Council of the European Union

Brussels, 11 May 2016
(OR. en)

8634/16

LIMITE

JAI 357
COSI 74
ENFOPOL 129
CYBER 46
CATS 32

NOTE

From:	Presidency
To:	Standing Committee on Operational Cooperation on Internal Security (COSI)
Subject:	Effective operational cooperation in criminal investigations in cyberspace

1. Over the last decade the possibilities of new Information and Communications Technology (ICT) features and the way people are using ICT have dramatically changed the landscape of cybercrime as well as the investigation and prosecution of it. Web-based applications and cloud computing are normal these days. Transport of information easily takes the shape of anonymous communication.

2. Cybercrime, like the internet, is borderless. Cybercriminals can target from one country victims in another country, whilst using infrastructure based in a third country. Effective action against cybercrime relies heavily on international cooperation between police and prosecution services. Within the EU both Europol and Eurojust offer substantial assistance with investigation and prosecution. In order to keep up with the rapid developments in the field of cybercrime, more effective and intensified operational cooperation is key.

3. The NL Presidency prioritises, in line with the Renewed European Union Internal Security Strategy[1], the improvement of international operational cooperation and development of an EU approach for investigations in cyberspace, including on enforcement jurisdiction.

[1] 9798/15

4. With a view to furthering the development of an EU approach for investigations in cyberspace, the Netherlands Presidency hosted a Conference on "Crossing borders: Jurisdiction in Cyberspace" on 7 and 8 March 2016 in Amsterdam[2] to highlight the issue of cross border law enforcement and investigation powers. Possible ways forward on how to deal with legal and other challenges posed by traditional interpretations of enforcement jurisdiction in cyberspace, the loss of location and cooperation with private parties were discussed. In order to improve judicial cooperation, a network of cybercrime prosecutors and judges is anticipated.

   Council conclusions on improving criminal justice in cyberspace and on the establishment of the European Judicial Cybercrime Network will be presented at the CATS meeting on 19 May 2016, with a view to their adoption at the JHA Council meeting of 9-10 June 2016. The Ministers will be also invited to provide a political guidance on some of the open issues regarding enforcement jurisdiction in cyberspace.

5. The Renewed European Union Internal Security Strategy Implementation Paper (5298/1/16 REV 1) stated that COSI would discuss, in the framework of the EU Policy Cycle for organised and serious international crime, the effectiveness of operational cooperation between the law enforcement agencies within the field of cybercrime on the basis of experiences with the operational action “Illicit trade markets via the darkweb” of the EMPACT project on cyberattacks.

6. In this paper the Presidency identifies a number of recommendations for the improvement of future criminal investigations in cyberspace on the basis of the EUROPOL report “Strengthening the fight in the EU against cyber-enabled forms of serious and organised crime”, which is annexed to this paper.

   This EUROPOL report is based on “Joint Actions” that have recently been undertaken under the EMPACT framework against significant threats posed by illicit online trade and criminal financial schemes supporting various forms of cybercrime and cyber facilitated crime. These Joint Actions encompassed two operations:

[2] 7323/16

a) **DELETED**

b) **DELETED**

7. The EUROPOL report also draws on the final report of the Working Group on Cybercrime of the European Police Chiefs Convention held at Europol on 24 and 25 September 2014, as well as on other relevant reports (e.g. the joint paper prepared by Europol and Eurojust on "Common challenges in combating cybercrime"[3] and the evaluation reports on several Member States adopted by GENVAL under the seventh round of mutual evaluations on "the practical implementation and operation of European policies on prevention and combating Cybercrime") .

COSI is invited to:

a) Discuss this paper and take note of the report by Europol;

b) agree on the recommendations outlined below in this document.

