Octopus Conference 2016
Cooperation against Cybercrime

16 – 18 November 2016

Palais de l'Europe, Council of Europe, Strasbourg, France

Version 23 November 2016

Key messages

Some 300 cybercrime experts from 90 countries, 12 international and 40 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 16 to 18 November 2016 for the Octopus 2016 Conference on cooperation against cybercrime. The Conference was opened by Thorbjørn Jagland, Secretary General of the Council of Europe, and commenced with a special session on the occasion of the 15th anniversary of the Budapest Convention on Cybercrime. Andorra deposited the instrument of ratification of the Convention during this session to become the 50th Party to this treaty.

Key messages resulting from Octopus 2016 are:

- Increasing cybercrime, attacks against critical infrastructure, fraud, hate speech and terrorist misuse of information technologies are considered major threats. Cloud computing and encryption enhance the complexity of the challenge. The capacity of criminal justice authorities to counter such threats and to ensure the rule of law remains limited. At the same time, mass surveillance, control of online content and restrictions to the freedom of speech also raise concerns. The prevention and control of cybercrime and other forms of crime online must meet human rights and rule of law, including data protection requirements. The debate on encryption is a reflection of a dilemma that is sometimes difficult to resolve. Article 15 of the Budapest Convention on conditions and safeguards remains more important than ever.

- The Budapest Convention, 15 years on, remains the most relevant international agreement on cybercrime and electronic evidence not only as a guideline for domestic legislation and as a basis for international cooperation, but also a catalyst for capacity building and a framework for multi-stakeholder cooperation as demonstrated by this Octopus Conference. By addressing issues such as access to evidence in the cloud, it will remain relevant in the years to come. States are encouraged to accede to the Budapest Convention and its Protocol on Xenophobia and Racism as well as the data protection 108 of the Council of Europe.

- Access to evidence on servers in the cloud, that is, in foreign, unknown, shifting or multiple jurisdictions for criminal justice purposes is necessary for governments to meet their obligation of protecting society and individuals against crime. Voluntary cooperation by multi-national service providers – in the disclosure of subscriber information and in emergency situations also of other data – is most valuable but also raises concerns. The draft Guidance Note on Production Orders for Subscriber Information (Article 18 Budapest Convention) should help put such cooperation on a clearer legal basis. Measures such as an online tool on provider policies and on powers for production orders in Parties to the Budapest Convention, regular meetings of major providers with the Cybercrime Convention Committee and participation by providers in capacity building activities should facilitate cooperation in practice. A common procedure and platform for all requests to major providers should be given consideration. At the same time, a

Protocol to the Budapest Convention is considered necessary. The proposals made by the Cloud Evidence Group of the Cybercrime Convention Committee have received broad support during the Conference.

- Capacity building remains one of the most effective ways to help societies address the challenges of cybercrime and electronic evidence. Practical examples demonstrate the feasibility of this approach. Ingredients for success include designing programmes in support of holistic processes of change with political commitment as a prerequisite, commencing projects with a detailed situation and needs analysis, embedding training within training institutions to ensure sustainability, and involving the private sector in capacity building projects. Closer cooperation between organisations offering assistance would result in more effective use of resources and more sustainable impact.

- Legislation

  - In the Asia/Pacific region, reforms of legislation on cybercrime and electronic evidence have accelerated, often with the Budapest Convention serving as a guideline to ensure compatibility with international standards. Where legal reforms are accompanied by capacity building efforts – for example with the support of Japan, South Korea, UNODC or the Council of Europe – criminal investigations, prosecutions and adjudication of cases of cybercrime and other offences involving electronic evidence increase.

  - In Africa, several countries have moved ahead with reforms of domestic legislation, often using the Budapest Convention as a guideline. At the same time, more than half of African countries do not yet have the necessary legislation in place. Countries with draft laws should advance and complete their reforms, including rule of law safeguards to law enforcement powers. The Malabo Convention of the African Union reflects a clear political commitment by African leaders with regard to cybersecurity, data protection and cybercrime, but would need to be backed up by the Budapest Convention for operational criminal justice measures and international cooperation in practice. Reform of legislation needs to be followed by capacity building.

  - In Latin America, many countries have reformed their substantive criminal law using the Budapest Convention as a guideline, while specific procedural law provisions on cybercrime and electronic evidence remain a challenge. Given the similarity of the procedural law of countries of Latin America, many countries may move ahead in a similar way to deal with electronic evidence.

