COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 25 April 2016 CODEXTER (2016) 2

COMMITTEE OF EXPERTS ON TERRORISM

(CODEXTER)

TERRORISM AND THE INTERNET

DISCUSSION PAPER

30th Plenary Meeting

Strasbourg (France), 19 – 20 May 2016

Secretariat of the Counter-Terrorism Division
Information Society and Action against Crime Directorate, DG I

codexter@coe.int - www.coe.int/terrorism

Summary

The present Discussion Paper provides an overview of the main challenges arising from the use of internet for terrorist purposes. It focuses on four main issues, namely: problems related to encryption of devices and data; blocking and taking down of websites and social media accounts used for terrorist purposes; jurisdiction issues related to data stored in other jurisdictions, including "the Cloud"; and, identification of physical/legal persons behind IP addresses used for terrorist purposes. The Discussion Paper refers to international and European relevant conventions and judicial decisions, as well as academic papers and online articles of qualified publicists. Finally, the Discussion Paper contains a series of recommendations addressed to the CODEXTER concerning possible measures to be taken at the international level, including the feasibility of engaging with major Internet companies through a platform to be established under the Council of Europe Strategy on Internet Governance (2016 – 2019).

1. Background information

On 19 May 2015, the Committee of Ministers adopted the Action Plan on "The fight against violent extremism and radicalisation leading to terrorism" to reinforce the legal framework against terrorism and violent extremism and to prevent and fight violent radicalisation through concrete measures in the public sector, in particular in schools and prisons, and on the Internet.

Noting that the Internet and the social media are widely used by those who seek to recruit terrorist fighters, the Committee of Ministers acknowledged that action in this area must be stepped up, with due respect for the fundamental principle of freedom of expression and information, as enshrined in the European Convention on Human Rights.

On the basis of its Terms of Reference for 2016 – 2017, the CODEXTER, at its 29th Plenary Meeting, discussed a document containing proposals for priority areas for its work in the biennium and decided to address terrorism and the Internet as the first priority subject to be examined. The CODEXTER noted that the Council of Europe, through its various competent committees, is in a unique position to facilitate international cooperation and prevent the use of the Internet by terrorists to spread their message of hatred and terror.

At its 7th meeting (16 – 17 March 2016), the Bureau of the CODEXTER decided to appoint Mr Mario JANECEK (Bosnia and Herzegovina) as Coordinator for the topic of "Terrorism and the Internet".

In order to facilitate the deliberations of the CODEXTER, the Secretariat, in consultation with the Coordinator, requested Mr Eirik Trønnes Hansen, Prosecutor, NCIS Norway, as expert on cyber-crime related issues, to prepare a discussion paper analysing the main challenges arising from the use of the Internet for terrorist purposes and pointing out the main problems and – possibly – solutions.

The present discussion paper is the outcome of the work of Mr Eirik Trønnes Hansen and is intended to form the basis for the discussions of the CODEXTER at the occasion of the 30th

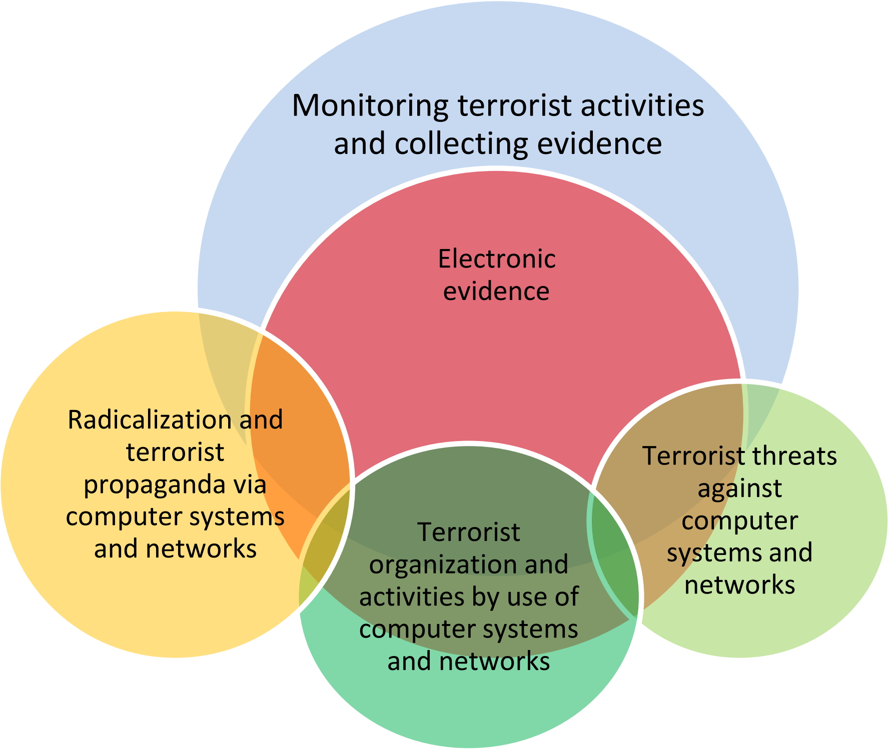
Plenary Meeting of the Committee. This document does not necessarily reflect positions of the CODEXTER.

2. **Introduction**

With the ever increasing growth of internet technology, services and use, terrorist use of internet is an increasing challenge for law enforcement and for the public safety.

In this discussion paper, the terms “terrorism” and “terrorist offence” are based on Article 1 of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) according to which:
For the purposes of this Convention, "terrorist offence" means any of the offences within the scope of and as defined in one of the treaties listed in the Appendix.