[3] 14812/15

RECOMMENDATIONS

DELETED

DELETED

EUROPOL | EC3 European Cybercrime Centre

The Hague, 2 May 2016

EDOC # 826504v4

STRENGTHENING THE FIGHT IN THE EU AGAINST CYBER-FACILITATED FORMS OF SERIOUS AND ORGANISED CRIME

1. Introduction

Whilst the internet is continuously expanding its presence and value in the daily lives, work and structures of society, it also offers increasing possibilities for criminals to develop new business models, markets and partnerships. Partially, those possibilities derive from technological developments like encryption and obfuscation of internet traffic; partially room for criminal manoeuvre results from the difficulty that law enforcement and policy makers have to keep up with crime evolution.

This note aims to present some concrete examples of how crime and criminal processes have evolved as a result of evolving internet communication technologies with a view to enabling the identification of possible avenues to address these phenomena more successfully by means of enforcement strategies and policy measures.

The main criminal themes mentioned as examples in this document, in particular illicit trade on the Darknet and the practices in criminal finance associated to that, have also been elaborated in several other reports. Some references are suggested at the end of this note to find more detailed information.

2. Some current criminal practices facilitated by internet technology

One of the main advantages that the internet can offer to criminals is anonymity. This applies in several senses, which make it very difficult to discover and attribute crimes, especially if the anonymous operating possibilities are combined.

The development of dark markets and criminal forums on hidden networks such as TOR[4] and I2P[5] (both generally referred to as *Darknet*) are good examples of the anonymization marking 21st century crime. Traders and buyers can operate apparently anonymously on a market with a wide variety of criminal commodities and services, including drugs, weapons, stolen goods, forged documents and currencies, multiple cybercrime services, such as botnet renting for DDoS attacks as well as executing such attacks on demand, tailor made malware, zero-day exploits[6], malware testing against anti-virus products, intrusion, password cracking and sales of large quantities of email accounts for spamming, stolen payment card credentials, child abuse material and even assassination on demand.

Apart from serving as a safe haven for illicit trade the anonymity of the Darknet also offers a protective environment for like-minded individuals to meet each other, share their deviant experiences and thoughts on extremism, terrorism and child sexual abuse and where possible to proliferate to a wider audience. Criminals and extremists are also known to use the criminal online forums to exchange methods and best practices to better protect themselves against detection and law enforcement intervention.

The anonymization of illicit trade is conveniently facilitated by the availability of anonymous payment services. There are many financial products with varying levels of asserted anonymity, such as virtual currencies, of which Bitcoin is also among criminals becoming the most preferred, and prepaid debit cards to facilitate criminal transactions and money laundering. But even the cashing out of criminal profits is available as a criminal service online.

Yet another dimension worth mentioning in the context of anonymity is that of recruitment and criminal partnerships. Due to the existence of criminal communication forums on the Darknet (but not exclusively there since there are also many on the open net) it is very easy for criminals to find each other in an anonymous environment and to explore possibilities for criminal partnerships and cooperation. But also, the ease of using fake identities in any form of communication and on regular social media makes it possible to recruit even *bona fide* individuals for unknowing participation in criminal processes. This applies sometimes as part of money mule schemes for the laundering of the proceeds of various forms of crime.

---

4 TOR stands for *The Onion Router*. The origin and destiny of traffic are obfuscated by re-routing of traffic via several nodes whilst information is gradually encrypted and decrypted. As such, the protection is built in multiple layers, hence the naming after the onion.

5 I2P stands for the Invisible Internet Project and works with comparable obfuscation techniques.

6 These are unknown vulnerabilities in hardware or software that allow intrusion and hacking.

In regard to the latter, organised crime groups involved in cybercrime or cyber-facilitated types of crime often use money mules to cash out the financial gains from criminal activities. Money muling (cashing out payments) is an important element in the cycle of criminal processes such us online fraud, illicit drug trade and human trafficking. For that reason specific attention is also given to that phenomenon in this note.

A money mule is someone recruited and deployed by criminals as part of the money laundering process. Such persons are tasked to cash out, transport or transfer amounts of money between different payment accounts and/or payment instruments, often in various jurisdictions in exchange for a promised commission payment.