- Terrorist misuse of information technology, such as cyberattacks against computer systems, including critical infrastructure, their use for logistical purposes, including the planning of terrorist attacks or the dissemination – often via social media - of illegal contents, including terrorist threats, promotion of or incitement to terrorism, recruitment or training, xenophobia, racism or other forms of hate speech contributing to violent extremism, radicalisation and terrorism, is a serious threat. At the same time, countering terrorist misuse of ICT raises concerns regarding the freedom of expression, right to private life and other human rights. Strengthening criminal justice capacities, counter-narrative, and public/private and international cooperation as well as full implementation of international agreements are important elements of the solution. Encryption protects privacy but also represents one of the main obstacles for criminal investigations. Practical solutions with appropriate safeguards need to be found.

- Proceeds-generating crime online is increasing considerably. Follow-the-money approaches should also be pursued with regard to crime online. Good practices include

closer inter-agency cooperation between financial intelligence and financial investigation units on the one hand and cybercrime units on the other. Tasks forces with banks, Internet service providers, Computer Security Incidents Response Teams and Internet industry for sharing malware and threat intelligence will help prevent attacks at an early stage. Training of the judiciary and other capacity building are needed.

- Rendering international cooperation more efficient is essential. Follow up should be given to the Recommendations adopted by the Cybercrime Convention Committee in December 2014. Full use should be made of mechanisms such as 24/7 networks of the G7, INTERPOL and the Council of Europe, or of EUROJUST or of instruments such as the European Investigation Order. Practical proposals for a more effective role of 24/7 points of contact are available and should be implemented. Annual meetings of 24/7 points of contact should be organised. Procedures for requests for data in emergency situations via mutual legal assistance should be established.

- Cooperation between different organisations and initiatives towards the common goal of preventing and controlling cybercrime is improving steadily as the benefits of such cooperation become more obvious. Online tools and databases made available by organisations facilitate cooperation and enable governments to identify needs, establish baselines and measure progress. Efforts to generate synergies between organisations will need to continue.

Octopus 2016 was the 10th Conference on Cybercrime of its kind. The bottom line and overall message remains the same:

COOPERATE!

The Octopus Conference is part of the Cybercrime@Octopus project which is funded by voluntary contributions from Estonia, Japan, Monaco, Romania, United Kingdom, USA and Microsoft. Estonia, Japan and USA have made funding specifically available for the Octopus conference.

Programme overview

WED, 16 NOVEMBER			
Plenary session	*Hemicycle*		
9h00	Special Session: BUDAPEST CONVENTION – 15th ANNIVERSARY *(English/French/Russian/Spanish)*		
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/F)*	*Room 3 (E)*
14h30	Workshop 1: ► Capacity building on cybercrime: good practices, success stories and lessons learnt	Workshop 2: ► Legislation on cybercrime and capacity building in the Asia/Pacific region	Workshop 3: ► Service provider/law enforcement cooperation on cybercrime and electronic evidence
20h00 Social dinner in an Alsatian restaurant			
THU, 17 NOVEMBER			
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/S/F)*	*Room 3 (E)*
9h30	Workshop 4: ► Terrorism and information technology: the criminal justice perspective	Workshop 5: ► Legislation on cybercrime and electronic evidence in - Africa - Latin America	Workshop 6: ► International cooperation: workshop for 24/7 points of contact and MLA authorities
Workshop sessions	*Room1 (E/F/S/R)*	*Room 2 (E/F)*	*Room 3 (E)*
14h30	Workshop 7: ► Seeking synergies: Initiatives of international and private sector organisations	Workshop 8: ► Targeting proceeds from crime online	Workshop 9: ► Crime and jurisdiction in cyberspace: access to electronic evidence
FRI, 18 NOVEMBER			
Plenary session	*Room 1 (E/F/S/R)*		
9h30	Plenary: ► Results of workshops ► Human rights and rule of law in cyberspace: threats and safeguards ► Conclusions		
13h00	*End of conference*		

Workshop Summaries

Workshop 1: Capacity Building on Cybercrime: ingredients for success

16 November 2016, 14h30 – 18h00, Room 1 Palais

Moderator: Panagiota- Nayia Barmpaliou

Rapporteur: Esther George

The aim of workshop 1 was to identify ingredients for success, impact and sustainability of capacity building programmes. Capacity building has become the privileged international approach to address the challenges of cybercrime and electronic evidence. This is reflected, among other things, in the establishment of the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania (April 2014), the outcome of the UN Congress on Crime Prevention and Criminal Justice (Qatar, April 2015), the Global Cyber Space Conference (The Hague, Netherlands, April 2015), the establishment of the Global Forum for Cyber Expertise (GFCE) and in the policies and programmes of a number of international organisations.