The Appendix refers to 11 international conventions[i]: Several of the conventions deal with terrorist acts against communications (civil aviation, maritime navigation), but currently, no international convention deal specifically with terrorism against computer systems and networks or with terrorist use of computer systems and networks. These issues may still be covered by the Council of Europe Convention on Cybercrime, (CETS No. 185). In Guidance Note # 6 (4-5 June 2013), the T-CY states that critical information infrastructure attacks may be covered by the Convention Articles 2, 3, 4, 5, 7, 8, 11 and 13. These articles in the Convention would also apply if an attack could be connected to terrorist activities. The T-CY is currently working on a guidance note for terrorism and the Convention on Cybercrime. In addition, the measures in the Convention for securing electronic evidence applies also in cases connected to terrorist activities, including Articles 23, 25, 29 and 32. The current main challenges can be illustrated with this diagram:


Monitoring terrorist activities and collecting evidence
Electronic evidence
Radicalization and terrorist propaganda via computer systems and networks
Terrorist organization and activities by use of computer systems and networks
Terrorist threats against computer systems and networks

These different activities, both regarding various terrorist activities and law enforcement actions against terrorism, will typically include electronic evidence. Many of the issues regarding electronic evidence and terrorism will be quite similar for terrorist activities compared with other types of crime. Terrorists have most likely used internet services for internal communication since the technology was available. With increasing use and increasing technological possibilities, even simple measures have been used by terrorists to reduce the chances for detection.

The New York Times wrote April 27 2008:

http://www.nytimes.com/2006/04/27/world/europe/27iht-spain.html?_r=0
"One of the leading figures indicted in the March 11, 2004, train bombings in Madrid used a simple trick that allowed him to communicate with his confederates on ordinary e- mail accounts but avoided government detection, according to the judge investigating the case.

Instead of sending the messages, the suspect, Hassan El Haski, saved them as drafts on accounts he shared with other radicals, according to papers issued by the judge, Juan del Olmo. They all knew the password and so they could access the accounts to read his comments and post replies, according to the judge.

This ruse meant that there was no digital trail that the authorities could easily trace, according to the judge and government. Had the messages been e- mailed, the government might have monitored them, as is common across Europe.

Intelligence officials have said in the past that terrorist groups were using the trick, which investigators call a "virtual dead drop." But few concrete examples have come to light, especially in an attack as extreme as the Madrid bombings, which killed 191 people."

The recent experiences regarding the so-called "Islamic State/ISIL/Daesh" have increased public and law enforcement interest in how terrorists use the internet and other electronic systems and networks.

Other reports have focused on specific cases, for example the report "Anders Behring Breivik's use of the Internet and social media" from Jacob Aasland Ravndal, FFI (The Norwegian Defense Research Establishment), 2013, regarding the attacks in Oslo and at Utøya, Norway, July 22, 2011: http://journals.sfu.ca/jed/index.php/jex/article/view/28
"This article describes Breivik's use of the Internet and social media along four dimensions: (1) online radicalization, (2) online gaming, (3) online attack preparations, and (4) online propaganda. (…)

A key finding in this study is that Breivik likely never discussed his terrorist plans with anyone online. Moreover, his comments on various Internet forums do not stand out as particularly when compared to typical far-right online discourse.

In other words, Norwegian security authorities would likely not react to his online postings even if he was being monitored. (…)

Breivik's online posts also indicate that his critical views on Islam and socialism ***had been established long before*** *the so-called counterjihad blogs were created. This means that these blogs may have played a less decisive role for Breivik's early radicalization than assumed by many.*

Later on, however, these blogs certainly strengthened Breivik's radical thinking, although they come across as far less radical than his own ideological statements after 22 July. (…)

"Breivik's e-mail correspondence shows that he first and foremost wanted to become a professional ***author and publisher****. He proposed to establish a so-called cultural conservative paper journal together with Norwegian bloggers he admired, who were also critical of Islam and multiculturalism. (…)*

The fact that ***he was rejected by several of the people he looked up to*** *may have had a decisive influence on his violent radicalization. (…)*

Breivik ***gathered all the necessary information to build his bomb online.*** *He also* ***financed*** *the terrorist attacks through an online company, and used the Internet, in particular e-Bay, to buy materials such as body armor, weapons components and bomb ingredients.*

Breivik also systematically used ***social media platforms*** *such as Facebook and Twitter for* ***propaganda*** *purposes."*

The experiences from the Madrid bombing as well as the Oslo and Utøya attacks show some practical limitations: how can law enforcement search for electronic messages when no messages are sent? In addition, there are also legal limitations. As mentioned in the UNODC report, Chapter 1, B, I, nr. 11:

"It is important to emphasize the distinction between mere propaganda and material intended to incite acts of terrorism. In several Member States, in order to be held liable for incitement to terrorism, a showing of the requisite intent and a direct causal link between alleged propaganda and an actual plot or execution of a terrorist act is required. For example, in a contribution to the expert group meetings, a French expert indicated that the dissemination of instructive materials on explosives would not be considered a violation of French law unless the communication contained information specifying that the material was shared in furtherance of a terrorist purpose."

These limitations may be based on protected rights, such as freedom of speech, right to privacy and data protection. Solutions and improvements regarding the fight against terrorism must be done in balance with these and other civil society rights and safeguards. Several reports and publications have discussed these issues, including the UNODC report "The use of the internet for terrorist purposes" (2012).

https://www.unodc.org/documents/frontpage/Use_of_Internet_for_ Terrorist_Purposes.pdf

There are several differences in how different areas of electronic communications are regulated and how law enforcement can access data in question. Traditional telecom companies offering phone services are typically regulated by specific national laws, that typically provide a duty of secrecy regarding their customers' communication, but also regulate how law enforcement may get access to information in criminal cases, such as lawful interception of communication. Companies offering various services for internet users are often offering their services across borders. This complicates jurisdiction issues. These companies and their data may be subject to production orders or search and seizure, but may offer encrypted and/or anonymized services, that make it difficult or impossible for law enforcement to get access to usable electronic evidence.

