Uniting forces against cyber challenges of terrorism

exchange of best practices

E-BOOK

This project was funded by the European Union's Justice Programme (2014-2020)

Preface

The use of cyberspace for terrorist activities as well as traditional and new forms of crimes create a complex environment and challenges for authorities dealing with crime investigation. The ever changing technology and technical developments in the field of communication tools and encryption of that communication (E2EE), the nature of the threat, the location of the crime scene, the anonymity of the worldwide web, the cross border aspect of these crimes, the substantive and procedural legal problems, the complex laws and difficulties, the time consuming information exchange, the conflict of legislations, the transmission of digital evidence, absence of internationally agreed framework for retention of data held by ISPs of are some of the challenges that countries and stakeholders are facing on a daily basis which significantly weakens terrorism research.

Therefore, practical approaches need to be found to make an efficient cooperation and communication possible between the police, the judiciary and other actors in relation to cyberspace-based terrorist activities and terrorist use of internet, and concentrate on specific problems they face on their daily activities and improve the exchange of information and best practices of different member states. This will enable them to counter the fluid, dynamic and organized use of cybercrime by terrorists.

This eBook is the outcome of an international seminar organized on this topic by the Judicial Training Institute (Belgium) in conjunction with Ecole nationale de la Magistrature France ENM; Scuola Superiore della Magistratura (SSM, Italy); Studiecentrum Rechtspleging (SSR, Netherlands); Krajowa Szkola Sadownictwa I Prokuratury (National School of Judiciary and Public Prosecution, KSSIP, Poland); National Institute of Justice Bulgaria (NIJ, Bulgaria) and Prosecutor office of Estonia and with financial support from the European Commission's Directorate-General for Justice.

We’d like to thank everyone involved in the making of this e-book

COLOPHON

Project: This eBook is the outcome of an international seminar organized by the Judicial Training Institute (Belgium) in conjunction with the Ecole nationale de la Magistrature France ENM; Scuola Superiore della Magistratura (SSM, Italy); Studiecentrum Rechtspleging (SSR, Netherlands); Krajowa Szkola Sadownictwa I Prokuratury (National School of Judiciary and Public Prosecution, KSSIP, Poland); National Institute of Justice Bulgaria (NIJ, Bulgaria) and Prosecutor office of Estonia and with financial support from the European Commission's Directorate-General for Justice. This eBook includes interviews, videos of the seminar, the presentations of the speakers at the conference and conclusions of the seminar. The presentations reflect the situation at the moment of this seminar.

Category:/Collection: International / Uniting forces against cyber challenges of terrorism exchange of best practices

Client: DG Justice European Union's Justice Programme (2014-2020) JUST-JTRA-EJTR-AG-2017-807049

Responsible editor: Mr. Raf Van Ransbeeck

Final revision: IGO-IFJ

Language version: English

Brussels, © Judicial Training Institute, January 2020.

Contact

Belgian judicial Training Institute (IGO-IFJ)

Louizalaan - Avenue Louise 54

1050 Brussel - Bruxelles

TEL +32(2)518 49 61

info@igo-ifj.be

www.igo-ifj.be

Disclaimer

This project/report/publication was funded by the European Union's Justice Programme (2014-2020), G.A. no 807049; The content of this report represents only the views of the authors. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Judicial Training Institute or the partners.

Terms of use

Reproduction of the texts of this report, except for commercial purposes, is authorized with the permission of the speakers of the seminar and of Judicial Training Institute.

INDEX

This project was funded by the European Union's Justice Programme (2014-2020)

Uniting forces against cyber challenges of terrorism - exchange of best practices

Opening Speech Mr. Raf VAN RANSBEECK, Director of the Belgian Judicial Training Institute

Ref.: INT/2019-139

22 October 2019

This seminar is organized by the Judicial Training Institute (Belgium) in conjunction with Ecole nationale de la Magistrature France ENM; Scuola Superiore della Magistratura (SSM, Italy); Studiecentrum Rechtspleging (SSR, Netherlands); Krajowa Szkola Sadownictwa I Prokuratury (National School of Judiciary and Public Prosecution, KSSIP, Poland); National Institute of Justice Bulgaria (NIJ, Bulgaria) and Prosecutor office of Estonia and with financial support from the European Commission's Directorate-General for Justice.

