of effectively fighting and preventing all types of crime. This must be accompanied by an increasing attention to the respect of fundamental rights, including data protection.

[2] Doc. 14812/15.

The ECJ's rulings [3] on European and national **data retention regimes** create both uncertainty about the possibilities to obtain data from private parties as well as a fragmented environment for cooperation between Member States. The Commission is working on guidelines [4] to assist Member States in constructing national legislation in conformity with the latest ruling. The negotiations on the new **draft e-privacy Regulation** [5] will have to address the current difference between the obligations put upon traditional telecommunication providers and those for "over-the-top" providers[6] (such as Skype, Whatsapp), because their services are being used interchangeably by customers and criminals.

The **Carrier-Grade Network Address Translation (CGN) Technology** [7] also contributes to the loss of data in the fight against crime because one single public IP address is shared by multiple subscribers at the same time without the service providers being able to define the exact user at an exact moment. Suggestions to address this matter will require not only sharing of technical/law enforcement expertise[8], but also cooperation with service providers (*e.g.* via the EU Internet Forum) and consultation with policy stakeholders in the digital single market in order to stimulate the IPv6 transition (where one IP address would be available for each user).

---

3 Judgement of the Court of Justice of the EU (Grand Chamber) *"Digital Rights Ireland and Seitlinger and others"* of 8 April 2014 in joined Cases C-293/12 and C-594/12; Judgement of the Court of Justice of the EU (Grand Chamber) *"Tele 2 and Watson"* of 21 December 2016 in joined Cases C-203/15 and C-698/15; doc. 5884/17.

4 Doc. 5775/17.

5 Doc. 5358/17.

6 Where audio, video and other media contents is delivered over the Internet without the involvement of multiple providers.

7 Doc. 5127/17.

8 Europol launched a law enforcement specialists on CGN network on 31 January 2017.

While it is generally confirmed that **encryption** is an essential tool in the prevention of cybercrime and the protection of fundamental rights [9], the growing use of encryption applications does pose serious problems for the effectiveness of law enforcement work and digital forensic analysis. Legislative and other measures have been taken at national level to mitigate the challenges, such as through compulsory disclosure provisions, but the existing differences lead to further fragmentation and increase the difficulties of cross-border cooperation. A reflection process [10] is on-going [11], led by the Commission and involving Member States and the relevant EU Agencies, to explore ways to improve the situation, notably the technical expertise and capabilities.

In addition, the use of decentralised **virtual currencies** hinders the possibilities of law enforcement to 'follow the money' and significantly complicates the possibilities for asset recovery and the prevention of fraudulent transactions. The lack of minimum standards for due diligence and know-your-customer for such services and the non-application of existing regulations compound to the problem.

b) Loss of location

Technological developments such as **cloud computing** and decentralised storage of data as well as the above-mentioned (criminal) use of **encryption**, anonymization tools, TOR networks, virtual currencies, Darknet have led to a situation where it may no longer (reasonably) be possible to establish the physical location of the perpetrator, the criminal infrastructure or the electronic evidence.

---

9 Informal meeting of Justice Ministers, Bratislava, July 2016; Europol & ENISA statement of 23 May 2016 (https://www.enisa.europa.eu/news/enisa-news/enisa-europol-issue-joint-statement)

10 Doc. 13993/16, as approved by Council on 8 December 2016.

11 Doc. WK 528/2017.

The "**e-evidence expert process**", set up further to the Council conclusions of June 2016 [12] and led by the Commission [13] dedicates one of its work strands to the definition of grounds for enforcing jurisdiction in cyberspace ("**connecting factors**") regardless of the physical borders, as well as to the impact of a differentiated treatment of specific categories of data. A recent expert meeting with Member States examined one concrete proposal originating from DE on direct cross-border access to data with notification. The same kind of questions are being examined in the framework of the **Council of Europe** Cloud Evidence Group, in consideration of the need of an additional Protocol to the Budapest Convention.

Meanwhile, in the context of **trade agreements**, the EU is stressing the need to avoid a type of "protectionism" that would impose unjustified data localisation requirements [14], as they could considerably harm all sectors of economy and hamper the free flow of data. The impact and interaction with data protection standards is currently being examined by the DAPIX Working Party, but the indirect influence on criminal justice work should also be considered.

Furthermore, as already mentioned in the Eurojust/ Europol joint paper [15], the loss of location may also result in **competing claims** to prosecution and underlines therefore the need for early involvement of judicial authorities, direct police-to-police channels for cooperation and communication, and **continuous innovation in the process of operational collaboration** [16].