Type	**Legal regulation**	**Direct requests from own jurisdiction?**	**Direct requests from other jurisdictions?**
Telecom providers	Specific, national telecom provisions, duty of confidentiality.	Some requests, based on national law, ex. subscriber information.	Usually not, this may be specifically against national law.
Social media and e-mail companies (Google, MS, Facebook, VK…)	Data protection laws, user agreements, other provisions	Some requests, based on national law, ex. subscriber information. Production order?	Some requests, based on national law, ex. subscriber information. Different practices in the U.S., vs. EU vs. Russia. MLA?
Website hosting	Data protection laws,	Some requests, based	Some requests, based on

companies	user agreements, other provisions	on national law, ex. subscriber information. Production order?	national law, ex. subscriber information. Different practices in the U.S., vs. EU. MLA?
Internet registrars	Data protection laws, user agreements, other provisions	Some requests, based on national law, ex. subscriber information. Production order?	To some extent. Some data is in searchable public registers. MLA?

3. Problems related to encryption of devices and data

3.1 Introduction

Encryption can be described as a process where information is altered so that it can only be read by authorised parties, for example the sender and the intended recipient. Encryption systems often use two keys: a public key, available to anyone, and a private key, that allows the authorised parties to get access to the information in question. Some encryption schemes are offered by vendors as commercial products, others (for example OpenPGP) are open standards, to be used by anyone.

Encryption can be a valuable tool for individual users and industries, to protect privacy and secure data from intrusion and criminal abuse of data and system access. However, encryption may give law enforcement challenges to access data and services that otherwise might have been used to collect evidence in criminal investigations, including terrorist cases.

The legal and practical challenges may vary in different situations, as described below.

3.2 Encryption of non-networked devices held by the suspect

For non-networked devices held by the suspect, for example disk drives, getting access to encrypted data may be a technological challenge, but rarely a legal challenge. In some cases, the password is available. It may be written down on a piece of paper found during search and seizure, or stored on the device. Sometimes the suspect informs the police about the correct password. Law enforcement in European jurisdictions can generally use the password to unlock, at least if the password was obtained by the police in a legal way (search and seizure, production order etc.). In these cases, no third party interests are involved.

If the correct password is not available, law enforcement may try to use special software or other methods to "guess" the correct password. This is generally seen as an extension of search and seizure, and will not create new legal issues, at least not for non-networked devices.

Some jurisdiction such as the UK, have legal instruments that may compel a suspect to disclose the encryption key for data. According to The Regulation of Investigatory Powers Act, Section 49 (3), *"A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary –*

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the United Kingdom."

This will include terrorism investigation, including law enforcement activities to prevent terrorist attacks.

According to this act, Section 53 (5) (a), failure to comply with a notice ("*if he knowingly fails*") may lead to imprisonment for up to five years in a national security case.

Similar legal instruments have been discussed in other European jurisdiction, but the main focus has been on compelling third parties to give access to data. The issue of self-incrimination (cf. the European Convention on Human Rights Article 6 and related practice from the European Court of Human Rights) could be an issue in cases where suspects should be compelled to give law enforcement access to data.

3.3 Encryption of non-networked devices held by others

Non-networked devices with information of value as evidence may be held by witnesses and other third parties. The device may be subject to search and seizure or production orders, but if the data in question is encrypted, is there duty to assist in unlocking? This will depend on local legislation. One example, Compare with the Norwegian Criminal Procedure Act Section 199 a:

"*When conducting a search of a data-processing system the police may order everyone who is dealing with the said system the information necessary for gaining access to the system. A breach of duty to provide information which is committed by persons other than the person charged shall be punishable pursuant to section 339, No. 1, of the Penal Code.*"

In addition to the issue of self-incrimination, access to encrypted data may also face legal challenges if the device is held by people with no duty to testify (close family members) or people/legal persons with legally protected duty of confidentiality (lawyers, priests, medical professionals etc.). Unless there is a legal exception from the general duty of confidentiality in terrorism cases, based on local laws, it may be problematic or clearly not possible to comply persons from these protected groups to disclose information to law enforcement.

3.4 Telecom services

Traditional telecom services are generally regulated by national laws, including provisions that may require the telecom company to make lawful interception technically possible. These regulations will generally make it more difficult or not possible for European telephone companies to offer phone services that could not be monitored by local law enforcement where required by legal provisions and court orders.

3.5 Non-telecom internet services

While telephone services in Europe have been regulated by local laws, and often historically where offered by one state-owned service, newer services like e-mail, web site hosting, social media, chat, Voice over IP etc., are not covered by the telecom regulations. One difference is that while telecom companies typically offer their traditional services clearly within one jurisdiction at the time, newer internet services may offer their services across borders and often worldwide. In addition to different regulations, there's an issue of correct jurisdiction for non-telecom internet services.

Most internet services offer some kind of password protection, to prevent abuse. Some internet services offer automatic encryption, for example of e-mail messages. Other services, like website hosting, may have stored data encrypted by the user.

There's generally no specific national or international regulation for encryption in these cases. In might be possible for law enforcement to contact the service in question and request access to data. However, if the data is encrypted, either by the user or by the company in question, the provider may not be able to decrypt the messages in their own service.

