GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Bucharest, 21 October 2019

Report on the

International conference on online investigations: Darknet and online sexual violence against children

30 September-1 October 2019, The Hague, Netherlands

Jointly organised by EUROJUST and by the GLACY+ joint project of the Council of Europe and the European Union

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

1 Introduction

1.1 Background and justification

As societies rely increasingly on the use of information technology, cybercrime and the use of electronic evidence become challenges for criminal justice authorities and to the rule of law. With offences involving computers and electronic evidence evolving rapidly both in number and in sophistication, effective countermeasures to enhance international judicial cooperation in cybercrime cases in a consistent and harmonized manner is essential.

Eurojust and the Council of Europe have agreed to join forces and to support such efforts through the "International conference on internet investigations: Darknet and online sexual violence against children".

Eurojust stimulates the coordination of investigations and prosecutions between the competent authorities in the Member States of the European Union and improves cooperation between competent authorities of EU Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests. Eurojust supports in any way possible the competent authorities of the EU Member States to render their investigations and prosecutions more effective when dealing with cross-border crime. Eurojust competence covers the same types of crime and offences for which Europol has competence, cybercrime being one of them.

The European Union and the Council of Europe assist countries through a range of joint projects, including the GLACY+ project on Global Action on Cybercrime Extended implemented by the Cybercrime Programme Office of the Council of Europe (C-PROC). GLACY+ helps create the necessary capacities to implement the Budapest Convention and to cooperate internationally within the framework of this treaty in countries committed to implement it.

The Budapest Convention is the most relevant international treaty on cybercrime and electronic evidence with currently 64 Parties and 8 Observer States. Work on an additional protocol on enhanced cooperation commenced in September 2017.

Law enforcement agencies and prosecution services are increasingly required to deal with identification of cybercriminals in foreign jurisdictions or with the retention of data that is located abroad, and the use of tools such as the 24/7 points of contact network and mutual legal assistance treaties have become key to successful investigations and prosecutions. Other avenues such as ad-hoc arrangements with private companies can also be explored for data sharing and for the provision of information on a voluntary basis

However, investigators and prosecutors have often reported difficulties in using these tools, mainly related to issues such as: lengthiness of the overall process, partial or no execution of the requests, necessity to cope with very diverse legislations and policy frameworks, and different levels of collaboration provided by the private sector.

This is the case when judicial and law enforcement authorities are performing internet investigations into the Darknet or when addressing the phenomenon of online sexual violence against children.

The Council of Europe and Eurojust addressed these issues with a specific focus on strengthening international cooperation amongst police, prosecution services and central authorities for MLA by streamlining the respective procedures for MLA on Cybercrime and Electronic Evidence and in providing other solutions such as the reinforcement of the capacities of countries and national authorities through

training, drafting and/or reviewing legislation and/or national policies and strategies, improving reporting systems and the monitoring of statistics, providing guidelines in specific thematic areas and recent trends (e.g cloud evidence) and demonstrating the features and advantages of the Budapest Convention and its protocol.

1.2 Expected outcome

By the end of this international conference, experts from participating countries were expecting to have enhanced their knowledge with regard to the investigation of sexual violence against children in the darknet:

- On how to successfully conduct investigations in the darknet and related cases of online sexual violence
- On how to use specific investigative tools in practical cases
- On the work carried out by different international organizations and tools available to address the phenomena of online sexual violence against children in the darknet.

1.3 Participants

The Council of Europe invited 2 representatives from the following 38 countries and across the following C-PROC projects:

- GLACY+: Argentina, Benin, Brazil, Burkina Faso, Cabo Verde, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Mauritius, Mexico, Nigeria, Panamá, Paraguay, Philippines, Senegal, Sri Lanka, Thailand and Tonga;
- CyberEast: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine[1];
- iPROCEEDS: Albania, Bosnia and Herzegovina, Kosovo*[2], Montenegro, North Macedonia, Serbia and Turkey
- CyberSouth: Algeria, Jordan, Lebanon, Morocco and Tunisia.
- EndOCSEA@Europe: Armenia, Azerbaijan and Ukraine[3]

All participants are officials engaged in international cooperation, in particular with experience in cybercrime and electronic evidence or specialized prosecutors on cybercrime or officials from the Central Authority for MLA or Law Enforcement Officials engaged in the fight against cybercrime.

Each participating country designated one specialized prosecutor or member of the central authority and one Law Enforcement Officer with experience in investigating cybercrime (ideally the head of a cybercrime unit if available).

In addition, the following organizations/institutions were invited to appoint participants:

- One representative of each EU Member State at Eurojust;
- The liaison prosecutors of USA, Norway, Switzerland, Ukraine, North Macedonia and Montenegro represented at Eurojust
- One representative of the United States Department of Justice;
- One representative of UNODC;
- Two representatives of Europol;
- Two representatives from INTERPOL;

[1] *Armenia, Azerbaijan and Ukraine should only appoint one participant per country under CyberEast*
[2] *This designation is without prejudice to positions on status and is in line with UNSC Resolution 1244/1999 and the International Court of Justice Opinion on the Kosovo Declaration of Independence.*
[3] *The priority countries of EndOCSEA@Europe project should appoint only one participant per country*

- One representative from the EU-DEVCO;
- Two international experts designated by the Council of Europe

With a total of 120 participants.

1.4 Location

The workshop took place at the EUROJUST premises in The Hague, The Netherlands at Johan de Wittlaan 9, 2517JR The Hague

Interpretation was provided in English, French, Spanish and Portuguese

2 Day by Day participations

2.1 Day 1 - Monday, 30 September 2019

2.1.1 Opening Session

The conference was opened by Ladislav HAMRAN, President of the College of Eurojust, Alexander SEGER, Head of Cybercrime Division and Executive Secretary of the Cybercrime Convention Committee (T-CY), Council of Europe (CoE) and Carlos BANDIM-BUJAN, Program Manager, Unit B-5, EU-DEVCO, European Commission, Brussels (BE)

Ladislav HAMRAN welcomed everyone to Eurojust for this second conference organized by CoE through the GLACY+ project together with Eurojust, noting the attendance of representatives from the 28 EU Member States, from 38 additional countries as well as regional and international organisations (Eurojust, Europol, Interpol and UNODC) and the private sector. He emphasized that the purpose of the conference was to enable all parties to cooperate together in order to address the phenomenon of online child sexual exploitation as an international issue by focusing on the CoE Conventions, the assistance which could be afforded in cross border cases by Eurojust and other organisations present.