Dear Colleagues,

As the director of the Belgian Judicial Training Institute and on behalf of all the partners of this project, it is my great honour and a pleasure to welcome you all at this European seminar on "Uniting forces against cyber challenges of terrorism – exchange of best practices", which is funded by the European Union's Justice Programme (2014-2020).

I am proud to say that in collaboration with our partners, we have delivered a high quality programme. This three day seminar combines two subjects which are crucial today: cybercrime on the one hand and terrorism on the other.

Today, besides the positive benefits, internet technology and cyberspace are also a playground for traditional crimes such as prostitution and trafficking of

This project was funded by the European Union's
Justice Programme (2014-2020)

illegal drugs. And new forms of criminality have emerged such as phishing and the use of internet for terrorist purposes.

One thing is for sure: the technology is here and it is here to stay. But we don't know yet where the applications of these technologies will end and, more importantly, to which ends they will be used.

The European Union has recognised the need to combat the terrorist use of Internet and has adopted legislation due to the significant role Internet plays in the logistic, operational and communication activities of terrorist organisations. Be it for encrypting their messages or renting cars or apartments.

Last month, the UN Secretary-General, Mister Antonio Guterres, stressed the importance of cross border cooperation when he said that "international cooperation is the first priority of all counterterrorist strategy." According to him "countries need to cooperate with one another as well as with partners including the private sector and civil society to successfully address those challenges".

He further stated that the new threat is "cyber-terrorism". In that regard, he did not only touch upon the need for a common and global approach, he also highlighted the importance to "complement security measures with prevention efforts that identify and address root causes, while always respecting human rights."

Indeed, a global and lawful approach is indispensable. This does not only mean collaborating among judicial authorities, it also involves joining forces with private partners. In the words of the former European Commissionner, Julian King: *« Si l'on veut aider les citoyens et toutes les entités concernées à être plus responsables, il faut impliquer aussi les géants du Net »*.

As most of you witness every day, the use of cyberspace for terrorist activities as well as traditional and new forms of crimes has created a complex environment

This project was funded by the European Union's
Justice Programme (2014-2020)

and challenges for authorities dealing with crime investigation: a virtual component has been added to the location of the crime scene, perpetrators are acting both in the real world and in the world wide web, the laws and the legal problems have become more complex due to cross-border activities and information exchange has become more timeconsuming.

That is why, in cooperation with internal and external partners and with the funding of EU, we have created this high quality and practice oriented programme. The purpose of the programme is to give you a thorough understanding of the international legal framework, to explain the existing tools combatting cybercrime, to give you an overview of challenges and to exchange best practices between colleagues from different members states in the fight against cyber-terrorism.

In order to offer you a substantively strong and a up-to-date programme, we have invited 14 leading experts, who will give you more insights in the European an international framework. They will also guide you through the technical developments in the field of communication and help you search for common legal grounds.

To give you a broad overview of the topic we have invited experts with broad profiles: you will not only meet experts from judicial authorities, you will also meet professionals from internet providers who will tell you their side of the story. Among the speakers we are also proud to welcome experts from the US.

And of course, this programme wouldn't be possible without your presence and interactive support. To facilitate the exchange of information between the different authorities, we have brought together 88 judges and prosecutors from all the corners of the EU and also from Albania, whose participants we welcome very warmly.

This project was funded by the European Union's Justice Programme (2014-2020)

The documentation, presentation and the recommendations that you will share this week will be published in a restricted e-book. It will collect this week's best-practices and will serve as a useful guide for you and many other experts in Europe dealing with similar cases related to cyber-terrorism.

Let me finish by thanking the many project partners involved in this training seminar:

- First of all , the European Union for sustaining and funding this programme.
- Then our partners involved in this project with whom we are cooperating for many years
    - The Ecole nationale de la Magistrature in France;
    - The Studiecentrum Rechtspleging in the Netherlands;
    - The Scuela Superiora della Magistratura in Spain;
    - The National School of Judiciary and Public Prosecution in Poland;
    - The National Institute of Justice in Bulgaria;
    - The Prosecutor's Office in Estonia.
- The Belgian Working group and all the members of the Scientific committee who designed and advised on the program
- The many speakers from and outside the EU who will share their experience with you.
- Our Belgian project team: Axel, Karin, Jos, Umit Luisa and Thomas for the support during the next days.
- And last but not least, you all for contributing to a strong and safe Europe.

I hope that you will enjoy the time you will spend together this week and I wish you all a very fruitful seminar.

Now it is my pleasure to give the floor to the deputy director of our Belgian institute, Mr Axel Kittel.