As mentioned in the introduction, encryption of data may be a good practice for many users. Several large scale breaches of data security could have been prevented if the data in question had been encrypted. There is a real need for individual users and businesses to protect their information. In some cases, law enforcement still need to access data and encryption appears to be a growing challenge. A production order may be legally possible, but unlocking the encrypted device may still not be technically possible.

One possible difference between encryption of non-networked devices and encryption of online services is that the service providers *could* implement some limitations to the encryption, with an option to access the data flowing through their services. This would be comparable with the possibilities for lawful interception that traditional telecom companies offer within a specific legal framework. The counterargument, from many businesses and public advocacy organisations, is that "backdoors" are unsafe and may be abused by others. In addition, the possibility of "backdoors" may reduce consumer trust in their products and services.

Some internet services may not have an identifiable owner or a legal entity to contact for decryption assistance. One example is open source protocols like XMPP, an internet messaging service protocol, also known as Jabber. These protocols may be used by a number of parties that in turn may be difficult to identify. Another question is if these parties would be able to decrypt their services if asked.

BBC News reported April 5, 2016 that the popular WhatsApp internet messaging service, is introducing encryption of their services:

www.bbc.com/news/technology-35969739
"With end-to-end encryption, messages are scrambled as the leave the sender's device and can only be decrypted by the recipient's device. It renders messages unreadable if they are intercepted, for example by criminals or law enforcement WhatsApp, which has a billion users worldwide, said file transfers and voice calls would be encrypted too. The Facebook-owned company said protecting private communication was one of its "core beliefs". (…)

Users with the latest version of the app were notified about the change when sending messages on Tuesday. The setting is enabled by default. (…)

Other messaging apps with end-to-end encryption include Telegram, which is known to be used by the so-called Islamic State to share information."

In theory, governments could introduce laws that would put internet services within a legal framework comparable to how traditional telephone services are regulated. In part due to the transnational nature of many internet services, this has not happened yet in Europe. Unless WhatsApp services should be regulated in the United States, as this an American company, it would be difficult or impossible for European countries to regulate the encryption services offered by WhatsApp. It would also be difficult or not possible to try to block WhatsApp services from using European internet networks.

3.6 Encryption of network services

Encryption of networked devices, like smartphones, gives law enforcement many of the same challenges as encryption of internet services. One recent example has been the San Bernadino case[ii], where the FBI tried to compel Apple to assist in unlocking an iPhone used by one of the attackers in the December 2, 2015, attack.

Apple had resisted a court order requiring them to provide new software to allow officials to access a phone. The request was limited to disabling the mechanism that locks the device if an incorrect password is entered repeatedly. This could enable the FBI to "guess" the password an unlimited number of times. Eventually, the FBI dropped the court case, as a third party company had offered software that could give possible access to the phone in question. According to several report, the access method used in this case, might not work in future cases, as Apple has updated the software for iPhones and increased the security.

This illustrates one difference between law enforcement access to telecom data compared to data from devices or services: telecom companies are typically required by national laws to set up their systems to make lawful interception possible. Law enforcement access to encrypted or protected devices and systems, depend on technical possibilities that may be unusable after future software updates or other changes.

Encryption of networked devices is to some extent related to encryption of internet services. Companies like Apple and Google offer a variety of services to their iPhones, iPads and Android devices. So while law enforcement may get access to some services as long as the phones use traditional telecom services, encryption makes it more difficult, and increasingly not possible, to get access to data stored on the devices. In various degrees, access to internet services used by the devices, is more difficult than access to telecom data, in part due to encryption of services, but also because jurisdiction issues connecting to cloud services makes it more time consuming for law enforcement to get access to the data in question.

4. Blocking and taking down of websites and social media accounts used for terrorist purposes

Websites, social media and other internet services may be used by terrorists and terrorist organisations for radicalisation, propaganda and communication. One challenge for law enforcement is to identify these channels for communication, as mentioned in the introduction. Some of these channels are based on encrypted "deep web" platforms. Others use publicly available services, like Facebook, Twitter, website hosting services etc. The so-called Islamic State has to some degree used the end-to-end encrypted messaging app Telegram for internal communication and for propaganda purposes.

Many countries have general provisions that could be used for certain actions against internet content, for example to seize internet domains within their own jurisdiction. For example, in the report "measures of Blocking, Filtering and Take-Down of Illegal Internet Content: The Netherlands" to the Council of Europe from A.R. Lodder & K.E. Sandvliet, Dep. Transnational Legal Studies, Center for Law & Internet at the Vrije Universiteit Amsterdam:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732764

"There is ***no specific regulation on issues of blocking, filtering, and take-down in Dutch law****. However,* ***a wide body of case law*** *exists, primarily based on the liability exemption for information society service providers as laid down in Article 196c book 6 Civil Code (implementation of EU Directive 2000/31/EC on e-commerce). (…)*

In general, illegal content can be taken-down, blocked or removed ***based on a court order****, which – following Article 196c(5) book 6 (6:196c) DCC – does not have to take into account the different 'roles' of the Internet service provider, meaning the ISPs that fall under the mere conduit provision also have to obey such an order. Notably, the hosting provider is the most common ISP asked to take down material. (…)*

The Dutch Code of Criminal Procedure (DCCP) has a special section for ***terrorist crimes****. For instance, Article 126zi DCCP indicates that suspicion is not necessary but mere indications of terroristic crimes suffice for an investigating officer to ask from an ISP information about name, address, ZIP code, and residence. Regarding filtering* *the government indicated this does not work adequately, since in case of terrorism unlawful content is not as evident as compared to e.g. child-pornography, resulting in a disproportionate interference with the right to freedom of speech."*

Blocking internet content, especially content from other jurisdictions, create different legal challenges.