Alexander SEGER stated that GLACY+ was an important initiative on cybercrime financed by both CoE and the EU. He questioned why only a minute fraction of cybercrime cases reported resulted in criminal proceedings when cybercrime was such a huge issue. He noted that child abuse materials were increasing in volume and that the criminal justice response needed to keep pace by making better use of legislation improving laws where necessary and by cooperating. It was for governments to provide enough resources so that a difference could be made by all worldwide. He suggested that the conference should be more of a workshop to resolve practical issues. Further, he emphasised that 64 countries are now Parties to the Budapest Convention explaining that the proposed 2nd Additional Protocol to the Convention which was being worked up specifically to improve international cooperation (MLA between the parties and direct cooperation with ISPs) would hopefully be finalised by the end of next year. In order to improve the effect of existing procedural measures available under the Budapest Convention, he was looking for agreement regarding the direct disclosure of traffic data from ISPs to law enforcement (LE) and also support for the use of production orders to obtain traffic data with a view to pursuing direct disclosure of content from ISPs in emergency situations providing this could be reconciled with data protection provisions. In the meantime, better use should be made of existing tools and cooperation arrangements he hoped that each of the delegations would be able to take away three or four actions from the presentations and translate them into actions using them to make a difference.

Carlos BANDIM-BUJAN emphasised the importance of the Budapest Convention as the main instrument of relevance to combatting cybercrime. He talked about ongoing efforts in the EU to improve preservation and obtaining of electronic evidence as between EU Member States and efforts beyond the EU in capacity building on cybercrime issues to the benefit of the entire international community. For these purposes he complimented the GLACY+ Project as a model to follow.

The conference then proceeded with presentations in accordance with the agenda, the main points of which are summarized below:

2.1.2 Session 1

Challenges, obstacles and constraints for international cooperation in investigating and prosecuting in the darknet, in particular cases of online sexual violence against children in different regions of the world (Latin America, Africa, Europe, Asia and Oceania)

Moderator: Alexander SEGER

Delegation of Argentina (LATAM) - Lucio Gonzalo Otero, Mariano Damian Manfredi:

The Argentinian delegation, speaking on behalf of the Latin-American (LATAM) region, summarized the issues faced from a prosecutor's perspective in LATAM countries as legislative, including the classification of cybercrimes in legislation, clarification of criminal procedural law, the need for specialists, specifically a trained cadre of prosecutors, the certainty of being able to access evidence across borders, the lack of technical resources, equipment and training to support pre-trial investigative actions and improve communications between experts, prosecutors and judges.

From an investigator's perspective, Interpol is relied upon in cross border investigations, efforts are also being made to research in the dark web and specifically on child abuse and exploitation, work is being done on the use of Artificial Intelligence (AI) to identify perpetrators and to identify victims with e.g. the national center for missing and exploited children; but also, with ICACC, Osint and the dark web, cyber Tipline, SIP.ar (Sistema de Identificación de Pedofilia). An example was given of operation "angel guardian" where 97 victims were found in Argentina (10-13 years old), in all 7 LATAM countries involved.

Alexander SEGER commented that adoption of the Budapest Convention procedural standards was proving to be difficult in LATAM countries and that was problematic.

Delegation from Senegal (West Africa region) – Mandiaye NIANG: speaking about African issues in combating cybercrime on sexual offenses against children.

The speaker indicated that he had sent out a questionnaire in advance of the conference to other African countries. He confirmed that the phenomenon of child pornography is growing in Africa but that it is not being effectively dealt with. In addition, he felt that available statistics from the police did not represent the reality and in any event many countries do not have the ability to gather reliable statistics which means that even the visibility of cases was difficult.

He went on to state that legal frameworks were inadequate in that the Budapest Convention, being the principal instrument available, had been signed by only 9 African countries (of 43) and that the Malabo Convention (an African Union instrument to support regional cooperation) had been signed by 9 countries but only ratified by 5. Whilst a lot of effort had been made in e.g. Senegal, Cabo Verde, Burkina Faso, African countries still need specific expertise relating to the obtaining of electronic evidence.

The differences between legal systems is also represented as difficulty in terms of coordinating between civil law and common law countries. At national level in civil law countries, the speaker noted that there was a lack of interaction between police investigators and magistrates responsible for overseeing requests for seizures.

Direct cooperation with ISPs was also an issue, difficulties to act in coordination, particularly with GAFAM (Web Giants – Google, Amazon, Facebook, Apple and Microsoft).

Alexander SEGER commended the speaker for taking the initiative to issue a questionnaire and noted that West African countries seemed to be more advanced than those in East Africa.

Delegation from Philippines (Asia)- Lolita L. LOMANTA: presentation focused on South East Asia

The speaker focused on South East Asia and introduced ASEAN a regional organization representing 11 countries and promoting cooperation between them.

She stated that the developing internet market, whilst supporting legitimate business opportunities in the region, also facilities child sex exploitation. This is represented by production and sharing of child sexual exploitation materials (CSEM) online, as well as grooming and live-streaming of CSEM explaining that this is especially prevalent in The Philippines. The Darknet is seen as a problem due to anonymity and the impossibility of enforcing the law.

She went on to state that distribution of CSEM is fuelled by the high demand for these materials and that poverty, disparity and inequality were the precursors. She quoted research which showed that 77% of perpetrators were within the child's circle of trust and that victims are minors aged 12 and older.

The speaker went on to question the sufficiency of legislation in the countries of the region that there was no legislation on reporting obligations for ISPs and that sexual grooming was not criminalized. Key challenges relate to victim identification due to lacking domestic legislation, inadequate law enforcement responses to online child sexual exploitation and abuse (OCSEA), incomplete or non-existent national action plans and lack of cooperation from private sector companies.

She recommended the following action points for the region: harmonization of national legislation for responding to OCSEA using the Lanzarote Convention as a reference point, harmonization of national laws for the collection of evidence, promotion of international cooperation and cooperation with the private sector (ISPs), the inter-connection of relevant data bases, the strengthening of law enforcement responses, the development and implementation of national action plans and the implementation of clear regulations for private sector ISPs.

Mieke DE VLAMINCK, Judicial Cooperation Advisor, Eurojust – For Europe

The speaker started by discussing a joint Europol-Eurojust questionnaire on "investigations of darknet criminality". The results, based on replies from 21 European countries, have been published in the third issue of the Cybercrime Judicial Monitor, which will soon feature on the Eurojust website. Its conclusions show that, except for a few Member States, most countries do not have specific legislation concerning online investigations and thus law enforcement applies general legislation on undercover investigative techniques and surveillance by analogy in these cases. She explained that the findings differentiate between active and passive presence of law enforcement online:

- "Passive presence" online is considered within the general competence of law enforcement; it is covered by the legislation on observation/surveillance and includes activities such as monitoring and logging of user activity. This is allowed in practically all EU Member States.

- "Active presence" amounts to undercover investigations and includes engaging in conversations and pseudo buys. In some countries, taking over darknet and vendor accounts is also possible. There are more stringent requirements and limitations for being actively present online, depending on countries' national legislations. None of them allow provocation by law enforcement, some do not allow the commission of crimes, and overall, these measures have to be limited in time and depend on the authorisation of court/judge/prosecutor.