OPENING

Raf Van Ransbeeck

Director of the Belgian Institute of Judicial Training (IGO-IFJ)

WATCH THE VIDEO

INTERVIEW

Erik PLANKEN

Ministry of Justice of the Netherlands and former chair of the

Cybercrime Convention Committee

WATCH THE VIDEO

Interview

Uwe RASMUSSEN

Legal Director, Magnusson

WATCH THE VIDEO

Interview

Alexandra LINK

Trial Attorney, Cyber Team , U.S. Department of Justice

WATCH THE VIDEO

Interview

Janey YOUNG

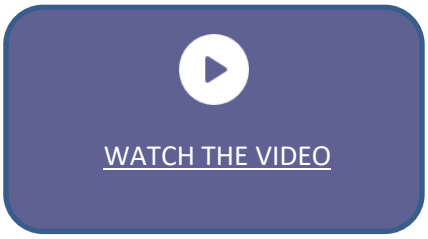
Europol's European Cybercrime Centre (EC3), Team Leader – Dark Web Team

WATCH THE VIDEO

Interview

Eric FILIOL

Professor in the field of information and systems security at ENSIBS, France



Interview

Jan KERKHOFS &

Federal Magistrate, at Federal Prosecutor's Office, Organized Crime Section,

Cyber Unit

Philippe VAN LINTHOUT

Investigating Judge specialised in terrorism cases, Court of First Instance Antwerp, Division Mechelen

Uniting forces against cyber challenges of terrorism - exchange of best practices

PROGRAM

This seminar is organized by the Judicial Training Institute (Belgium) in conjunction with Ecole nationale de la Magistrature France ENM; Scuola Superiore della Magistratura (SSM, Italy); Studiecentrum Rechtspleging (SSR, Netherlands); Krajowa Szkola Sadownictwa I Prokuratury (National School of Judiciary and Public Prosecution, KSSIP, Poland); National Institute of Justice Bulgaria (NIJ, Bulgaria) and Prosecutor office of Estonia and with financial support from the European Commission's Directorate-General for Justice.

Ref.: INT/2019-139

Rapporteur: **Robrecht DE KEERSMAECKER**, Deputy Prosecutor General

---

1. Tuesday 22 October 2019

During the afternoon and evening: arrival of the participants at the **Silva Hôtel Spa-Balmoral Balmoral 33, 4900 Spa** www.silvahotelspabalmoral.be

18:30 Check-in

19:00 Welcome by **Raf VAN RANSBEECK**, Director of the Belgian Institute of Judicial training, and by Axel **KITTEL,** Deputy Director of the Belgian Institute of Judicial training institute followed by a reception

19:30 Opening diner with Belgian gastronomic specialty

---

2. Wednesday 23 October 2019

08:30-09:00 Check-in

09:00 Opening of the seminar, welcome of the participants and overview of the three days of the conference by **Raf VAN RANSBEECK**, Director of the Belgian Institute of Judicial

Training and by **Axel KITTEL,** Deputy Director of the Belgian Institute of Judicial training institute

Chair of the seminar: **Axel Kittel,** Deputy Director of the Belgian Institute of Judicial training institute

09:10-09:55 Theoretical approach: **International legal framework for European countries regarding combating** terrorism by **Jeroen BLOMSMA**, Policy officer European Commission DG Migration and Home Affairs – Counter Terrorism

- European Counter terrorism directives
- Legal tools for judicial cooperation regarding terrorism
- Challenges in counterterrorism

10:00-11:00 Practical approach: **Overview of challenges** – interactive presentation (in plenary session) by **Philippe VAN LINTHOUT** , Investigating Judge specialised in terrorism cases, Court of First Instance Antwerp, Division Mechelen and **Jan KERKHOFS,** Federal Magistrate, at Federal Prosecutor's Office, Organized Crime Section, Cyber Unit

- (Lack of) International cooperation:
  - Jurisdiction and cross-border gathering of digital evidence
  - Public-private cooperation
- Data Retention
- Encryption of the data carrier (device) and of the communication

11:00-11:30 Coffee break

11:30-12:00 Theoretical approach: **The Budapest Convention and its toolbox regarding fighting cybercrime used for terroristic purposes** by **Erik PLANKEN** from the Ministry of Justice of the Netherlands and former chair of the Cybercrime Convention Committee