Several countries in Europe have considered possible blocking and/or takedown of internet accounts used for terrorist purposes. For example, recent changes in French legislation, opened for takedown orders. This and similar legal instruments have been criticized by some, as a possible challenge to freedom of speech. One example in a statement from the OSCE Representative for Freedom of the Media, of March 30, 2015:

www.osce.org/fom/14276
"OSCE Representative on Freedom of the Media Dunja Mijatović said today that the unilateral decisions by the Interior Ministry in France, without judicial oversight, to block five websites for allegedly causing or promoting terrorism represents a serious threat to free expression and free media.

"Blocking websites without judicial oversight may endanger free expression and free media and creates a clear risk of censorship of online content by political bodies," Mijatović said.

The representative urged the French authorities to reconsider the parts of the anti-terrorist law enabling website blocking, which was passed in November last year. (…)

The representative also noted with concern legislative debates in several OSCE participating States over provisions with a similar potential impact on the freedom of expression. There include new criminal provisions approved in Spain regarding access to or dissemination of extremist content, and certain anti-terrorist provisions in proposed Bill C-51 in Canada."

These concerns could be reduced if website blocking could be done with judicial oversight, for example court orders, but freedom of speech would still be a potential challenge against content blocking.

Another challenge is of practical nature. If content is blocked, the source of the content may just move to a different internet forum, a new domain name or a different account on the same social network. This "whack-a-mole" problem is also known in connection to other types of internet content, from unapproved sharing of copyrighted content, to illegal distribution of child sexual abuse material.

In addition to national legal instruments, many internet services consider use by terrorist organisations etc. to be a violation of the user agreements. Court orders or national legislation may not be needed to remove content in violation of user agreements. February 5, 2016, the New York Times wrote:

www.nytimes.com/2016/02/06/technology/twitter-account-suspensions-terrorism.html?_r=0

[Twitter] had suspended 125,000 Twitter accounts associated with extremism since the middle of 2015, the first time it had published the number of accounts it has suspended. Twitter also said it had expanded the teams that review reports of accounts connected to extremism, to remove the accounts more quickly. (…)

The 125,000 suspensions could include users who have continued creating new accounts after previous ones are suspended, a common practice among ISIS supporters, experts said.

In a blog post on Friday, Twitter said violent threats and the promotion of terrorism had long been against its terms of service. For almost three years, Twitter has worked closely with groups that are trying to counter extremist tactics through positive messaging, the company said. Twitter said it decided to intensity its push against extremist posts on its own."

Another example of a service that has blocked some content and accounts based on user agreements and internal policies is Telegram, a service offering end-to-end encrypted chat and messaging services. In an interview with CNN February 23, 2016, Telegram founder Pavel Durov said that the company has never disclosed data, but that they have closed down some terrorist related content:

www.cnn.com/2016/02/23/europe/pavel-durov-telegram-encryption
"(…) Durov insists that the "overly simplistic solutions" suggested by intelligence services, blocking access to apps and allowing governments to break in to secure communications are not the answer.

"When you look into them, you realize that they wouldn't work and they would actually make the situation worse", he says. "Essentially they want companies providing encrypted messaging services to implement 'back door' solutions." The problem with that approach, he says, is that you cannot make messaging technology secure for everybody except terrorists. "You cannot make it safe against criminals and open for governments. It's either secure or not secure, he said. (…)

Durov says a number of governments – including that of Britain – have reached out to him for help in the past, but encryption means that even he can't access his user's messages.

"For two and a half years of our existence we haven't disclosed a single bite of data of our users," he says proudly. (…) Telegram has stepped in to shut down public channels on its app that were being used by ISIS – at the last count, the company says they have closed more than 600 of them.

"Every day four or five channels are reported by our users and we take them down", Durov explains."

The practices from services like Twitter and Telegram indicates that content blocking based on violation of user agreements may be easier to implement that blocking based in national laws.

Any conclusions or recommendations from CODEXTER, should take into account related, previous recommendations from The Council of Europe. The Council of Europe Steering Committee on Media and Information Society has given a Recommendation CM/Rec(2014)6 on a

Guide to human rights for Internet Users. This recommendation was adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies In the Appendix to this recommendation, filtering and blocking content is discussed:

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31

"49. Nationwide general blocking or filtering measures might be taken by State authorities only if the filtering concerns specific and clearly identifiable content, based on a decision on its illegality by a competent national authority which can be reviewed by an independent and impartial tribunal or regulatory body in accordance with the requirements of Article 6 of the ECHR. (…)

51. Filtering and de-indexation of Internet content by search engines entails the risk of violating the freedom of expression of Internet users. Search engines have freedom to crawl and index information available on the World Wide Web. They should not be obliged to monitor their networks and services proactively in order to detect possibly illegal content and should not conduct any ex-ante filtering or blocking activity unless mandated by a court order or by a competent authority. (…)

53. It is possible that companies, such as social networks, remove content created and made available by Internet users. These companies may also deactivate users' accounts (e.g. a user's profile or presence in social networks) justifying their action on non-compliance with their terms and conditions of use of the service. Such actions could constitute an interference with the right to freedom of expression and the right to receive and impart information unless the conditions of Article 10, paragraph 2 of the ECHR as interpreted by the Court, are met. (…)

55. The Guide alerts Internet users that online service providers that host user-created content are entitled to exercise different levels of editorial judgement over the content on their services. Without prejudice to their editorial freedom, they should ensure that Internet users' right to seek, receive and impart information is not infringed upon in accordance with Article 10 of the ECHR. This means that any restriction on user-generated content should be specific, justified for the purpose it is restricted, and communicated to the Internet user concerned. (…)
59. The Council of Europe's Committee of Ministers affirmed the principle of anonymity in its Declaration on Freedom of Communication on the Internet. Accordingly, in order to ensure protection against online surveillance and to enhance freedom of expression, Council of Europe member States should respect the will of Internet users not to disclose their identity. However, respect for anonymity does not prevent member States from taking measures in order to trace those responsible for criminal acts, in accordance with national law, the ECHR and other international agreements in the fields of justice and the police."