The speaker noted that the challenges are similar in most countries and concern the sufficiency of legislation in terms of special provisions, coordination with different jurisdictions, the technical nature of the operations, lack of resources and the limitation – in time - of the measure. Encryption and anonymization are also major obstacles when investigating online.

Joint investigation teams (JITs) are considered a useful tool in cross border investigations but challenges remain due to varying rules on confidentiality in EU Member States and it is part of Eurojust role to facilitate cooperation between different countries and jurisdictions as well as discussing and overcoming such challenges.

Delegation from Tonga (Oceania) – Sela ALEAMOTUA - For Oceania

The speaker from the Tonga Attorney General's Office (AGO) confirmed that the South Pacific region shares common challenges. She explained that Tonga is the first country of the South Pacific to sign the Budapest Convention. She stated that the main challenges within the South Pacific is the legislative framework, where some Countries have some form of legislation in place but face challenges in its application, and most have no legislation at all.

Legislative frameworks exist but are not properly applied; in Tonga no serious cybercrime case has reached the prosecution stage to date.

Further, efforts are being made to improve formal international cooperation at a regional level and meetings are held to share experiences and to find ways forward. As far as the darknet is concerned, it has just made things far more complicated and in Tonga they are still at the stage of trying to understand it.

The speaker thanked GLACY+ for their support to date. In conclusion, recommendations would be to make use of existing legislation, to introduce new legislation and to work on international cooperation.

Alexander SEGER commented that working on legislation is an ongoing issue.

2.1.3 Session 2

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)

Ms. Christel DE CRAIM, Vice-Chair of the Lanzarote Convention Committee, Brussels (BE) - Discussion moderated by Manuel ALMEIDA PEREIRA, Council of Europe

The speaker introduced the Lanzarote Convention as the first international instrument to comprehensively protect children from sexual exploitation and abuse. To date all 47 CoE member states have signed the Convention and 44 have ratified. The Convention is also open to other countries outside of CoE.

The speaker explained that the Convention introduces regulatory provisions to be applied to prevent abuse carried out within the child's "circle of trust" as well as substantive law which covers criminal offences. A challenge is that the Convention was drafted in 2006/7 and that the digital world has changed since then. However, the Convention is regarded very much as a living instrument. For example, about the relatively recent phenomenon of sexting, it is important to find a balance between allowing it and making known the risks associated with it; the speaker emphasized that this is not an issue which can be stopped but that children need to be aware of the risks of sharing this material. A short video on You Tube "it also concerns me" helps children to understand. Even pictures shared or taken by children amongst themselves could be considered as child abuse when they are disseminated on the internet.

The speaker reiterates that the Convention focuses on children abused within their circle of trust and that it supports children being able to find a way to report appropriate conduct. For this purposes police officers need appropriate training.

It is emphasized that ICT possibilities should allow children to discover the world for themselves, but it is difficult for CoE to protect children entirely. Nevertheless, criminalization and prosecution are not the only appropriate way forward, preventative actions are equally important e.g. through screening of professionals and other people (volunteers) working with children. Also, parents can be a target group here so that they are able to protect their children. For this purpose, videos and tutorials are being developed.

The issue of domestic violence is also being considered by the Convention Committee, until recently this was seen as an issue between parents, but it is recognized not only that children are caught up in it as well, but this can develop into sexual abuse to be shared online.

The question of grooming has also been discussed and an opinion on grooming has also been issued by the Convention Committee, the opinion is not legally binding but offers a helpful way forward.

The speaker was asked questions from Chile about the Convention Committee views on sexting; in response the speaker said that this was a challenging issue, that it should not necessarily lead to criminalisation and that children should be made aware of associated risks of the material being shared online. There should not be a zero-tolerance policy as children would always continue to do this amongst themselves.

A further question was asked by Dominican Republic regarding the exact message on prevention and what kind of measures should be relied upon; the speaker indicated that awareness raising, screening, including screening of volunteers should be the way forward.

A final question came from Bosnia & Herzegovina regarding appropriate action regarding underage marriage. The speaker stated that this had been exacerbated by the migration crisis, that the Convention Committee is aware of this as problem but has not yet formally considered the issue of forced marriage.

2.1.4 Session 3

Eurojust mission, objectives and core tasks and available judicial tools for efficient international cooperation and MLA in Cybercrime matters

Ms Daniela BURUIANA, National Member for Romania at Eurojust and Chair of the Cybercrime Team, Eurojust, The Hague (NL) - Discussion moderated by Manuel ALMEIDA PEREIRA

The speaker opened by explaining that the mission of Eurojust operates on both operational and strategic levels. She stated that cybercrime is a global issue developing in a complex environment where the internet is both a great facilitator and a great disruptor, she pointed out that global issues require global solutions in order that cybercrime could be dealt with effectively, which at this moment are not in place.

She explained that Eurojust is the EU's Agency on judicial cooperation and as such supports and facilitates judicial cooperation and coordination between judicial authorities, from the investigation phase to prosecution and trial phase. Eurojust is a unique structure in the world with 28 EU Members and 6 liaison magistrates from countries outside the EU (USA, Switzerland, Norway, Montenegro, North Macedonia, Ukraine) present altogether at Eurojust. Eurojust cooperates with third countries (which allow liaison magistrates to be appointed to Eurojust) based on cooperation agreements (there are 11 of those) and through contact points of which there are currently 47.

The speaker enumerated several common challenges in cybercrime generally as including the loss of data, loss of location, the time-consuming nature of international cooperation – even with the European Investigation Order - the differences in legal frameworks, public private cooperation, evolving threat landscape and the resulting expertise gap.

Concerning the child sexual exploitation cases, Eurojust conducted some years ago a judicial analysis of the casework in this field where the following challenges were identified: 1) time consuming MLA, (2) the fact that there are significant numbers of victims spear across different countries, huge volume of materials/data to be assessed and high numbers of cases and parallel investigations which are not properly coordinated.

The supporting tools offered by Eurojust include coordination of cross border investigations and prosecutions with early involvement of judicial authorities, facilitation of execution of MLA, legal advice, support to setting up and functioning of joint investigation teams (JITs). Statistics for 2016-2019 showed an increase in relevant cases and continuing use of JITs in appropriate cases.

A case example of fast and effective cooperation was given in Operation "Dark Room"; this was a case opened in August 2017 by Norway involving also Romania. A JIT was established between the countries by the end of September 2017 with two coordination meetings organised by Eurojust and a takedown resulting in the suspects being detained and victims receiving protection. A challenge was that Skype was used by the suspects to facilitate communications, which doesn't allow a recording of the material being exchanged. Chat logs appeared to be a primary source of information for the investigators but not easy to track for the same reason.

