Council of the
European Union

Brussels, 30 November 2015
(OR. en)

14812/15

LIMITE

CYBER 119
JAI 940

REPORT

From:	Eurojust / Europol
To:	Delegations
Subject:	Common challenges in combating cybercrime

Delegations will find in Annex a joint paper by Europol and Eurojust on "Common challenges in combating cybercrime".

The Hague, 30/11/2015

Common challenges in combating cybercrime[1]

As identified by Eurojust and Europol

1. Introduction

This joint summary of common challenges in combating cybercrime has been informed by Eurojust's and Europol/EC3's case work, joint deliberations and expert input. It has been sourced from operational experiences and lessons learned, final reports of several thematic and strategic meetings with national experts and relevant stakeholders, strategic reports and assessments such as Europol/European Cybercrime Centre's (EC3) Internet Organized Crime Threat Assessment (IOCTA), as well as various open sources.[2]

[1] For the purpose of this document, the term cybercrime refers to the types of computer-facilitated and computer-enabled crimes that fall within Europol and Eurojust's mandates, such as cybercrimes causing serious harm to their victims (e.g. child sexual exploitation), cybercrimes affecting critical infrastructure and information systems in the EU, and cybercrimes committed by organized groups, particularly those generating large criminals profits (e.g. online fraud).

[2] Specifically the Cybercrime Convention Committee assessment report on the MLA provisions of the Budapest Convention of 3 December 2014, two studies conducted for the Committee on Civil Liberties, Justice and Home Affairs, titled "Cybersecurity In The European Union And Beyond: Exploring The Threats And Policy Responses" and "The Law Enforcement Challenges Of Cybercrime: Are We Really Playing Catch-Up", both from 2015, UNODC's Comprehensive Study on Cybercrime (Feb. 2013) and ITU's report on 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (Sep. 2012), amongst others.

2. Aim

This summary aims to identify and categorize the common legislative challenges in combating cybercrime, predominantly from a law enforcement and prosecution viewpoint, and informed by operational and practical experiences. In doing so, it proposes six main areas – loss of data, loss of location, legal frameworks, public private partnerships, international cooperation, and the rapidly developing threat landscape and resulting expertise gap. This summary also looks at some of the practical implications of these challenges.

This document is meant to set the scene and serve as a starting point for further discussions with relevant stakeholders about possible approaches to address the observed challenges. Given the mandates of both Eurojust and Europol, these discussions should *inter alia* include the strengthening and further alignment of legal and practical instruments concerning mutual legal assistance and the (expedited) exchange of information and e-evidence for the purpose of investigation, prosecution, protection against and prevention of cybercrime. In any case, solutions to observed challenges – be they legislative or practical in nature – should strike a fair balance between security and civil liberties, such as the right to privacy and the right to free speech.

3. List of common challenges in combating cybercrime

I. Loss of data

The overturning of the Data Retention Directive (DRD) by the European Court of Justice (ECJ) has left law enforcement and prosecutors uncertain about the possibilities to obtain data from private parties. In some Member States (MS), there is (still) legislation in place to ensure that Internet Service Providers (ISPs) retain data for law enforcement purposes, whereas in other MS, national legislation has been annulled in the wake of the ECJ judgement. In those MS, some ISPs retain some data for commercial or accounting purposes, where others have no data available to support law enforcement investigations. Such discrepancies impede the work of the cyber competent authorities and may result in loss of investigative leads and ultimately affect the ability to effectively prosecute criminal activity online. Additionally, the current situation may create an unjust pressure on the investigating authorities to prioritise their activities in accordance with the different data retention frameworks currently in place, rather than focusing on high-value targets.

A growing number of electronic service providers implement default encryption of their services. At the same time, tools that enable personal encryption of communications and other data are widely available and promoted. This means that traditional communication techniques like wiretapping are becoming less effective and the possibilities of digital forensic analysis are negatively affected. As a result, criminals are able to effectively and indefinitely hide critical evidence and activities (like live streaming of child sexual exploitation) from law enforcement. According to the IOCTA 2015, more than three-quarters of cybercrime investigations in the EU involved the use of some form of encryption to protect data.

It is noteworthy that some MS have adopted national level legislative measures such as compulsory disclosure provisions in order to mitigate the challenges, but the difference in approach and the lack of an EU-wide law is problematic and leads to further fragmentation.

In addition, the use of decentralised virtual currencies and the increased use of tumbler/mixer services[3], effectively prevent law enforcement to ‘follow the money’ and significantly complicate 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.

[3] A tumbler or a mixer is a service that attempts to break the links between the original and the final address by using several intermediary wallets. The service may also randomize transaction fees and add time delays to transactions.

II. Loss of location

Recent trends such as the increasing criminal use of encryption, anonymization tools, virtual currencies and the Darknets[4] have led to a situation where law enforcement may no longer (reasonably) establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence. In these situations, it is often unclear which country has jurisdiction and what legal framework regulates the (real time) collection of evidence or the use of special investigative powers such as monitoring of criminal activities online and various undercover measures.

Moreover, the growing use of cloud-based storage and services means that data stored in the Cloud could be physically located in different jurisdictions, which may have incompatible legal frameworks.