In a report to the Council of Europe Conference of Ministers responsible for Media and Information Society "Freedom of expression and democracy in the digital age" (Belgrade, 7-8 November 2013), Professor Ian Brown, University of Oxford, wrote (page 22-23):

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680484e7e
" Other difficult questions are raised for freedom of expression, assembly and association by State national security

and counter-terrorism programmes. The international law principles described by UN Special Rapporteur Frank La Rue are a useful starting point for consideration. He suggested for example that rules banning support for terrorist activities and organisations should only be used to justify restricting expression that is intended and likely to incite imminent violence, and never should apply to political debate, elections, reporting on human rights/government activities/corruption in government, peaceful demonstrations/political activities, and expression of opinion, dissent, religion or belief, including by minorities and other vulnerable groups.

The Committee of Ministers should consider recommending further procedural and substantive standards for "safe harbours" and other self and co-regulatory mechanisms (building on their Recommendations on filters, social networking and search engines), and to legal procedures that allow courts to order blocking - ensuring the impact on freedom of expression, assembly and association are fully taken into account. These could build on the Court's procedural standards deriving from Articles 6 (the right to a fair trial) and 13 (the right to an effective remedy), and the limits the Court has placed on interferences with the rights in Articles 8, 10 and 11, which must:

- *Be based on legal rules that are clear, accessible and foreseeable (and to the extent possible are set out in statute law);*
- *Meet a "pressing social need";*
- *Not be disproportionate to the purpose, nor ineffective;*
- *Have an "effective remedy", preferably judicial, if they do not meet these test."*

Regarding judicial control and effective remedies, it should be taken into account that a significant amount of the terrorist-related content that is the focus of takedown interest, may come from unidentified parties, in other jurisdictions, and that the amount might be significant. As mentioned above, from the middle of 2015 to February 2016, Twitter suspended 125,000 accounts associated with extremism. For social media services, blocking content is related to one account at the time.

If there should be a national, legal mechanism for blocking other internet content, such as websites hosted in other jurisdictions, there would probably be a need for ISP-level filtering. To make this type of content filtering effective, each country would probably have to implement both a legal mechanism that applies to all ISPs in their jurisdiction, and also make sure that all or at least a large majority of the ISPs actually have a technological system to facility website blocking.

Regarding "effective remedy" and the need for court orders, it could also be taken into consideration that this has not been raised as an issue for spam. As writer in the report from Lodder and Sandvliet mentioned above, *"If ISPs did not use spam filters, probably no one would use e-mail any longer."* Few if any of the parties responsible for sending out spam, send complaints to the ISPs or to local courts when their content is blocked by spam filters. Still, what one party may consider being terrorist activities on the internet, others might view as political statements, and political statements may have a higher degree of protection than commercial activities.

Another example, regarding de-linking of content, is currently being done by search engines like Google and Microsoft Bing, based on the "Right to be forgotten"-principle. Based on the ruling by the EU Court of Justice of 2014[iii], Google and Microsoft have set up the website https://Forget.me to receive requests to remove or de-link content from Google and Bing. Requests are processed by Google or Bing, not by any public authority, and their process is apparently not adversarial.

There is currently in place a filtering mechanism for child sexual abuse material, CIRCAMP[iv]. 14 European countries are part of this network, co-funded by the European Commission EC Safer Internet Programme. In theory, a similar approach could be used to block terrorist-related internet content, but this would probably have to be done as a separate initiative, not as an extension of the current programme.

Internet content filtering is not uncontroversial. One counter argument is that it is not workable; another is that an effective filtering system would be comparable to the so called "Great Firewall of China"[v]. A very wide ranging filtering of internet content would not be acceptable in a European context, due to possible restrictions on freedom of speech and concerns about censorship. On the other hand, more targeted and purpose-limited filtering or blocking of content might be acceptable, based on the principles and approaches described above.

Before the issue of blocking or removing content, it should be considered what kind of content this applies to, how and where this content is published or distributed, and also if blocking or filtering is feasible. Different situations may require different technological and legal solutions. Some examples on unwanted content being removed, blocked, filtered or de-linked without a public adversarial process include

- Spam: flagging and/or removal by ISPs, e-mail providers and/or services like Spamhaus.
- Privacy violations: de-linking by search engines, based on complaints.
- Content in violation of user agreements: suspension of accounts, decided by social media companies, web site hosts etc.

On the other hand, one should be careful to extend these practices too far. Freedom of speech; freedom to access information; due process and public transparency are basic rights and basic expectations from the public in Europe. This also applies to challenging and problematic material and content.

5. Jurisdiction issues related to data stored in other jurisdictions, including "the Cloud"

Stored computer data may be relevant as evidence in criminal investigations, including terrorism investigations. Different types of data may be of interest as possible evidence:

- Subscriber information;
- Traffic data;
- Content data.

There are several different types of internet-related providers, including:

- Telecoms
- Social media and e-mail companies (Facebook, Microsoft, Google, VK etc.)
- Website hosting companies
- Internet registrars
- Proxy, VPN and other anonymity service providers
- Internet financial service providers (PayPal, Western Union, TransferWise etc.)