The predicate offences that such proceeds derive from can vary a lot. The criminal gains can come from forms of cybercrime, such as phishing, malware and spam, but it can also be linked to more traditional types of serious and organised crime, such as drug trafficking, illicit trade and trafficking of weapons, trafficking of human beings, forgery of documents, etc.

It is noteworthy that a small percentage of money mules are not aware that they are being used to commit fraud or other forms of crime, but have become victims to a scam, set up intentionally by criminals (for instance, by means of fake job advertisement offering cash rewards in exchange for a service). Nevertheless, the vast majority are knowingly and willingly taking part as money mules within the criminal scheme.

3. Key challenges for law enforcement

The new directions that criminals head for are often chosen in function of the expected profits and the chances of getting caught. It is therefore not surprising that the latest criminal tactics usually include elements that hamper detection, investigation and prosecution. As such, successful police operations can have a catalysing effect on criminal innovation.

The difficulties for law enforcement in policing the Darknet were described quite comprehensively in the final report of the Working Group on Cybercrime of the European Police Chiefs Convention of 2014. These difficulties were listed as follows:

The first one is that of detection. Obviously, law enforcement should only focus on the abuse of anonymity for criminal purposes. But the detection of crimes on Darknets requires a legal basis. Although police surveillance in the public environment of the off-line world is uncontested, in the online world this is not clearly arranged in all jurisdictions of the EU.

The second and probably the most important issue is that of attribution. The re-routing of Internet traffic over various nodes and the obfuscation of its origin makes it difficult to locate the device used for the communication. The same applies to the server on which criminal services are hosted. Most Member States' competent authorities lack the technical competence to overcome the anonymisation. Where tracing could be enabled, for instance with the help of private partners or academia, the legal framework in most Member States does not permit the use of such instruments. A dependency therefore exists on some law enforcement partners outside the EU that must allocate such resources to their own investigations first.

In cases in which criminals and criminal infrastructures have been detected, the third issue is that the scope of possible legal action taken is restricted by jurisdictional boundaries. In recent years international cooperation has improved, but the possibilities for judicial cooperation with countries in Eastern Europe, including Russia, Southeast Asia, South America and most parts of Africa are still limited for the majority of EU Member States.

Following the money - one of the traditional ways of investigating serious offences - is suffering from the increased popularity of virtual currencies among criminals. Apart from the technical challenges of investigating crypto-currencies and other schemes, there is a lack of direction at policy level. Member States appear to have a predominantly national approach to regulation, if any at all. The differences between the legal frameworks applied within the EU complicate cross-border law enforcement cooperation, while allowing criminal networks to select the most ideal conditions for their cause.

Last but not least, the techniques that are being used to enhance anonymity and to reduce detection are getting more and more sophisticated. This applies in particular to the use of state-of-the-art encryption that is very hard to break. Initial signs are already emerging that police services are confronted with encryption they cannot break[7]. Some virtual currency schemes are introducing increasingly advanced techniques to hide the traces of the criminal money flows.

[7] www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013

As regards the recruitment and deployment of money mules by criminals the following challenges can be added:

The detection of criminal transactions related to money laundering is for a large extent dependent on the cooperation with the private sector. The transfer of sums of money between bank accounts, but also between payment systems such as money transfer services, credit card companies, virtual currencies and traditional bank accounts, call for dedicated attention by financial service providers. Moreover, they require an adequate legal basis for processing and sharing between financial industry partners and law enforcement to effectively discover and investigate money laundering and money muling. That legal basis may be different or lacking, depending on the EU Member State in which the financial service providers operate.

Given the recruitment methods used, in particular when seemingly lawful business methods are presented, it is important to establish and demonstrate criminal intent of those money mules that knowingly and willingly take part in the money laundering schemes. However, often police officers, prosecutors and judges have a tendency to gratefully accept the excuses of money mules, which may lead to a lack of thorough investigation of the facts and circumstances.