The loss of location may also result in competing claims to prosecution, underlining 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[5].

III. Legal framework

Despite the existence of international legislative instruments, differences in domestic legal frameworks in the MS and international instruments often prove to be a serious impediment to international criminal investigation and prosecution of cybercrime. This is partly due to an incomplete transposition of international instruments to domestic legislation.

[4] According to the IOCTA, cybercriminals, such as child sex offenders and producers, make increasing use of the Darknet and other similar areas. Darknets and other environments offering a high degree of anonymity are also increasingly hosting hidden services and marketplaces devoted to traditional types of crime, such as the drug trade, selling stolen goods, firearms, compromised credit card details, forged documents, fake IDs, and the trafficking of human beings.

[5] One example is the Joint Cybercrime Action Taskforce (J-CAT) that is housed at Europol.

The main differences regard the criminalization of conduct as well as provisions to investigate cybercrime and gather e-evidence. Adaptation and alignment of these legal frameworks is often time-consuming and difficult, due to the rapid evolution of the cybercrime threat landscape. The application of existing legislation however could at least partly be extended by expressly seeking case law with regard to new developments (e.g. virtual currencies, anonymization tools and various criminal modus operandi) and by harmonizing and streamlining existing operational processes (like the MLA process and setting standards for the collection and transfer of e-evidence). Still, the proliferation of the Internet and the growing sophistication of cybercriminal ventures require specific legislation that regulates law enforcement presence and action in an online environment (including undercover activities and the takedown of digital criminal infrastructures).

In an international context, no common legal framework exists for the *expedited sharing* of evidence (as does exist for the *preservation* of evidence). This means that in practice, even though evidence is preserved, it may take a long time before it is available for the criminal investigation or judicial proceedings in the requesting country.

IV. Public-private partnerships

Cooperation with the private sector is vital in combating cybercrime. Not only does the private sector hold much of the critical evidence of cybercrimes, but private party takedowns of criminal infrastructures, removal of illicit content and reporting of data breaches to law enforcement are among the most effective measures to stop cybercrime. However, effective and trust-based cooperation with the private sector requires a suitable legal framework, which does not currently exist in all MS. Moreover, data protection regulation and fear of liability may pose serious obstacles to cooperation with private industry.

There is also a need for standardised rules of engagement with private industry, as well as a clear understanding of the extent to which private parties can obtain evidence themselves and the legal implications of their actions.

In an international context, it is often difficult and/or time-consuming to establish which jurisdiction regulates the preservation and collection of evidence from online service providers. Some MS have a basis in legislation or case law that allows law enforcement to directly request or subpoena an online service provider outside of their territory, whereas other MS are bound to the process of MLA.

V. International cooperation

The collection of electronic evidence is often a time-sensitive issue. The current process of MLA is perceived as being too slow and cumbersome to gather and share evidence effectively. The differences in legal systems and frameworks require early coordination and involvement of judicial authorities. There is a clear need to streamline the MLA process wherever possible, for instance by aligning and using existing model requests and using a common taxonomy of cybercrime terminology. Furthermore, the various existing legal tools and mechanisms could be better promoted at international level.

There is also a clear need for a better mechanism for cross-border communication and the exchange of information for the purpose of investigation, prevention and protection, but also to ensure that any ensuing formal MLA request conforms to all the relevant legal requirements of the requested country. It this context, it is necessary to differentiate between data requests that need to follow the MLA process (e.g. content data) and requests that typically do not need to follow the MLA process.

Furthermore, the current differences in legal frameworks effectively lead to the emergence of online criminal hot spots and (virtual) safe havens, where criminal investigation and prosecution as well as evidence collection are challenging.

VI. Evolving threat landscape and the expertise gap

Cybercrime is evolving rapidly, at a scale and speed never before seen, making it difficult for law enforcement and prosecutors to keep pace. Current and expected future trends require an increasing level of expertise from practitioners. Currently no EU-wide standards for training and certification exist. Nonetheless, existing initiatives such as the European Cybercrime Training and Education Group (ECTEG) and the activities under the EMPACT policy framework are already paving the way towards addressing the expertise gap at EU level. Still, alignment of existing programmes within the MS and (further) implementation of the current EU-wide initiatives is necessary.

Moreover, in order to have justice in cyberspace, the courts must be equipped to deal with the technical and innovative particularities of cybercrime.

4. Addressing the challenges identified

While the main focus of this joint summary is to highlight practical and legal challenges in fighting cybercrime, it suggests considering a number of key principles and priorities in successfully addressing them. These fall under the following broad headings:

- Streamlining and strengthening of existing legal tools, mechanisms and initiatives
- Framework for the exchange of information for the purpose of cybercrime investigation, prosecution, prevention and protection; this should include relevant national and international stakeholders such as private industry, and to the extent possible follow a standardised approach
- Strengthening of the rule of law in cyberspace, specifically by addressing the criminal abuse of new technologies
- Training and education with a view to educating all actors involved in combatting cybercrime in law enforcement and the judiciary

It is noteworthy to highlight that the challenges presented herein are primarily based on the direct operational experiences of and deliberations by Eurojust and Europol; the topic could further benefit from more extensive but solution-oriented research and a broader comparison of existing legislation at national and international level.