The Judicial Cybercrime Monitor produced yearly by Eurojust based on the input of the European Judicial Cybercrime Network containing a collection of court rulings in the field of cybercrime, updates on legislation in the field at EU and national level as well as topics of interest was mentioned as a helpful tool for practitioners in building knowledge and sharing expertise.

Furthermore, at strategic level Eurojust is supporting the European Judicial Crime Network (EJCN) and cooperates closely with Europol (EC3) including a dedicated Seconded National Expert (SNE) from Eurojust. In conclusion the speaker emphasized the need to keep pace with trends and developments in cybercrime which require an increasing level of cooperation, coordination and expertise from practitioners. Subsequently MLA process should be faster enough and more effective.

The knowledge of current tools, instruments and judicial facilitator actors is vital for practitioners in order to be efficient in their cross-border investigations/prosecutions.

There were questions from Ghana, Benin and Dominican Republic on how to access Eurojust tools and assistance; the presenter recommended that if they have cases with EU Member States to ask that member state to open a case at Eurojust.

2.1.5 Session 4

Obtaining electronic evidence under the Budapest Convention: current procedures, issues encountered

Ms Rajka VLAHOVIC, Consultant for the Council of Europe - Discussion moderated by Manuel ALMEIDA PEREIRA

The speaker first discussed the scope of the Budapest Convention (offences involving computer systems and electronic evidence) and the relevance of the procedural powers to the substantive offences created by the Lanzarote Convention. She explained that obtaining of evidence pursuant to the Budapest Convention was ultimately based on the adequate implementation of the procedural powers in national criminal procedural law and effective MLA process and procedure.

She went on to provide an overview of the procedural provisions, their purpose and effect and went on to look at each power in more detail recounting problems in implementation and the impact it could have. She explained the crucial notion of the preservation power and the importance of the production order for the purpose of cooperating with ISPs to obtain evidence. She stated that inadequate implementation ultimately weakens the position of the States Parties to deal adequately with cybercrime.

Further, she discussed MLA process and procedure making the point that States Parties were dependent on existing arrangements which varied between the EU (direct transmission) and other states (transmission through central authorities) noting that the Budapest Convention required MLA requests to be dealt with on an expedited basis. She mentioned the T-CY Assessment Report of 2014 on International Cooperation and relevant findings and recommendations. She drew the participants' attention to a number of tools developed by CoE to improve and assist MLA including: guidance note #10 which explains how to obtain subscriber information through the use of the domestic power of a production order (Article 18 1 (b), template requests for preservation of data and MLA for obtaining subscriber information, as well as the online resource which remains under development, having the purpose of informing a requesting State Party of the assistance they could hope to obtain from another State Party and the limitations of such assistance, making the wider point that such guidance, be it national or regional, assists the MLA process.

She concluded by referring to direct cooperation with ISPs and the possibility of reciprocal data sharing agreements pursuant to the US CLOUD Act which puts such direct cooperation on a legal footing for the first time, but which represents a bi-lateral solution or series of bi-lateral solutions which may not be within the means of every state. Meanwhile a multi-lateral solution in terms of simplified MLA procedures regarding subscriber information and direct cooperation with ISPs in the context of the proposed 2nd Additional Protocol is awaited next year.

A comment from the Sri Lankan delegation mentioned difficulties with admissibility of evidence obtained from service providers. Advised that this was a matter of national law; some mainly common law countries may have specific technical requirements which have to be fulfilled before evidence could be admitted whereas others may allow a freer evaluation of evidence.

Questions from Ghana and Burkina Faso on the application of Article 32, advised that this would be covered in a separate session on day 2.

2.1.6 Session 5

Collaboration with national and multi-national service providers: current practices, issues encountered and opportunities

Alexandra GELBER, Deputy Chief of the Child Exploitation and Obscenity Section (CEOS) of the United States Department of Justice, Washington (US) - Discussion moderated by Daniela BURUIANA, Eurojust

The speaker introduced herself as being the US Department of Justice expert on the Lanzarote Convention. She explained that her presentation would cover three areas; cooperation with mainstream ISPs, the darknet and companies sovereign-less by design.

Firstly, with regard to mainstream ISPs, the speaker made the point that these companies are not required by law to search their systems for material, in the event that they become aware of such material it is reported to the national centre for missing and exploited children (NECMEC). In that event the company is required to preserve the material for 90 days. However, in practice companies (e.g. Microsoft) do conduct voluntary searches. She explains that the issue is to find a balance between privacy and mandatory obligations. The speaker also emphasized the sheer volume of tips; in 2014 one million tips were made regarding millions of images of sexual abuse. She stated that 95% of the reports to NECMEC ultimately go on to foreign countries for national authorities to pursue and to obtain necessary data through MLA.

She identified the problems in cooperating with mainstream ISPs as (1) notification given to customers and (2) data retention which only applies once a report is made.

The speaker acknowledged that the receiving of a report from the US poses a problem for competent authorities in other countries as evidence must be pursued through international cooperation mechanisms. She mentioned that the Budapest Convention (through the proposed 2nd Additional Protocol) and the US CLOUD Act represent (potential) improvements in international cooperation. She acknowledged that tips are increasing but these increases have not been complemented by increase in resources. She noted that countries have legal gaps, resource gaps and experience gaps.

A particular concern however, is what would happen if all the information (tips and reports) becomes unavailable, there is real potential for this in view of the plans by Facebook to introduce end to end encryption. In her view companies are making decisions which impact on public safety. The speaker believes that the USA could do more in terms of data retention subject to constitutional limitations and like other countries by putting public safety at the heart of the process.

Secondly, in discussing the Darkweb and in order to illustrate the scale of problem, the speaker stated that in Spring 2019 the top three hidden services relating to child exploitation had a membership of 1.5 Million and that only one child exploitation-related hidden service introduced online on 1st April 2019 reached 200.000 members within 28 days. One Tor bulletin board dedicated to "hard core" or sadistic violence with very young children has 800.000 members. The speaker emphasised that darkweb is a challenge for all of us in the sense that there is no prospect of collaboration with the Darkweb as the onion router (Tor) project is deeply committed only to the security of its users and does not acknowledge the resulting danger to the safety of individuals.

Thirdly, the speaker discussed companies "sovereign-less by design" such as Telegram which makes no disclosures to government entities and practices end to end encryption. It claims that it protects freedom of expression and privacy without any acknowledgement of risks to children. Another company mentioned by the speaker was *Protonmail* https://protonmail.com/security-details which is established

in Switzerland taking advantage of strong privacy protections available under Swiss law. An intervention by a Swiss representative suggested that Swiss authorities are working on new rules to force *Protonmail* to open their encrypted files to judicial authorities.