12:00-13:20 Practical approach: **The gathering of digital evidence in an international context using the Budapest Convention** by **Jan KERKHOFS,** Federal Magistrate, at Federal Prosecutor's Office, Organized Crime Section, Cyber Unit and **Philippe VAN LINTHOUT** , Investigating Judge specialised in terrorism cases, Court of First Instance Antwerp, Division Mechelen

- The Budapest Convention toolbox
  - Spontaneous information sharing
  - Cross-border
  - 24/7
  - Art. 18 of the Convention
  - Jurisdiction and cross-border gathering of digital evidence
  - Yahoo (and Skype) case as a case study

13:20-13:30 Question time
13:30-14:30 Lunch time
14:30-15:30 State of the play on investigation side, confronted with the service providers abroad

- **Obtaining Electronic Evidence from the United States,** by **Alexandra LINK,** Trial Attorney, Cyber Team , U.S. Department of Justice
- **Belgian example** by **Juan CORRIAT** Chief Officer, DSU-NTSU-CTIF
- **"The Italian job"** by **Francesco CAJANI,** Public Prosecutor at the Prosecutor's Office in Milan, High Tech Crime Unit – Counter terrorism Department
    - Cooperation with the ISP's in an emergency situation
    - The WhatsApp case

15.30 Coffee break in the seminar room
15:45- 16:45 **Cooperation with internet providers**

- **Challenges of obtaining evidence from abroad by Uwe RASMUSSEN,** Legal Director, Magnusson
- **Trust & Safety at Facebook: Processes and policies related to support of criminal investigations and response to legal requests** by **Tim FAGAN** Trust and Safety Manager, EMEA, FACEBOOK

16:45-17:00 **Q&A**

17:30 Departure for Stavelot Abbey
18:00 Visit of the National Museum of Formula 1 and aperitif
19h30 Dinner in the Stavelot Abbey

---

3. Thursday 24 October 2019

09:00-10:30 **State of the play on investigation side:**

- **The EU strategy for tackling crime on the dark web** by **Janey YOUNG**, European Cybercrime Centre, Team Leader - Dark Web Team
- **Encryption of the data carrier (device) and of the communication** by **Francesko COLLAT**, Cyber ALAT
- Q&A

10:30-10:50 Coffee break

10-50- 11.30 **Criminalization of online terrorism self-study** by **Antoon SCHOTSAERT** ,Federal Magistrate , Belgian Federal Prosecutor's Office, Counter terrorism Unit

11:30-12:30 **Follow the money – crypto-currencies** (block-chain analysis, tracking, how to break mixers,…) by **Pawel PIK**, Prosecutor at the Regional Prosecutor's Office in Gdansk Financial and Tax Crimes Department

12:30-13:00 Presentation o**f the practical cases and methodology of the workshops by Jan KERKHOFS, Philippe VAN LINTHOUT and Antoon SCHOTSAERT** (see titels above)

l13:00-14:00 Lunch

START OF THE WORKSHOPS

14:10-15:50 Start of the workshops (introduction to the workshop will be made by its moderator)

15:50-16:15 Coffee break

16:15-16:45 Workshops (4 break out rooms)

16:45-17:00 Report in plenary by representatives of the different working groups
Question time and conclusions of the workshops

17:30 Departure for the Domaine de Berinzenne
18:00 Free walk in the wood
19h00 Dinner in the Berinzenne lodge

4- Friday 25 October 2019

09:00-09:45 **Take down terrorist propaganda** by **Alberto GARCIA MORALES** , Team Leader, Operations Department ECTC, Internet Referral Unit, Team Leader, EUROPOL

9:45-11:00 **Recent developments and Trends on the concept of cyber terrorism** by **Eric FILIOL**, professor in the field of information and systems security at ENSIBS, France

11:00-11:15 Coffee break

(Recommendations will be drafted after the seminar by the scientific committee.)

