Council of the
European Union

Brussels, 13 March 2017
(OR. en)

7021/17

CYBER 30
COSI 45
CATS 19
JAI 196

REPORT

From:	Eurojust / Europol
To:	Delegations
No. prev. doc.:	14812/15
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, 02/03/2017
EDOC#866212v10

Common challenges in combating cybercrime[1]
As identified by Eurojust (EJ) and Europol (EP)
Version 2.0

Introduction

This joint summary of common challenges in combating cybercrime has been informed by Eurojust's and Europol's European Cybercrime Centre's (EC3) 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's EC3's Internet Organised Crime Threat Assessment (IOCTA), as well as various open sources.[2] It should however be noted that discussion of existing challenges could further benefit from more extensive (and broader) research and a closer comparison of existing legislation at national and international levels.

This version of the document constitutes an update of the document of 19 January 2016 (EDOC #866212), taking into consideration the pertinent developments since then. Previous versions of this document are herewith replaced.

[1] For the purpose of this document, the term cybercrime is used in a broad sense and referencing Europol's and Eurojust's mandates, i.e. attacks on information systems (cyber-attacks), cyber-enabled crimes (such as non-cash payment frauds and various crimes related to child sexual exploitation online) and investigations in cyberspace, in the context of organised and serious cross-border criminality.

[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.

1. Aim

This document aims to identify and categorise the common challenges in combatting cybercrime, predominantly from a law enforcement and prosecution viewpoint, and is informed by operational and practical experiences. In doing so, it identifies 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 document also looks at some of the practical implications of these challenges.

This document is meant to set the scene and serve as input for continuing discussions with relevant stakeholders about possible approaches to address the observed challenges, informing and complementing also existing initiatives and projects. Given the mandates of both Eurojust and Europol, these discussions should *inter alia* include the strengthening and further alignment of legal frameworks 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.

Loss of data

Data retention

The overturning of the Data Retention Directive (DRD) by the European Court of Justice (CJEU) in its ruling of 8 April 2014[3] 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, ISPs retain some data for commercial or accounting purposes, but 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 creates 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. The CJEU's ruling of 21 December 2016 in the Tele2 Sverige and Watson-cases[4] may well have exacerbated this problem, but its precise impact on the practice of criminal investigations and prosecutions has yet to be assessed.

Since the Court's 2014 ruling, the lack of unified retention of electronic communication data across the EU has proven a key challenge to investigating cross-border cybercrime. The operational experiences of both agencies have shown that electronic communication data is key to the successful investigation and prosecution of serious crimes (including cybercrime). The absence of a unified data retention obligation is felt in all three of the mandated cyber areas: cyber-attacks, online child sexual exploitation, and payment card fraud. Comprehensive analyses performed by Eurojust[5] and Europe's Data Protection Office[6] after the 2014 CJEU-ruling, have underlined the value of electronic communication data for criminal investigations and prosecutions and have shown that the majority of law enforcement and judicial authorities in the Member States would support a legislative framework at the EU-level.

---

3 ECLI:EU:C:2014:238 (case C-293/12)
4 ECLI:EU:C:2016:970 (case C-203/15 and C-698/15)
5 13085/15
6 EDOC#848769, developed on the basis of a survey to the EU MS and Eurojust's analysis (13085/15).

The Justice and Home Affairs Council in December 2015[7] reiterated the need for an EU-wide approach to mitigate the fragmentation of the legal framework on data retention across the Union and called for a new legislative initiative to be set forth.

Carrier Grade NAT

The loss of data challenge is also felt from the wide-spread implementation of Carrier Grade NAT (CGN) technologies by Internet Service providers (ISPs).[8] With CGN, ISPs and electronic content providers may not log certain types of information (like source port numbers and destination IP-addresses) that would otherwise allow law enforcement to associate criminal activity back to an end-user. Cyber investigators may be confronted with long lists of potentially hundreds or thousands of end-users associated with a particular public IP address, the investigation of which requires much resources, incurs large delays and generates privacy and data protection issues for many innocent customers. For these reasons, authorities may move to drop the case.

Encryption

Furthermore, 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. While this counts as a positive development to increase cybersecurity in general, traditional investigative techniques like wiretapping are becoming less effective and the possibilities of digital forensic analysis are negatively affected as a result of the increased implementation of encryption. This leads to a situation where criminals are able to effectively and indefinitely hide critical evidence and activities 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. Almost half of the MS also noted the increased use of encrypted email. The growing use of encryption by criminals to protect their communications or stored data was also recognised as considerable challenge in the IOCTA 2016, potentially leading to loss of critical intelligence and evidence. Twenty European countries, including 13 MS, reported the use of encryption software by cybercriminals in a deliberate (and generally successful) attempt to protect their data. The use of encryption is an established trend also among child sex offenders, who

---

7 14937/15

8 Carrier Grade NAT (CGN) is a technology that allows a single IP address to be shared by potentially thousands of subscribers/end-users on the same network simultaneously. CGN is used by 95% of mobile providers (network operators and mobile virtual network operators) and close to 50% of traditional Internet Service Providers (ISPs: cable, fiber and ADSL) worldwide (see also doc. 5127/17).

increasingly use it to conceal their online illegal activities and the illicit material stored on their devices.