A question was asked by a representative from Panama regarding the practice of US ISPs of giving notification to the customer (potentially as suspect). The speaker responded that it was possible to stop this by court order on a case by case basis. A second question by the same representative pondered on whether it would be possible to pursue the owners of Telegram for facilitating child sexual abuse. The speaker suggested that this may not be impossible provided that guilty knowledge could be attributed.

A second question form Eurojust queried whether cyber tip reports were always followed up. The speaker stated that this depends on the level of information provided, companies decided on how much information to provide and that sometimes there was insufficient information to constitute child abuse.

2.1.7 Session 6

Case studies on darknet and online sexual violence against children: challenges, obstacles and solutions encountered (Costa Rica, Colombia, Thailand)

Presentation of Case "Riño - Rescatando Inocentes" by the Costa Rican delegation- Angie TREJOS VARGAS-Moderated by Manuel ALMEIDA PEREIRA

The case was notified by NCB/Interpol France and concerned sexual abuse images of children (mainly young girls). The case began in 2015 and involved the taking of photographs by a photographer in his studio in Costa Rica. Both the photographer and website were identified as www.belindaplay.com and evidence was recovered through searches. Inquiries were made by Unidad Especializada en Investigacion de Trafico de Menores and Mexican authorities. Payments for the materials were made via PayPal and other credit cards. Videos cost from 500 to 5000$. Users were identified through payments and at least 26 victims were identified and protected. In Costa Rica the perpetrators are serving custodial sentences, in Mexico an appeal is ongoing.

Presentation of Case "Lobo feroz" by the Colombian delegation - Nubia Viviana VARGAS VILLAFRADET and Oscar Ivan MENDOZA GARCIA - Moderated by Manuel ALMEIDA PEREIRA

A short movie introduced the Columbian National Police and its work against cybercrime. The following statistics were given: a total of 5434 denunciations were made to 2010 and 889 in 2019. A total of 328 suspects were arrested in 2010 and 45 in 2019.

The case "Lobo Feroz", conducted over a period of several years, concerned the apprehension of Hector Manuel Farias Lopez alias Anthony, known world-wide for selling and producing child sexual abuse material (videos). The victims aged 5 to 15 were paid cash and forced to undergo abuse by adults which was filmed and distributed. The suspect learned that he had been denounced and left to travel around Columbia. A total of 276 victims were discovered. Some 22 messages furnished by BCN/Interpol Mexico assisted in identifying the whereabouts of the suspect. The case proceeded by analysing available electronic evidence and cell phone devices and involved cooperation between different prosecutors' offices in Colombia (Bogota, Barranquilla). Other inquiries in the field led to identification of 4 victims in Mexico and 6 different locations, also new witnesses were found. International requests for arrest and extradition followed as well as work with both Interpol and Europol. The suspect was eventually located in Venezuela and was extradited to Colombia in 2018.

Presentation of two cases by the Thailand delegation – Niwate ARPAWASIN - Moderated by Manuel ALMEIDA PEREIRA.

The first case arose from information given by Google to US authorities who sent it on to Thailand. It was not possible to trace the IP address based on Thai legislation as the address was too old (over three months). But the picture provided by Google contained a GPS location. In Thailand, Facebook adds an ID number which helps to identify individuals. As a result of this, the perpetrator was identified, apprehended and prosecuted for child abuse and sentenced to 12 and a half years imprisonment.

The second case is ongoing and concerns DekHee.com. The website is hosted in USA and payment for materials is made by e-currency. Google cooperated and giving the identification of relevant Gmail addresses. Pictures helped to identify users (same picture or same faces from social networks). The same perpetrator was promoting various gay, hetero, porno and child abuse websites but also gambling sites. The inquiry consists of following the suspect from one website to another, using different URLs checkers, Google spread sheets, chrome web store, and then going from a phone number to an email address, etc. Thousands of URLs were checked, one site has a following of 14 million people. All are accessible on the internet, not on darknet using Google as the search engine.

A particular problem that was faced concerned pre-paid sim cards, ISPs use Network automatic transmitters (NAT) to get more benefit and it is a time-consuming process to get the information from ISPs.

2.1.8 Session 7

Empowering Cyberspace and New technologies Lab; Innovation Center INTERPOL; The Project DarkTOOLS

Rolf van WEGBERG, Cybercrime researcher at TNO and Delft University of Technology, The Hague (NL) - Moderated by Manuel ALMEIDA PEREIRA

A document was distributed to participants explaining project DarkTOOLS, TNO is a research institute and one of its areas of research is darknet policing, working with the Innovation Center at Interpol in Singapore. TNO helps also to monitor and understand the dark web and how criminal cases can be built. Its aim is capability building for Interpol member countries on dark net policy, the development of a darkweb capability road map to show what is going on, use of darkweb crawling, examining the "state of the onion", blockchain analytics, following the crypto currencies and dissemination of the above through research output and law enforcement training.

The speaker explained that "crawling" helps to understand if the law enforcement and justice interventions have an impact; this depends on types of interventions made (examples were given of Operations Marco Polo 2013, Onymous 2015, Bayonet 2017). After conclusion of the operations, the volume of the market grew, meaning that operations do not stop the traffic, the crime is simply displaced (operation Bayonet is a good example).

One lesson to retain was that the anonymous world enhances anonymization: if I change my name and anything else, I am recognisable with, it will be difficult to identify me again.

The speaker then spoke about the "state of the onion namely the fragmentation in the dark market ecosystem; a significant portion of "banned products" have niche platforms (child sexual abuse, red rooms); a significant portion is available for facilitators (hosting, wiki/forums: e.g. 286 new "*dot onions*" sites in a week in 2019).

The speaker emphasized three roads to intervention in darkweb cases:

- Through de-anonymization of payments, crypto currencies
- Go after anonymity (infiltration, or undercover activities)
- Go after security (misconfigurations in *"dot onion"* domains).

The speaker received a question from Colombia asking how the assistance of TNO could be accessed. The speaker replied that an MLA request to the Dutch authorities would be required.

Representatives from Chile queried the admissibility of evidence from the TNO source. The speaker replied that the law of the location where the evidence was seized would be applicable and would show how the evidence had been obtained.

2.1.9 Session 8

EU and international organizations' experiences and tools for internet investigations on darknet and online sexual violence against children

CSE investigations and Darknet - Silviu CRISAN Europol– Moderated by Manuel ALMEIDA PEREIRA

The speaker introduced the role of Europol explaining that. Europol offers support and coordination to EU police forces, a decryption platform, operational meetings, an intelligence and analysis hub and the secure exchange of intelligence. Europol also runs strategic support, in capacity building, platforms for experts, webinars (through CEPOL) and cooperation with private sector, industry and academia. Operational and strategic support is provided to Europol's partners in preventing and combating the activities of criminal networks involved in the sexual exploitation of children was provided through Analysis Project Twins which conducts victim identification.

The speaker emphasized that CSE investigations require coordination of national law enforcement authorities and support from international police and judicial institutions.