11:15-12:00 Prosecutor challenges and aspirations in cyberterrorism by **Frédéric VAN LEEUW**, Belgian Federal Prosecutor, Federal Prosecutor's Office

12:00-12:30 Conclusions of the Seminar

12.30- 14:30 Lunch

End of the seminar

DOCUMENTATION

Philippe VAN LINTHOUT

Investigating Judge specialised in terrorism cases, Court of First Instance Antwerp, Division Mechelen

WATCH THE VIDEO

WATCH THE DOCUMENTION (PDF)

Documentation

Erik PLANKEN

Ministry of Justice of the Netherlands and former chair of the

Cybercrime Convention Committee

WATCH THE VIDEO

WATCH THE DOCUMENTATION

(PDF)

Documentation

Jan KERKHOFS

Federal Magistrate, at Federal Prosecutor's Office, Organized Crime Section,

Cyber Unit

WATCH THE VIDEO

WATCH THE DOCUMENTION (PDF)

WATCH THE DOCUMENTION (PDF)

Documentation

Juan CORRIAT

Chief Officer, DSU-NTSU-CTIF

WATCH THE DOCUMENTION (PDF)

Documentation

Francesco CAJANI

Public Prosecutor at the Prosecutor's Office in Milan, High Tech Crime Unit – Counter terrorism Department

WATCH THE DOCUMENTION (PDF)

Documentation

Uwe RASMUSSEN

Legal Director, Magnusson

WATCH THE VIDEO

WATCH THE DOCUMENTION (PDF)

Documentation

Tim FAGAN

Trust and Safety Manager, EMEA

WATCH THE DOCUMENTION (PDF)

Documentation

Janey YOUNG

Team leader, AP Dark Web European Cybercrime Center (EC3)

WATCH THE DOCUMENTION (PDF)

Documentation

Pawel PIK

Prosecutor at the Regional Prosecutor's Office in Gdansk Financial and Tax Crimes Department

WATCH THE VIDEO

WATCH THE DOCUMENTION (PDF)

Documentation

Eric FILIOL

Professor in the field of information and systems security at ENSIBS, France

WATCH THE VIDEO

WATCH THE DOCUMENTION (PDF)

Documentation

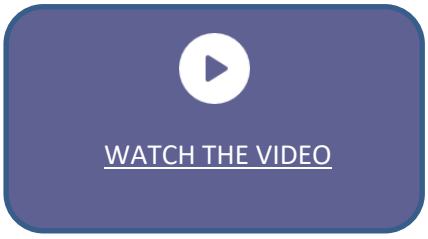
Frédéric VAN LEEUW

Belgian federal Prosecutor, Federal Prosecutor's office

Documentation

Antoon SCHOTSAERT

Federal Magistrate, Belgian federal Prosecutor's Office, Counter terrorism Unit



This project was funded by the European Union's Justice Programme (2014-2020)

Uniting forces against cyber challenges of terrorism - exchange of best practices

WORKSHOP SCENARIO

There has been a mass shooting in a mosque in New-Zealand, with more than 50 casualties as a result. The attack was performed by a white supremacist who wanted to hit hard on the Muslim community. From intelligence services you receive the information that a person in your country could be identified as a suspect who made a video which was distributed via the Telegram channel *@greenbird* (an IS linked channel), in which he announces to retaliate on behalf of IS with a suicide attack in a public place somewhere in Europe. The video shows images of an AK47 and a bomb belt which seems to be professionally put together. OSINT investigation could not determine if the images of AK47 and the bomb belt or recuperated from already existing images on the internet. The Telegram profile of the suspect could be linked to a mobile phone number +32 487 45 67 43 (Belgian) in the database of Europol which was previously detected in a Spanish CT investigation. Telecommunication investigation shows that the number is a prepaid and is no longer activated (out of use since 12 September 2018, no identification possible).

The suspect presumably could be identified as the named J.L., 22 years old, last known to be living in your capital. Currently he is under the radar, without fixed address. With OSINT he can be linked to a Facebook profile named 'Paradise lost' on which he posted two months ago a picture of himself with the raised index finger with reference to the Shahada. The picture is posted with the comment that 'Europe must suffer and pay'. No other recent FB activity is detected. The EXIF-data of the picture could be interesting since the picture looks to be taken in a living room somewhere. A request to Facebook leads to the IP address 86.105.22.100 (Romanian); the IP address is used on 2018-09-11 11:30:47 UTC to create the FB profile. The *basic subscriber information* received from FB also shows the mobile number +32 487 45 67 43 and the gmail account paradiselost97@gmail.com. A request to Google leads to an identifiable IP address in your capital; on the identified address live according to the national registry 2 people: B.M. and C.J. According to confidential information from State Security, B.M. and J.L. visited a few months ago the same radicalized mosque where the *salafiya jihadiya* was being preached. B.M. was photographed with Abu Jihad Al Belgiki.