Access to these kinds of data, especially when these are stored and processed by internet connected services, create several questions regarding jurisdiction, including:

- Nationality/location of the victim
- Nationality/location of the suspect
- Headquarter for the company processing the data
- Other offices for the company processing the data, for example a regional data controller office
- The physical location of the server where data is stored
- Multi-tiered solutions

All these possible solutions are today used by different countries, different companies and different legal sectors. For law enforcement access to data in criminal investigations, including in terrorism cases, jurisdiction may be decided differently in different contexts.

Several large companies offering services on the internet are based in the United States. Getting access to data from the United States for law enforcement in European countries may both be easier and more difficult compared to getting access to data from other European countries. Large companies like Google, Facebook, Microsoft and Apple have dedicated teams for law enforcement requests and often publish law enforcement guidelines. These guidelines may be a bit different from one company to another. The solutions may also be different for smaller companies or for companies in sectors like website hosting.

- Subscriber information is often available via direct requests to the company in question, based on American law and company practices.
- Content data (e-mail, chat logs, stored photos and documents etc.) is typically only available through requests for mutual legal assistance, and after a U.S. court order, but the data in question may be temporarily preserved after a direct request, cf. the Cyber Crime Convention (the Budapest Convention) Article 29.

Many larger internet companies publish transparency reports, with descriptions and statistics describing requests from law enforcement. Some examples:

- Google: https://www.google.com/transparencyreport/

- Microsoft: https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/
- Facebook: https://govtrequests.facebook.com/

Many telecom companies also provide similar transparency reports. Telecom data is regulated by other provisions than data from companies offering internet services. Unlike companies providing other internet services, the telecom companies typically only provide data to law enforcement within their own jurisdiction, and cannot provide data from subsidiaries or related companies in other jurisdictions. Companies like Vodafone and Deutsche Telekom have published transparency report for their different subsidiaries and related companies, country by country.

- Vodafone:https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html
- Deutsche Telekom: https://www.telekom.com/dataprotection and https://www.telekom.com/transparency-report

In the 2014 report, Deutsche Telekom stated: https://www.telekom.com/corporate-responsibility/data-protection/transparency-report/297130
"Deutsche Telekom does not respond to inquiries from authorities outside of Germany. Any inquiries of this nature must be submitted to Deutsche Telekom via the relevant German authority."

Although this is not mentioned in the 2015 report, this may not reflect a change of practice.

The National Institute of Standards and Technology (NIST) in the U.S defined cloud computing as *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

One of the basic characteristics of cloud computing, is that the data may be stored and accessed from different locations. In practice, data can be stored or accessed worldwide, and data can be moved rapidly. In many cases, the end user may not be aware of where the data is stored.

The Council of Europe (T-CY) has an on-going work on these issues. A working group, The Cloud Evidence Group, will present a final report in November 2016. In a discussion paper from the Cloud Evidence Group to the CoE Cybercrime Convention Committee of May 26, 2015[vi], one challenge for law enforcement is described:

"Cloud computing" means that data is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions:"

The document then refers to a draft report from the NIST, "Cloud Computing, Forensic Science Challenges" (see Chapter 4, Preliminary Analysis):

http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf
"In traditional computer forensics, due to the centralized nature of the information technology system, investigators can have full control over the forensic artefacts (router, process logs, hard disks). However, in the cloud eco system, due to the distributed nature of the information technology systems, control over the functional layers varies among cloud actors, depending on the service model. Therefore investigators have reduced visibility and control over the forensic artefacts. "

In addition to these technological challenges, there are several practical and legal challenges. These are not unique for cloud computing, but the transborder nature of cloud computing increases the challenges. One issue is time. Access to data in other countries often depends on mutual legal assistance. These processes are based on old practices, and typically use paper based documents sent via several parties by traditional mail. Even with international instruments like the Budapest Convention and various European instruments and cooperative efforts, it takes time from a request is sent to the data in question is available. In many cases, the requested data is just a part of a longer chain of evidence, and one piece of evidence may require new requests to other jurisdictions. In the above mentioned discussion paper from the T-CY, the Cloud Evidence Group stated:

"Mutual legal assistance remains the principal means to obtain evidence from foreign jurisdictions for use in criminal proceedings. In December 2014, the Cybercrime Convention Committee (T-CY) completed an assessment of the functioning of mutual legal assistance provisions. It concluded, among other things, that:

The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.

The Committee adopted a set of recommendations to make the process more efficient. These recommendations should be implemented.

At the same time, MLA is not always a realistic solution to access evidence in the cloud context for the reasons indicated above."

6. <u>The identification of physical/legal persons behind IP addresses used for terrorist purposes</u>

In a Council of Europe T-CY report of December 3, 2014, the importance of IP addresses in criminal investigations is described in the introduction, (Section 1, page 4).

http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
"Obtaining information from Internet Service Providers to identify a user (subscriber) of a specific Internet Protocol (IP) address at a specific time or, vice versa, to identify the IP addresses used by a known person 1 is crucial

for criminal investigations and proceedings related to cybercrime and electronic evidence. Subscriber information is also the most often sought data in the context of international cooperation. (…) IP addresses may be considered subscriber information – as opposed to traffic data – if the purpose is to obtain the identification of a subscriber in relation to an IP address. "

From the conclusions (Section 3, page 28):

" In conclusion:

- *most Parties differentiate between subscriber information and traffic data;*
- *in some countries, the interference with the rights of individuals is considered to be substantially different when obtaining subscriber information, including in relation to an IP address, in a specific criminal investigation on the one hand, and traffic data on the other;*
- *consequently, in those countries, different rules should apply for obtaining such information;*
- *conditions for obtaining subscriber information are rather diverse in the Parties at this point;*
- *however, more harmonized rules for obtaining subscriber information would facilitate international cooperation.*
- *It is recommended that the T-CY:*
- *facilitate greater harmonization between the Parties on the conditions, rules and procedures*
- *for obtaining subscriber information;*
- *encourage Parties to take account of the observations of this report when reforming their domestic regulations."*

Different countries and different jurisdictions have differences regarding legal provisions and regulations regarding lawful access to subscriber information. These differences may make it more difficult and more time consuming to identity the customer behind and IP address. Another issue is that different companies and different technology sectors may have a variety of practices regarding storing subscriber information and user logs, regarding what kind of information is required to open an account at a service provider, regarding information sharing between companies and their partners, resellers etc.