The speaker discussed Operation SKY which was initiated by Spanish Police, offenders used Skype to talk about child abuse and exchanged large volumes of CSEM. Support by Europol initiated assistance via J-CAT (cyber specialists in Europol) in 2017. As a result, four hands-on offenders were arrested, and five 5 victims were safeguarded.

Operation Titanic II concerned Elysium a darknet platform and involved Germany, France, Spain and Italy. Victims were younger than 11 and the platform allowed appointments to be made in order to carry out abuse on the children. Agencies from a large number of countries contributed intelligence and 14 arrests were during a planned period.

The speaker went on to discuss innovation in investigation stating that specialised victim identification task forces at Europol were working on consolidating data and generating leads in through image analysis and then passing on these leads to the countries concerned so that the investigations could proceed at national level. Tips accessed through open source material were also pursued and passed to relevant countries. "Bellingcat" is a valuable open source which was awarded a prize for its work.

Also discussed was the "trace an object" initiative to stop child abuse is a crowdfunding operation which began in 2017, engaging the law enforcement community and public through a dedicated website http://europol.europa.eu/stopchildabuse. There was an example of a book found on a video, information about it was sent by Russia and Ukraine resulting in two victims being identified in March 2018 in Moscow for abuse committed in 2005. This system has helped to identify 9 victims and arrest 2 offenders.

2.1.10 Session 9

Vulnerable Communities, Crimes Against Children,

INTERPOL, *Global Complex for Innovation, Singapore - Gordana VUJISIC - Moderated by Manuel ALMEIDA PEREIRA*

The speaker introduced Interpol as an organisation of 194 member countries. The specific purpose of the presentation was to discuss the Crimes against Children Unit whose main activity is victim identification. Capacity building is also carried out by Interpol focusing on training in victim identification, helping member countries to build investigations and through sharing tools such as the ICSE data base. Interpol engages in offender management through the use of Interpol notices, the speaker noted the Green Notice used to disseminate information on convicted child abusers who travel. Prevention tools are also available including lists of child abuse sites with URL and a "hash list" for the private sector.

The speaker mentioned the OPTE project www.opte.org, which shows the growth of the internet between 2000 and 2016. She emphasized that technology did not create child sexual abuse, it democratized it. Today only 4% of the internet is on the surface web, whilst 96% is in the darkweb. Over 80 % of visits on darkweb are for the purpose of paedophilia research paid for by crypto currency (e.g. Bitcoin). Data is downloaded from these sites and placed on the data base so that the process of identification can begin.

The expert also presented two short case studies (cases not disclosed for this report)

At the close of Day 1, Manuel ALMEIDA PEREIRA reminded delegations to consider their "take away" from the conference. Each delegation should prepare around 2-3 relevant points covering what they would disseminate with their national peers, upon their return.

2.2 Day 2 - Tuesday, 1 October 2019

2.2.1 Session 10

EU and international organizations' experiences and tools for internet investigations on darknet and online sexual violence against children -continued

Counter-Cybercrime Education, UNODC, Vienna (AT) - Kamola IBRAGIMOVA, moderated by Daniela BURUIANA

The purpose of the presentation was to discuss UNODC's activities on transnational organized crime with reference to cybercrime. The three pillars of the UNODC Global Programme on Cybercrime include capacity building, research and analytical work and normative work to assist states to implement the UN instruments. The globally deployed staff is providing regular, ongoing training and mentoring.

Examples of activities - directly or indirectly addressing online child sexual exploitation and abuse (CSEA) - include the development and delivery of training courses on Cryptocurrency and Darknet investigations. UNODC delivers Cryptocurrency Investigation course as an awareness-raising course (available in open access at http://gpml-crypto.org/modules/Crypto%20English/launch.html), or as in-depth classroom-based course (more information can be obtained at unodc-cryptocurrency@un.org). In order to assist the analysis of electronic evidence, UNODC also supports Member States to build their digital forensic capacities (e.g. the opening of the first specialized forensics laboratory in Laos). Also, UNODC - jointly with the United Nations Counter-Terrorism Committee Executive Directorate (CTED)

and the International Association of Prosecutors (IAP) - has developed a practical guide for the obtaining of electronic evidence across borders. This can be accessed through UNODC's Sherloc platform.

Finally, the speaker mentioned UNODC's Education for Justice (E4J) initiative in implementation of the Doha Declaration, the purpose of which is to prevent crime (including cybercrime) through education activities and tools designed for primary, secondary and tertiary education levels. Some examples of such tools included the Online Zoo book (now available in 9 languages), the Zorbs animated series; and the University Module Series on Cybercrime.

The delegation from Senegal asked about the availability of a practical guide for the obtaining of electronic evidence across borders in the French language and the delegation from the Dominican Republic were interested in accessing the University Module Series on Cybercrime.

2.2.2 Session 11

The Global Forum on Cyber Expertise (GFCE); Bringing together stakeholders and expertise to build efficient cyber capacities

Global Forum on Cyber Expertise (GFCE), The Hague, NL - Wouter VEENSTRA, moderated by Daniela BURUIANA

The speaker presented GFCE, officially launched during the Global Conference on Cyberspace 2015 (GCCS2015) to strengthen cyber capacity building efforts on a global scale.

The GFCE is a fast-growing community aiming to become the global coordinating platform on Cyber Capacity Building. GFCE Members are countries, IGO's and large private entities while GFCE Partners are usually Knowledge Partners (academia, think tanks, etc.) and Implementing Partners (tech community, specialized SME's, etc.) and stakeholders who formally cannot become a Member like UN bodies (e.g. UNIDIR, UNODC). The community currently consists of 82 Members and 21 Partners from all continents and has 2 co-chairs, India and the Netherlands.

The GFCE provides a neutral and informal platform for policymakers, experts and private companies to discuss best practices, exchange knowledge and share expertise with a focus on the areas of cyber security and cybercrime. The core objective of the GFCE is to identify successful policies, practices and ideas, and to multiply these on a global level.

The most important working mechanism are the GFCE Working Groups on 5 prioritized themes as presented in the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building: Cyber Security Policy and Strategy, CIM & CIIP, Cybercrime, Cyber Security Culture & Skills and Cyber Security Standards.
The overall purpose of the WG's is to enhance cyber capacity building by

- *Coordination of efforts* by mapping of who is doing what and where, identify gaps, avoid duplication
- *Sharing expertise* by making available online best practices, toolkits, policies, frameworks on the so-called Cybil Portal.
- *Acting as a clearing house* by addressing requests received by Members connecting donors and implementers to recipient stakeholders.

The WG on Cybercrime consists of 23 countries, 10 International/regional Organizations, 6 Knowledge Partners and 7 Private Entities. They are focussed on Capacity building topics such as legal frameworks, legislation, cybercrime awareness campaigns and training of LEA's, Prosecutors and Judges. Currently the WG addresses a clearing request from The Gambia on a range of cybercrime topics.