Finally a house search is initiated. J.L. and B.M. are present and arrested. The bathtub has traces of what later will be identified as TATP. Seven AK47 chargers can be seized, as well as a flag of IS in the living room. J.L. is in the possession of an iPhone X, B.M. carries an iPhone 7plus. They discover in the living a laptop which is locked. On the keyboard there is a post-it which mentions "AbuJihad26", which could be a password. There is also a desktop in the living; B.M. was behind it when entering the apartment and he just performed a complete wipe of all the data, in which he succeeded. In the bedroom of C.J. there is a desktop running, which is unlocked. When they touch the keyboard, the screen opens and they see an opened Yahoo account, and a Telegram desktop application which shows several group chats. They also find the following, what looks like a 'seed' of a bitcoin wallet:

J.L. and B.M. are asked to give the code of their iPhones. They refuse. The police asks the magistrate in charge of the investigation for a warrant ordering them to disclose their passwords. The magistrate decides to not do that, even though he says it is legally possible; he doesn't believe they will cooperate

and time is ticking since it is not known where the TATP is and where C.J. is. He orders to hold the iPhone X before the face of J.L. in order to open the phone with face recognition. He also orders to use proportionate force to put the fingers of B.M. on the key button of his iPhone 7plus in order to open the phone. The lawyer of B.M., who arrived meanwhile, objects and says the fundamental right of his client are being infringed because he cannot be forced to incriminate himself and that he has the right to remain silent. The magistrate does not agree and they use force on B.M. to take his fingerprint (he is handcuffed and the police just use the immobility of his hands to take his fingers for this purpose). The iPhone 7plus is opened and they see that he has the 'BRD' app on his iPhone (bitcoin wallet). The police taps on the app but it seems that it is password protected to enter.
J.L. is being interviewed and he finally decides to collaborate with the judiciary. He declares that C.J. is the organizer and recruiter and that C.J. is in contact with high ranked people within IS and that they received funding to buy arms (AK47's) on the darkweb, as well as ammunition and ingredients for explosives. The funding was being done with virtual currencies. According to J.L. a sum of 5 bitcoins was put at their disposal (1 BTC = 7.150,80 EUR @ 18/10/2019). He doesn't know how to access the BTC wallet, he says B.M. does; B.M. still refuses to collaborate. Since J.L. is cooperating, he also gives the written voluntary consent to enter the mentioned full Yahoo-account (which was according to J.L. a shared account) and the connected Flickr account which contains a mass of propaganda material. The Yahoo account contains communication on an attack in preparation.
C.J. is finally arrested too, but denies everything and stays silent.
The three of them are on trial.
J.L. confesses and also incriminates B.M. and C.J.
B.M. says his fundamental rights are violated because he was forced to witness against himself. He also says that the voluntary consent of J.L. to enter the Yahoo account and Flickr account do not apply to him. According B.M., J.L. could not give consent since the accounts were also used by him. B.M. also says that the picture with him and Abu Jihad Al Belgiki has been photoshopped by the police.
C.J. says nothing, except that B.M. is anyway right to say that the procedure is not respected.
Basically, according to B.M. and C.J., J.L. is a bad friend who had been offered shelter and abused their hospitality. They say he was a lone wolf who

LINK WORKSHOP

SPA, BELGIUM, 24 october 2019

IGO
Instituut voor
Gerechtelijke Opleiding
IFJ
Institut de Formation
Judiciaire

This project was funded by the European Union's
Justice Programme (2014-2020)

UNITING FORCES AGAINST CYBER CHALLENGES OF TERRORISM - EXCHANGE OF BEST PRACTICES

Spa (BE)

October 22-25, 2019

Conclusions and suggestions

Robrecht De Keersmaecker

INTRODUCTION

The seminar on 'Uniting forces against cyber challenges of terrorism - exchange of best practices' has taken place from 22 until 25 October 2019 at the Silva Hôtel Spa-Balmoral in Spa (BE). Chair of the seminar was Mr. Axel Kittel, Deputy Director of the Belgian Institute of Judicial training institute (IGO-IFJ). Rapporteur was Mr. Robrecht De Keersmaecker, Deputy Prosecutor General.

The seminar was organized by the Judicial Training Institute (Belgium) in collaboration with the *Ecole nationale de la Magistrature France* (ENM, France); *Scuola Superiore della Magistratura* (SSM, Italy); *Studiecentrum Rechtspleging* (SSR, Netherlands); *Krajowa Szkola Sadownictwa I Prokuratury* (National School of Judiciary and Public Prosecution, KSSIP, Poland); *National Institute of Justice Bulgaria* (NIJ, Bulgaria) and *Prosecutor office of Estonia* and with financial support from the *European Commission's Directorate-General for Justice*.