- Telecom providers: often national regulation, for example to require correct and complete user information, physical address, payment information etc.
- Social media and e-mail providers: largely unregulated
- Website hosting companies: largely unregulated
- Internet registrars: largely unregulated
- Encryption and anonymizing services: largely unregulated

One regulation that does exist for all processors of personal data is data protection regulations. One example is the EU Data Protection Directive, 95/46/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1995.281.01.0031.01.ENG

According to Article 6 (c), personal data must be *"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"*. This principle may also apply to subscriber information and IP logs. The Norwegian Data Protection Authority ruled in 2009 that two internet service providers had to delete the IP logs of their customers after up to 21 days, because further storing or use of this set of data was not necessary for billing purposes or other purposes that they were collected for.

Data retention is one way of keeping information that makes it possible to "push the rewind button" and try to connect IP logs to identifiable users. After a decision by the EU Court of Justice of April 8, 2014, the EU Data Retention Directive was declared invalid.

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

After this decision, various EU countries have come up with different solution. Some have implemented national data retention laws, while others have no data retention in place. This situation makes it more difficult for law enforcement to follow data back to an identifiable end user.

With wireless networks and other shared networks, one IP address may be shared among many users. Proxy services and anonymizing services makes it more difficult, or even impossible, to follow an IP address all the way back to the user. At best, identification requires one or several extra steps through various providers. One simple example:

http://people.opera.com/howcome/2009/unlikely-places/

" In January [2009], the Chicago Transit Authority noticed that lots of Norwegians Web users were tracking buses in Chicago online. (…) It's more likely that these «Norwegians» were Opera Mini users who happened to use Opera's server farm in Oslo. Bits find their way to and through unlikely places."

Another challenge is the migration to new internet technology. According to the Europol Internet Organised Crime Threat Assesment (IOCTA) 2014:

https://www.europol.europa.eu/iocta/2014/chap-4-3-view1.html

"The number of available IPv4 addresses is rapidly diminishing. Migration to the IPv6 protocol – which offers a virtually unlimited number of IP addresses - is in progress but likely to take a considerable amount of time to implement. This means that, during this transition period – which may last several years or more – alternative ways to assign IP addresses are deployed by operators in order to ensure the continuity of Internet traffic in a growing market. The intermediate solution known as a 'Carrier Grade Network Address Translation Gateway' (CGNAT), is now being used by Internet service operators in the EU.

The ability to link users to an IP address is crucial in the context of a criminal investigation. Where the CGNAT is used, multiple devices are connected on a local network with only one single IP address. ***Potentially, this technology enables providers to link thousands of users per IPv4 address and the ability to identify individual users is therefore significantly impaired.*** *The identification of users would require the retention of this data and its provision to LE by Internet operators."*

7. Conclusion

Terrorist use of internet services and infrastructure is an international challenge. Few international instruments deal specifically with this challenge. Instruments like the Budapest Convention are relevant for police cooperation against terrorism and electronic evidence. Several challenges remain, in part technological challenges, but also challenges due to current time consuming practices regarding mutual legal assistance.

Data protection and privacy issues should be always taken into consideration and balanced, as described by the European Court of Human Rights in the case of K.U. vs. Finland (Application no. 2842/02):

https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/K.U.%20v.%20FINLAND%20en.pdf

"49. (…) An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."

8. Recommendations to CODEXTER

The CODEXTER members are invited to take into consideration the following recommendations:

- To continue to follow closely the subject of "terrorism and the Internet" in order to address the issue also when analysing other developments, such as foreign terrorist fighters, terrorist training, financing of terrorism and terrorists acting alone.
- In line with the Council of Europe Strategy on Internet Governance (2016 – 2019), examine the feasibility of engaging with major Internet companies through a platform to be established under the aforesaid Strategy (paragraph 13, e).

Other relevant areas may, of course, be identified by CODEXTER during its deliberations.

****

[i] List of international conventions related to terrorism:

1 Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on 16 December 1970;

2 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, concluded at Montreal on 23 September 1971;

3 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, adopted in New York on 14 December 1973;

4 International Convention Against the Taking of Hostages, adopted in New York on 17 December 1979;

5 Convention on the Physical Protection of Nuclear Material, adopted in Vienna on 3 March 1980;

6 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, done at Montreal on 24 February 1988;

7 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, done at Rome on 10 March 1988;

8 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988;

9 International Convention for the Suppression of Terrorist Bombings, adopted in New York on 15 December 1997;

10 International Convention for the Suppression of the Financing of Terrorism, adopted in New York on 9 December 1999;

11 International Convention for the Suppression of Acts of Nuclear Terrorism, adopted in New York on 13 April 2005.

[ii] https://en.wikipedia.org/wiki/2015_San_Bernardino_attack

[iii] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[iv] http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking

[v] https://en.wikipedia.org/wiki/Golden_Shield_Project

[vi]https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59