Manuel ALMEIDA PEREIRA explained further that GFCE has an overview of relevant capacity building activities and that this helps to guards against duplication. He encouraged all delegations to consider joining the platform.

Questions from the Mexican and Dominican Republic (both Members of the GFCE) delegations asked about how to develop synergies. The speaker stressed the importance of a crosscutting, inter-ministerial national and international approach on cyber by having regular national assessments, drafting a national strategy and by seeking both international as public-private cooperation. A full list of members is on the GFCE website.

2.2.3 Session 12

Voluntary cooperation and formal assistance requests during internet investigations on Darknet and online sexual violence against children

Christian AGHROUM, Council of Europe - Robert LAID, Judicial Cooperation Advisor, Casework Unit, Eurojust; moderated by Daniela BURUIANA

Christian AGHROUM spoke about difficulties associated with international cooperation including: reciprocity (a legal issue), data retention periods, lack of technical inputs, exchange of evidence or extracts of evidence, length of escalation and de-escalation.

At the domestic level, lack of central points of contact, at national, federal, regional and, local levels, lack of common understanding between law enforcement and judicial authorities, duplication (different law enforcement and prosecutors working on the same investigations), lack of quick and efficient links between law enforcement and judicial authorities (e.g. in some countries police and justice do not use the same language); shared technical and human resources and difficulties due to the level of technical ability in the country (material, laboratories ; data preservation, time limit, volume, cost), level of trained people; how to keep them; ISP and other private sector links (obligation to assist or not, prosecution if no response).

Robert LAID presented the SIRIUS Project and its relevance to the developing of the knowledge related to obtaining of electronic evidence. The project builds upon public-private partnership and is restricted to EU Member States and third States which have concluded cooperation agreements with Eurojust and/or operational agreements with Europol. The speaker explained that the purpose of the project is to look into existing alternatives to the MLA process and, through that, improve knowledge related to the access to electronic evidence from private entities.

Some "best practice tips" relating to direct cooperation with ISPs were shared with the audience. The speaker emphasized that this whole issue was dependent first and foremost on preservation and the underlying retention of data by SPs. Specific concerns relating to the definition of urgency and emergency situations, also the substance of communications in terms of providing the correct amount of information to SPs as well as limiting the scope of the request. Another concern raised was regarding the terms of service under which SPs operate, in particular the question of confidentiality.

The speaker stated that the particular challenges for national competent authorities relate to the proportionality of requests made to SPs; he recommended the following: requests must not be overly broad and should be narrowed down as much as possible e.g. identifying the legal basis for the investigation and describing the nature of the investigation, the account/user identifiers concerned, the context and the timescale in connection with the offence.

A question from Chile concerned the existence of a list of contact points within ISPs, they were advised to use the means available – either publicly available information on the legal entity or establishing a contact through 24/7 Network for the relevant information.

A question from Benin concerned a cross border crime involving abuse and blackmail and the best way to take this forward urgently. Here proceeding through the 24/7 Network was recommended as well as the SP in the other country, however this would ultimately depend on the circumstances in the case.

A question from Thailand again raised the issue of admissibility of evidence obtained via voluntary cooperation. The response here was that this was ultimately a matter for national legal framework related to the admissibility of evidence.

2.2.4 Session 13

Special discussion panel with Internet Service providers and Industry on the exchange of information and provision of support to investigations and prosecutions on the Darknet and online sexual violence against children.

Bitdefender - Alexandru CATALIN COSOI, Chief Security Strategist, Bitdefender Bucharest - Sander DE GRUIJL, Data Protection Officer EOKM (Expertisebureau Online Kindermisbruik) Amsterdam moderated by Manuel ALMEIDA PEREIRA

The speaker explained that activities of Bitdefender, a private company, include involvement in training and capacity building with both law enforcement and prosecutors. Bitdefender also provides operational support in individual cases on request based on agreement by way of a memorandum of understanding (MOU) between Bitdefender and the relevant national competent authority. An example was given of a case involving ransomware and encryption of computer systems, Bitdefender assisted by providing decryption assistance which prevented ransom being paid into the hands of criminals. He also mentioned www.nomoreransom.org created with Europol, this is a platform helping everyone including law enforcement to understand deal with case involving ransomware.

A question from Burkina Faso confirmed how assistance could be sought by contacting the company and that such assistance would be provided free of charge under the condition that when the case was successfully completed Bitdefender would be mentioned in media coverage.

The speaker explained the activities of EOKM, a Dutch NGO which helps children, giving them direct advice on how to navigate the internet and how to report abuse to the police. They cooperate with law enforcement and Interpol, with a view to having relevant content removed from the internet, they report complaints to the Dutch Police and have created a new hash database. They hope to have capacity to work on the darknet during next years. Their INHOPE initiative helps countries to set up their own hotlines and points of contact.

2.2.5 Session 14

Overview on current practices on obtaining evidence from another country and the role of the 24/7 POC

Rajka VLAHOVIC and Christian AGHROUM, Council of Europe, moderated by Manuel ALMEIDA PEREIRA

The speaker presented an analysis of Article 32, Budapest Convention including T-CY Guidance Note #3 and advice of the Cloud Evidence Group (CEG) in 2017, emphasizing that the Article had been formulated

20 years ago based on minimal experience that had since been exceeded. She explained that individual countries had developed national solutions do deal with aspects of Article 32 (b).

Ultimately Article 32 is not enforceable, and countries are now securing extra-territorial access to data in other (enforceable) ways such as reciprocal data-sharing agreements (e.g. agreement between US and UK based on the US CLOUD Act) and using the "technical assistance" order in Australia. Nevertheless, the provision is there for those who want to use it within Guidance Note #3 and it remains under consideration within the context of the discussion on the 2nd Additional Protocol. This may result in a more user-friendly provision with a more explicit legal framework and clearer safeguards

The speaker presented a description of the 24/7 Network based on Article 35 of the Convention including examples to remind to the participants how "*each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: the provision of technical advice; the preservation of data pursuant to Articles 29 and 30; the collection of evidence, the provision of legal information, and locating of suspects.*"

2.2.6 Session 15

Conclusions and the way forward on the streamlining of procedures for MLA in cases of investigations in the darknet and online sexual violence against children

Rajka VLAHOVIC and Christian AGHROUM, Council of Europe, moderated by Manuel ALMEIDA PEREIRA and Daniela BURUIANA

2.2.6.1 Background

At the outset of the event representatives from Argentina, Senegal, Philippines, EU and Tonga outlined the problems and challenges in dealing with online investigations (darknet and online sexual violence against children) from their national and regional perspectives. The problems and challenges – with differences in emphasis amongst representatives - could be grouped around the headings listed below. These headings are further developed in a separate power point presentation (attached to Activity Report) and were discussed by the speakers. The headings are:

- Lack of comprehensive legislation (substantive and procedural (national and regional contexts).
- Lack of enough international cooperation arrangements regarding obtaining of evidence and (insufficient) regional arrangements.
- Requirement for training (specialised prosecutors)
- Requirement for resources at national level - human resources and to facilitate the keeping of statistics on relevant cases were mentioned.
- Lack of knowledge of tools including technical tools and technical investigative techniques.