CONCLUSIONS

The following conclusions can be drawn from the texts and presentations of the speakers, the general discussions and the workshops.

1. **Cybercrime** is everywhere and will become ever more **omnipresent** as digitalization (i.e. Internet of things) further disrupts societal paradigms. All actors should be aware of the fact that the internet unites terrorist organizations with lone wolves globally, giving way to unrestricted warfare, that fully takes advantage of newly available possibilities, so that a permanent **sense of urgency** is to be underlined in the fight against such threats.

The **challenges** in combatting cybercrime in general and with regards to terrorism in particular are many (data retention, encryption, loss of location, international cooperation and public-private cooperation, virtual currencies, etc.) and these are common to all actors involved.

2. The Budapest **Convention on Cybercrime** is generally considered to be a useful instrument in order to deal with some of these challenges in general and the complexity of cross-border e-evidence gathering in particular. However it is no silver bullet and solutions often necessitate carefully weighing fundamental rights against each other.

Practice has identified room for improvement especially when it comes to direct access to e-evidence abroad, and the Second Protocol to the Convention on Cybercrime is welcomed.

3. The **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225) and the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226)** are also eagerly awaited. These instruments will create a European Production Order and Preservation Order, including strong safeguards and oblige the service providers to designate a legal representative in the EU.

Also, the EU entering into an **executive agreement** with the USA under the **CLOUD Act** is also paramount to facilitate access to e-evidence since the majority of the bigger service providers are located in the USA.

4. Meanwhile, the existing framework for **Mutual Legal Agreement** should be further maximized and strengthened. Bettering mutual understanding of the legal systems of our partners could further expedite the current MLA process, especially with the USA (e.g. probable cause requirements, etc.). MLA procedures would greatly benefit from digitalization. In light thereof, the importance of the ongoing project "Cross border Digital Criminal Justice" (eEDES) led by the European Commission (DG Justice) and Eurojust should be underlined.

5. Cooperation with online service providers (OSP's) could also be improved, while taking into account GDPR compliance. The practice of a single point of contact on the side of law enforcement gathering all available and up-to-date information on which OSP can offer what information based on which grounds and through which channels is a clear advantage. Having this SPOC coordinate all requests for information for the OSP's improves confidence building and leads to more, quicker and better response. With regard to this, increased attention should be given to the SIRIUS project spearheaded by Europol, that is providing guidelines on specific service providers and investigative tools, since replies by OSP's on what kind of information they can offer are not always consistent between member states.

6. An important topic remains the issue of **encryption**, where law enforcement is at odds with an ever evolving criminal practice and a privacy lobby that depicts all attempts at trying to enforce cooperation from suspects or the OSP's and tech industry as an all-out attack on citizens' fundamental rights and democracy itself. During the workshops, it became visible that although we are all fighting the same fight within the same larger European playing field (e.g. the Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings) a clear legal framework seems to be lacking, giving rise to a wildly differing jurisprudence filling the void (e.g. order a suspect to provide a PIN-code; obtaining a biometric key by force, etc.). If accessing the suspect's device by way of breaking the encryption without having to resort to the abovementioned methods is to be preferred, Europol's Expert Platform on Encryption should be highlighted as it allows for the centralization and improvement of new technical possibilities to circumvent encryption and access data in clear text.

7. The increased use of the **Darkweb** (part of the internet that is not accessible through standard browsers) poses a specific threat; the fight against cybercrime on the Darkweb requires coordinated approaches that do not shy away from out-of-the box solutions. Successful operations mostly targeted the underlying illegal markets' trust with buyers and vendors and were carefully coordinated between various law enforcement agencies across borders.

8. Although the fight against cybercrime in general and terrorism in particular is a priority in most member states, it appeared from various discussions among the participants there is a significant difference in the available law enforcement **capacity and means** directed towards that end. While some member states have created robust entities with ample funding focusing solely on cybercrime, efforts of others have remained piecemeal and limited. The societal shift however seems to necessitate an overall increase in capacity and an integral approach, not only on a national level, but also between member states. Law enforcement does not have the luxury of re-inventing the wheel and experiences, guidelines and best practices should be shared actively and consistently among member states through available channels (Eurojust, Europol, etc.).