In the assessment performed by the Council under the Slovak Presidency,[9] 20 MS responded that encryption is encountered often or almost always in the context of criminal investigations. Recent developments also indicate that terrorists are increasingly abusing modern technology and online platforms to conceal their identities and activities.[10] The observed increase of operational security measures such as the use of multi-layered encryption among cybercriminals and terrorists[11] create serious challenges for investigations. It is noteworthy that some MS have adopted legislative measures such as compulsory disclosure provisions, in order to mitigate the encryption challenge, but on one hand it is not always technically possible to disclose the data or to circumvent the encryption and on the other hand there exists no EU-wide legislation.

Virtual currencies

In addition, the widening criminal use of decentralised virtual currencies[12] and the increased use of tumbler/mixer services[13], 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[14] for such services and the non-application of existing regulations compound to the problem. In 2016, a growing number of cybercrime investigations involved cryptocurrencies and blockchain analytics in order to progress the criminal business model, which is indicative of the need to ensure that law enforcement and judicial authorities have the expertise, tools and legislative and regulatory means at their disposal to 'follow the money'.

---

9 13434/16

10 IOCTA 2014; IOCTA 2016; TrendMicro, Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations (2016); Flashpoint, Tech for Jihad: Dissecting Jihadists' Digital Toolbox (2016).

11 IOCTA 2016

12 Unlike centralised virtual currencies such as WebMoney or PerfectMoney, decentralised virtual currencies such as Bitcoin do not have a single administrating authority that controls the currency.

13 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 randomise transaction fees and add time delays to transactions.

14 As an example, see the recommendations proposed by the Financial Action Task Force - http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Loss of location

Recent trends such as the increasing criminal use of encryption, anonymisation tools, virtual currencies and the Darknets[15] 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.

The loss of location may also result in competing claims to prosecution[16], underlining the need for early involvement of judicial authorities through Eurojust, direct police-to-police channels for cooperation and communication facilitated by Europol, and continuous innovation in the process of operational collaboration.[17]

Legal framework

Differences in legislation

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.

---

15 According to the IOCTA 2015 and 2016, 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.

16 Due to the cross-border nature of online services, electronic evidence can be stored in a different location from the one where the service is being provided; such situations result in challenges in defining which authority has competence of the investigatory measures – the one where the service is provided or where the data is physically stored.

17 One example is the Joint Cybercrime Action Taskforce (J-CAT) that is hosted and supported by Europol.

The main differences regard the criminalisation of conduct and 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. Case law (jurisprudence) can be a valuable tool to compensate for a lack of specific legislation, but unfortunately little case law exists with regard to new developments (e.g. virtual currencies, anonymisation tools and various technology-driven criminal modi operandi). Furthermore, existing operational processes (like the Mutual Legal Assistance process) could be harmonised and streamlined and forensic-technical standards for the collection and transfer of e-evidence could be developed.

The proliferation of the internet and the growing sophistication of cybercrime require dedicated legislation that more specifically regulates law enforcement presence and action in an online environment.

Expedited measures

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.

Online investigations

Similarly, there is a growing need for a harmonised legal framework at EU level for conducting online investigations, which would allow for more effective joint operational actions such as large-scale botnet and/or underground criminal forum takedowns. Specifically, possibilities to monitor criminal activities online and to lawfully collect critical evidence on the Deep Web and Darknets could be harmonised across the Union to allow for effective operational activities and subsequent introduction of evidence in judicial proceedings.

Public-private partnerships

Legal framework

Cooperation with the private sector is vital in combating cybercrime[18]. Not only does the private sector hold much of the 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 fight cybercrime. However, little consensus exists on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector,[19] while at the same time regulating legal and transparency issues surrounding that cooperation. Moreover, data protection regulation and fear of liability may pose serious obstacle to cooperation with private industry.

Rules of engagement

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.

Jurisdiction

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.

[18] See http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

[19] For example, whether national legal measures are applicable to service providers offering a service in that country but based in another jurisdiction; the new rules stemming from the new EU Data Protection Regulation and Directive and their implementation, etc.