Participants were provided with opportunities to comment on these issues which are further discussed under the analysis heading below.

Other contributions by participants included case studies presented during Day 1 by Costa Rica, Colombia and Thailand. These presentations demonstrated how cases were dealt with in national contexts using available (traditional) investigative powers including searches tracing of payments and analysis of communications data.

Remaining presentations allocated to Day 1 of the conference started by identifying relevant CoE legal frameworks (substantive and procedural law guidance notes and tools) the Eurojust mission to support judicial cooperation in the EU. The conference then moved on to discuss cooperation with US ISPs including the difficulties of investigating the darknet. In order to answer some of these difficulties and to supplement the knowledge of the participants with regard to darknet investigations, subsequent presentations covered the use of innovative (research based) techniques for investigating the Darknet and how to access such assistance, the use of proactive investigative tools (data bases) and initiatives for victim identification, how to engage with these as well as access to, and availability of, training opportunities/materials.

On Day 2 the conference proceeded with discussions of methods of obtaining evidence cross border, based on Budapest Convention Article 32, through the assistance of the 24/7 Network and in direct cooperation with service providers.
In order to supplement the effectiveness of cross border investigations and prosecutions, the final presentations identified opportunities to the participants to engage with cyber capacity building and resilience on a coordinated basis, innovative operational support to prosecutors and investigators in darkweb cases by the private sector and finally another private sector initiative focusing on support to child victims in the making of complaints to the police and though the establishment of hotlines.

2.2.7 Session 16

2.2.7.1 Closing session

The conference was closed by Manuel DE ALMEIDA PEREIRA, Project Manager of the GLACY+ Project, Council of Europe and Daniela BURUIANA, National member of Romania to Eurojust and Chair of the Cybercrime Team and Carlos BANDIN-BUJAN from the European Commission.

Participants reiterated their thanks to the organisers for the very useful event, for the knowledge that will be used to build their capacities and the opportunities to develop contacts and to build trust with colleagues from all over the world.

3 Conclusions

In conclusion, the clear takeaways for the participants, based on issues identified at the outset, questions asked, and comments made during the conference, are as follows:

1. The information provided on innovative methods of investigating the Darknet (featuring decryption) and how to access this form of assistance from private sector companies (primarily TNO and Bit Defender); as was pointed out at the outset of the conference, current investigative methods applied are based on existing legal frameworks on undercover investigations and surveillance which are of limited effect and do not adequately meet the challenges posed by darknet investigations.

2. The information on the availability of various training and capacity building opportunities as well as training materials and tools (cybercrime, crypto-currency and e-evidence) and how to access these (primarily UNODC and GFCE); the need for further capacity building through training and respective learning materials was identified as an issue essentially by the delegations that are not yet benefiting from the capacity building initiatives provided by the GLACY+ project.

3. In terms of international cooperation and MLA – identified by all regional delegations as an issue at the outset - the takeaways were evident on a number of different levels including:
    a. clear information on opportunities to engage with international, regional and private sector organisations for the purposes of victim identification (Europol, Interpol tools: data bases and EOKM) and operational support in cross border cases (Eurojust, Europol, Interpol);
    b. clear information on opportunities (specifically raised by a number of participants) for third countries to engage in cooperation with Eurojust, either on a case by case basis where EU countries are involved or, through a potential contact point relationship as appropriate;
    c. clear information on direct cooperation with US based ISPs and limitations of such cooperation (US DOJ); concerns had been raised regarding ISPs notification procedure and admissibility of evidence obtained from ISPs during the conference, also the importance of proportionate requests when addressing ISPs directly (Eurojust);
    d. as far as MLA was concerned, - the effectiveness of the MLA process had been raised at the outset - participants were provided with CoE guidance notes and tools in the form of specially formulated template requests (MLA and preservation) to assist this process; the templates were singled out as a particularly useful takeaway by Turkey and Ghana.

4. In terms of streamlining MLA, the way forward must include (in line with the recommendations in the T-CY Assessment Report of 2014) simplification of procedures at national level and use of electronic transmission given that the Budapest Convention requires requests to be processed expeditiously. Otherwise, requests themselves must be proportionate and the templates developed by CoE will assist with this including where ISPs are to be addressed directly.

5. Finally, as noted by delegations from Latin America, Africa, South East Asia and the Pacific at the outset of the conference, legal frameworks (substantive and procedural law) and international cooperation frameworks (MLA) were noted to be inadequate. Particular takeaways for CoE could be to focus on the level of implementation of the Budapest Convention in these regions to identify where the legislative problems actually lie and in addition, to consider how to strengthen MLA based cooperation in these regions. This would also provide an opportunity to promote the CoE template requests.

Participants also expressed a wish to include discussions on the admissibility of evidence (especially when obtained from service providers) and crypto currency with associated money laundering and identification of criminal assets in any subsequent conference.

In sum, the three expected outcomes of the conference were met: the participants' knowledge was enhanced in the following areas: conducting investigations on the darknet, the use of specific investigative tools in practical cases, and in relation to the work carried out by international organisations to address OSEAC on the darknet and their tools.

The Council of Europe C-Proc should continue pursuing effective implementation of the provisions of the Budapest Convention and improvement of MLA processes and procedures based on the T-CY Assessment Report of 2014 within the regions represented as appropriate.

It was expressed by almost all delegations that this joint conference could usefully become a regular event in the future as it provides an opportunity for participants to review progress in implementing the Convention and to further build their relationships.

Contacts:

At the Council of Europe:

Manuel DE ALMEIDA PEREIRA
Project Manager
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 32
Email: Manuel.PEREIRA@coe.int

Elvio SALOMON
Senior Project Officer
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 41
Email: Elvio.Salomon@coe.int

Sinziana HANGANU
Senior Project Assistant
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 87
Email: Sinziana.HANGANU@coe.int

At EUROJUST:

Daniela BURUIANA
National Member for Romania at Eurojust and
Chair of the Cybercrime Team
The Hague – The Netherlands
Tel: +31-70 412 5360
Mob: +31 6 119 57 605
Email: dburuiana@eurojust.europa.eu

Peter GOUWY,
Senior Judicial Cooperation Officer
Eurojust
The Hague – Netherlands
Tel : +31-70 412 5621
Mob : +31 6 479 34 828
Email : pgouwy@eurojust.europa.eu