SUGGESTIONS

The following suggestions can be distinguished from the texts and presentations of the speakers, the general discussions and the workshops.

1. A first suggestion relates to the Second Protocol to the Budapest Cybercrime Convention, designed to provide solutions for a more efficient criminal justice response to cybercrime and other crime involving electronic evidence in accordance with data protection and other safeguards. It is recommended that this new instrument is finalized and adopted with aforementioned sense of urgency in mind.

2. In addition, the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225), the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226) and an executive agreement under the CLOUD Act between the EU and the USA should be expedited further as they will offer a much needed legal framework to move forward in the fight against cybercrime in general and terrorism in particular.

3. **The eEDES platform** should be made operational and accessible to all Member States as soon as possible. In order to facilitate MLA procedures with the USA, it should be considered integrating the USA in the eEDES platform, thus further digitalizing and standardizing the existing MLA process with attention to the requirements of the various underlying legal systems.

4. Cooperation and communication between law enforcement and OSP's is (only) possible within the boundaries of the applicable legal systems. Member States should be encouraged to streamline the existing cooperation by installing a **Single Point of Contact** within law enforcement to gather all available information on the OSP's and keep this up-to-date, as well as coordinate all requests in order to maximize confidence building. It is recommended that the national SPOC's actively contribute to and draw upon the **SIRIUS** project within Europol as to increase sharing of knowhow and best practices. The SIRIUS project should also include smaller service providers, since they would greatly benefit from streamlining and standardizing cooperation with law enforcement.

It is recommended that Europol actively promotes the sharing of information with the SIRIUS project and sets in place a clear and accessible procedure for the Member States to communicate new developments and updated information on OSP's, big and small.

4. The same goes for sharing of decryption capabilities between Member States. Sharing this information with the **Expert Panel for Encryption** within Europol should be encouraged and the Expert Panel should actively promote its services to the benefit of the Member States.

5. New **out-of-the box approaches** to combatting cybercrime on the Darkweb should be actively sought and pursued, making use of newly available technologies (e.g. Artificial Intelligence powered chatbots consuming criminals' resources and time, flooding darkweb marketplaces, etc.). Europol should actively seek to expand this knowhow through train-the-trainer programs and should also strengthen its efforts in directly informing prosecutors and investigative magistrates of the available tools rather than limiting this information to police services.

6. Where Member States prioritize combatting cybercrime in national strategies, they should be encouraged to bring their **budgeting priorities** in alignment as to make sure that the necessary means and capacity are attributed to services fighting cybercrime and that the structures put into place maximize efficiency with regards to operational capacities and knowhow management.

ANNEXES

Click and read

KERKHOFS VAN LINTHOUT Guidelines Interpol CT EvidenceCollection 2018 03 EN-LR

KERKHOFS VAN LINTHOUT Guidelines UN Practical Guide Electronic Evidence ebook

KERKHOFS VAN LINTHOUT SKYPE First Instance Judgment 27-10-2016 EN

KERKHOFS VAN LINTHOUT SKYPE - Court Antwerp 15-11-2017 Engl.transl

KERKHOFS VAN LINTHOUT SKYPE - Court of Cassation 19-02-2019 - ENG

KERKHOFS VAN LINTHOUT YAHOO First Instance 2 March 2009

KERKHOFS VAN LINTHOUT YAHOO Court of Appeal Ghent 30 June 2010

KERKHOFS VAN LINTHOUT YAHOO Court of Cassation - September 4th 2012

KERKHOFS VAN LINTHOUT YAHOO Court of Appeal Brussels 12 Oct. 2011

KERKHOFS VAN LINTHOUT YAHOO Court of Cassation 18 January 2011

KERKHOFS VAN LINTHOUT YAHOO Court of Appeal Antwerp 20 Nov. 2013

KERKHOFS VAN LINTHOUT YAHOO Court of Cassation III - 1 December 2015

KERKHOFS VAN LINTHOUT T-CY(2013)7REV GN3 transborder V12adopted

KERKHOFS VAN LINTHOUT T-CY(2015)16 GN Article 18 v40final

KERKHOFS VAN LINTHOUT T-CY(2016)11 GuidanceNote11 terrorism V15adopted

T-CY(2016)2 CEG providercoop rep v17

T-CY(2016)5 CEG final rep v40provisional

CAJANI, All along the watchtower Handling and Exchanging Electronic Evidence, 2018

END

This project was funded by the European Union's Justice Programme (2014-2020)