Public-private cooperation

Although progress in addressing challenges associated with the public-private collaboration has been achieved,[20] such developments do not diminish the need to surround this form of cooperation with a solid and uniform legislative framework. This need is echoed in the Franco-German call to examine the possibility for a harmonised legal framework regulating the obligations for electronic communication service providers to effectively comply with legal process issued by investigating and judicial authorities.[21]

Internet of Things

Recent developments also show a growing need for regulation concerning the lack of security and privacy by design features of internet-facing devices (as indicated by the emergence of Internet of Things botnets) and common cybersecurity rules at EU level for the consumer market[22]. The current efforts at EU level regarding cybersecurity certification and labelling could also add value in addressing this challenge.[23]

---

20 For example, Europol's EC3 new Advisory Group on Communication Providers aimed at improving the voluntary cooperation in cross-border cybercrime cases, Eurojust's support to law enforcement and judicial authorities in Member States on the best practices for acquiring electronic data (content and non-content) from electronic communication providers, and the recent success of dismantling the Avalanche network, among others.

21 See https://www.euractiv.com/section/digital/news/eu-backs-franco-german-bid-for-access-to-encrypted-messages/

22 See https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/

23 See http://www.aioti.org/ and https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

International cooperation

The collection of electronic evidence is often a time-sensitive issue. The current process of MLA is perceived by practitioners 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. The implementation of the European Investigation Order (EIO) Directive may go some way in addressing these issues for the majority of MS. However, the EIO framework may not accommodate for the speed that is required to capture electronic evidence. Moreover, the Directive doesn't contain provisions that specifically facilitate the collection of common types of electronic evidence, meaning that additional tools need to be developed to facilitate the collection of electronic evidence under the EIO framework.

Simultaneously, the various existing legal tools and mechanisms could be better promoted at the 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 MLA request conforms to all the relevant legal requirements of the requested country. In this context, it may be relevant 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, because effective alternatives exist (for instance the possibility of directly requesting non-content data from US-based electronic service providers).

Furthermore, the current differences in legal frameworks and ineffective international cooperation may 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.

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), the Training of Trainers (TOT) Project and the training activities under the EU Policy Cycle 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 particularities of cybercrime.

3. Addressing the challenges identified

On-going activities

While the main focus of this joint summary is to highlight practical and legal challenges in fighting cybercrime, a number of relevant developments and activities can be identified that already provide forward momentum in addressing the issues.

The most relevant of these are the JHA Council conclusions of 9 June 2016 on *improving criminal justice in cyberspace*, which highlighted the need for concrete activities to (1) improve the current process of MLA, (2) improve direct cooperation with electronic communication providers and (3) improve the establishment of jurisdiction in cyberspace. Following-up on these conclusions, the Commission has initiated a work process, which also includes actions regarding the issues in relation to the EIO.

Eurojust and Europol actively contribute to the work of the Commission, while at the same time shaping and prioritising their own activities to align with the Commission's work process.

Other activities performed by the Commission (for instance with relation to the challenges of encryption) and the Council of Europe Cybercrime Convention Committee (T-CY) provide for the additional forward movement with regard to a number of the challenges mentioned in this document. Similarly, the outcome of the recently concluded EVIDENCE project[24] may contribute towards the establishment of forensic-technical norms regarding electronic evidence.

On a practical level, the establishment of the European Judicial Cybercrime Network (EJCN) introduces a new actor to the stage, which may fuel on-going discussions and activities with relevant practical expertise and play an important role in improving international cooperation against cybercrime among judicial authorities (similar to the EUCTF[25] on a law enforcement level).

---

[24] See http://www.evidenceproject.eu/about-evidence/concept-and-objectives.html

[25] In execution of the JHA Council conclusions of 27th – 28th November 2008 and of the 26th of April 2010, Europol together with the European Commission and the EU Member States have set up the European Union Cybercrime Task Force (EUCTF) composed of the Heads of the designated National Cybercrime Units throughout the EU Member States and Europol. The EUCTF is an inter-agency group formed to allow the Heads of Cybercrime Units, Europol, the European Commission and Eurojust to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond.

Open issues

Still, a complete resolution of the identified challenges is likely to require much more actions. Also, some of the challenges identified are not (specifically) covered by the on-going activities described above. For the purpose of addressing these issues, a number of possible actions and key principles can be identified. These activities should be executed in a coordinated and complementary manner, taking into consideration the relevant work already done at the EU-level. Relevant actions would include:

- Streamlining and strengthening of existing legal frameworks and operational processes.
- The establishment of a consolidated cooperation framework for the collection and exchange of evidence and 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.
- CGN technology has created a serious online capability gap in law enforcement efforts to investigate and attribute crime. This needs to be addressed through dialogue with content service providers via the EU Internet Forum and through engagement with internet access providers to collectively examine ways of limiting the impact of CGN technologies on criminal investigations.
- The development of an EU-wide framework for conducting online investigations, specifically on the Deep Web and Darknets.
- Strengthening the rule of law in cyberspace and establishing minimum cybersecurity standards, specifically by addressing the criminal abuse of new technologies.
- An EU agency-driven approach to discuss and identify alternative solutions to common challenges, such as the Europol-ENISA joint Working Group on Security and Safety Online.
- Training and capacity building for law enforcement and judicial authorities.