4. DELETED

DELETED

DELETED

DELETED

DELETED

5. Policy considerations

What these two investigations have in common is that they focus on the phenomenon of money laundering as the criminal process that connects the underground economy with the licit world. Neither of the two goes beyond what touches the surface. And it is exactly into the deeper layers of criminal structures and partnerships that law enforcement should reach to make a fundamental difference in the fight against organised crime.

To achieve that in practice, the current fragmentation of actors and their investigative actions should be considered. Some initiatives focus on drug trade, others on stolen goods, again others on the trade in weapons and explosives. These efforts would benefit from the joining of forces internationally and across law enforcement domains. This should include the investigative work to identify traders of illicit goods and services, the disruption of the logistics chains with the help of parcel services and customs and the localisation and take down of criminal infrastructure and the arrest of technical facilitators hosting the forums and illicit trading places with high-tech cyber capabilities.

DELETED

In terms of regulation, the speed of technical developments outpaces the ability for most legislators to update and adjust the general legal framework as well as that of criminal procedural law concerning law enforcement competences online. Moreover, when the gaps get filled, there is still the issue of diversity between EU Member States on how they resolve the regulatory challenges within their respective jurisdictions. This further complicates the vital international cooperation, as was also demonstrated in practice above. Therefore, an EU approach to the required regulation would be beneficial in terms of alignment and might even add to the efficiency and timeliness of the adjustments.

Last but not least, it must be emphasized that the anonymization techniques used for establishing TOR were and still are aimed at truly valuable causes, in particular to enable freedom of speech and authentic journalism and that spirit must be protected and preserved in any policy approach intended to minimize the abuses of anonymity for criminal purposes. The same applies to virtual currencies that have been created primarily for legitimate purposes and are in fact also used on a large scale for licit transactions.

6. Conclusions and recommendations

Suggestions for policy measures and enforcement strategies:

Increased attention and priority to combat the increasingly cyber-facilitated forms of serious and organised crime, such as the illicit online trade in all sorts of criminal commodities and services as well as the laundering of the proceeds thereof by means of a horizontal alignment of the operational focus across crime areas (cyber, drugs, weapons, etc.) in holistic, integrated investigation programmes;

Explicit (preferably EU-wide) regulation of the use of investigative techniques to detect illicit online trade and attribution to criminals as well as the localisation of criminal infrastructure (including undercover operations, test purchases, infiltration, hacking of devices and the use of so-called *network investigation techniques* to reveal the real IPs of criminals and criminal infrastructure);

Resolution of the jurisdiction questions and explicit authorisation of proportionate measures to determine geographical location in cases where the Darknet or obfuscation techniques are abused for criminal purposes;

Legal framework for the pro-active processing of data by private parties for the detection of forms of abuse affecting their services or customers and the sharing of that information with other private parties and law enforcement where relevant for the prevention and investigation of crimes;

Explicit criminalisation of the abuse of virtual currencies for criminal transactions and the facilitation of money laundering;

Extensive and continued innovative technical capacity building to enable the investigation and attribution of illicit online trade as well as the of blockchain technology of virtual currencies for investigative purposes;

Increased use of prevention and awareness campaigns to reduce innocent facilitation of organised crime by potential money mules and to reduce the attraction of illicit marketplaces and criminal online forums.

7. References

- Internet Organised Crime Threat Assessment (IOCTA) 2015, Europol's EC3, (https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015)

- Common Challenges in Combating Cybercrime, 2015, Eurojust & Europol, (http://english.eu2016.nl/documents/publications/2016/03/7/general-ej-ec3-joint-paper-version-1.0-final)

- European Police Chiefs Convention 2014 – Report of the Working Group on Cybercrime, 2014, (Not publicly available)

- End report of the ITOM (Illicit trade on Online Marketplaces) Project (to be issued shortly).