---

12 Doc. 10007/16: Council Conclusions on improving criminal justice in cyberspace.
13 Doc. WK 518/2017.
14 Doc. WK 959/2017.
15 Doc. 14812/15.
16 One example is the Joint Cybercrime Action Taskforce (J-CAT) that is housed at Europol.

c) Legal framework

Differences in the national legal frameworks of Member States and the still quite scattered and fragmented framework at EU level prove to be an additional impediment for the efficient and successful conduct of investigations and prosecutions in cyberspace. It is obviously a serious challenge to keep pace with the rapid technological development, but some harmonisation and streamlining of these frameworks might be beneficial, especially in certain more operational aspects such as the collection and **transfer of e-evidence** or of certain investigative measures in cyberspace. This reinforces the importance of the above-mentioned expert process on e-evidence, the on-going discussions on data retention, the coherence with the work done at the Council of Europe, amongst others.

Furthermore, a number of legislative proposals have been presented by the Commission, such as the **draft e-privacy Regulation** [17] or the **draft Audiovisual Media Services Directive** [18], which also contain aspects relevant to criminal justice in cyberspace, such as the definition of different types of electronic data and of service providers and the scope of service providers' obligations.

Given the already complex setting in which any new rules must fit, the consequences of different on-going and any upcoming legislative and policy processes must be considered in order to achieve a coherent common legal framework.

d) Public-Private Partnerships

Cooperation with the private sector is vital for the successful fight against crime because it holds much of the e-evidence critical for the successful outcome of investigations but also because this sector has the tools and capacity to take down criminal infrastructures, block and remove illegal content such as terrorist propaganda, child sexual abuse materials or hate speech, report data breaches etc. It is therefore one of the work strands of the above-mentioned **e-evidence expert process**.

---

17 Doc. 5358/17.

18 Doc. 9479/16.

The **EU Internet Forum** provides a common framework for cooperation with the private sector to reduce the accessibility of terrorist content online, to support civil society in delivering effective narratives online and to tackle hate speech on-line. The **Internet Referral Unit** within Europol flags terrorist content online and supports the referral process towards the providers concerning terrorist abuse of online tools. Different kinds of public-private **partnerships** have also been developed **at national level**.

All such initiatives require, however, a suitable legal framework and clear rules of engagement so that trust between the public and private partners can be built as a basis for this effective cooperation. Currently, the situation can vary greatly depending on the private partner, Member State (authority) or provider's host country. Furthermore, **data protection** rules raise a number of issues and fear of liability may pose additional obstacles to the cooperation with the private sector.

e) International cooperation

Given the inherent international nature of cyberspace, international cooperation is crucial and inevitable for criminal justice in cyberspace, and in particular for obtaining access to e-evidence. Although the possibility exists to request and obtain certain types electronic data directly from the service provider, the main mechanism for formal cross-border cooperation and obtaining e-evidence remains the Mutual Legal Assistance (MLA) procedure both within EU and with third countries, including the US where the big service providers are predominantly based.

The above-mentioned **e-evidence expert process** dedicates another of its work strands to streamlining this mechanism as it has proven inefficient to answer the current needs. A secure online platform will be put in place for the exchange of e-evidence based on the **e-CODEX** system (developed within the **e-Justice** policy), together with some standardised forms and procedures, notably within the context of the future **European Investigation Order** (EIO). However, further work in harmonising the existing domestic procedures for obtaining electronic evidence might become necessary in order to improve the criminal justice in cyberspace even further.

Discussions on the ways to streamline the current **MLA** procedure often form part of various bilateral talks with strategic partners, especially the **US** in the context of the regular EU-US JHA Ministerial or Senior Official meetings, as well as the annual cyber dialogue.

More in general, the regular **cyber dialogues with other third countries** such as China, Japan, Brazil, organised by the EEAS, may also touch upon aspects of relevance to criminal justice.

f) Evolving threat landscape and the expertise gap

Many of the key threats remain largely unchanged [19], but new and innovative *modi operandi* combining existing approaches, exploiting new technology (CGN, blockchain) or identifying new targets (Internet of Things or artificial intelligence) appear on a continuous basis. This makes it difficult for legislators, and even more for law enforcement and judiciary, to keep the pace.

In this respect, many efforts are being made to increase the level of general cyber(security) awareness and to expand and deepen practitioners' expertise. Initiatives include the **European Judicial Cybercrime Network [20],** the recently established **European Network of Law Enforcement Specialists on CGN** [21] within Europol, the **European Cybercrime Training and Education Group,** the national centres of excellence as well as the establishment of the Council Horizontal Working Party on Cyber issues.

These are some of the examples demonstrating the recurring effort of law enforcement, judiciary, policy makers, legislators, academia and training providers to develop and pool highly needed specialised skill-sets and expertise.

---

19 iOCTA 2016.
20 Doc. 10025/16.
21 https://www.europol.europa.eu/newsroom/news/closing-online-crime-attribution-gap-european-law-enforcement-tackles-carrier-grade-nat-cgn