CHALLENGES

In the context of the activities of mentioned organisations, the following was underlined:

- The challenges of cybercrime and electronic evidence increase at an exponential rate, and the knowledge acquisition programmes in these subjects need updating and modifying at a far greater rate than traditional types of criminal justice training. It is not only the technology that changes, but also the ways in which criminals commit crime and the legal challenges that their new methods impose.
- One of the key challenges is how capacity building programmes can be sustainable.
- Result-orientation vs ad hoc/one-off activities without linking to a broader change process/ reform.
- Training programmes developed in cybercrime subjects should not seek to sit outside of traditional training institutes, as many of the issues impact on types of training that have been undertaken for many years. Unfortunately, there is a lack of integration of training programmes in training institution for Law Enforcement and judiciary as there are elements of cybercrime and electronic evidence that should be included in all training programmes.
- The challenge of developing scalable and replicable programmes (Train the trainer methodology can assist).
- There needs to be a training strategy in order to avoid fragmented effort.
- The fact that each year, most organisation says that they intend to compliment and not compete with other organisations, yet we see, they still act, predominantly in isolation and still follow each other into the same jurisdictions with similar programmes.
- There is still unfortunately duplication of effort in this field.

GOOD PRACTICES

Good practices were shared by:

- The Council of Europe (CoE), United Nations Office of Drugs and Crime (UNODC), Interpol and the Organisation of American States.
- All 4 advocated that an assessment of the needs of the country concerned had to be evaluated (for example by a needs analysis) before developing training courses.

- All 4 are also concentrating on training the trainer in order to ensure that the training is sustainable.
- Some of the organisations are focusing on regional training as it encourages countries to work together and promotes regional cooperation.
- All 4 were able to give examples of joint working/ training they are undertaking. An example is the CoE and Interpol partnership in respect of GLACY+
- UNODC stated that they are also using e-training modules to reinforce their training.
- CoE gave extensive examples of the impact that they have had on the 7 GLACY countries of Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga and how this will be built on in GLACY+ and the other 5 projects.
- The Global Forum on Cyber Expertise (GFCE) is currently developing a roadmap on what cyber capacity building should comprise in the next 2 years.
- Examples of what is presently occurring in various countries was shared for example Mauritius and Sri Lanka shared the developments they are making in training criminal justice practitioners.
- Macedonia, Ukraine and Tonga shared their experiences of developing public private relationships. Macedonia and Tonga relationship with the private sector developed through proactive engagement, whilst Ukraine's was as a result of a reactive change namely cyberattacks on the critical national infrastructure changed their relationship with the private sector.

THE WAY AHEAD

- Capacity building should be seen as a holistic process of change on the basis of strong commitment by states, focused on results and institutional reform. This is applicable to all countries at any stage of maturity whether they are, developed and/or developing.

- The need to make training sustainable was recognised and it was agreed that the training of trainers is one way to achieve this.

- The whole-of-government, multi-stakeholders including private sector must be involved in capacity building projects.

- Before developing training there should be a needs assessment to ensure that training is tailored to the local context and requirements.

- There is a need to promote common standards (the Budapest Convention), substantive and procedural law and international cooperation.

- There should be a means to follow-up and a mechanism to evaluation the impact of the training / project.

- Need for trust-building between national authorities and the private sector.

- Organisations need to make more efforts to work together to coordinate activities and provide more effective and lasting support for countries and effective use of scarce resources.

Workshop 2: Legislation on cybercrime and capacity building in the Asia/Pacific region

16 November 2016, 14h30 – 18h00, Room 2 Palais

Moderators: Koichi Mizushima (Ambassador in charge of Cyber Policy, Ministry of Foreign Affairs), Shinsuke Shimizu (Consul General of Japan in Strasbourg and Ambassador, Permanent Observer to the Council of Europe) and Jayantha Fernando (Director, ICTA, Sri Lanka)

Rapporteur: Zahid Jamil (Pakistan)

Workshop 2 aimed at sharing good practices and discussing problems encountered as well as promoting accession to the Budapest Convention. The workshop was co-organised by the Government of Japan

The workshop showcased the reforms of legislation on cybercrime and electronic evidence which have accelerated in the Asia/Pacific region in recent years, participants shared their usage of the Budapest Convention as a guideline used to ensure compatibility with international standards. Additionally, the workshop dovetailed into the capacity building efforts that were connected with legal reform. In this regard the participants discussed and shared good practices and challenges encountered with respect to such legal reform and capacity building efforts. Finally participants also shared their efforts to promote accession to the Budapest Convention. The workshop was co-organised by the Government of Japan.

GOOD PRACTICES

- Various countries shared their recent successes and efforts to update, modernize and introduce legislation related to cybercrime and electronic evidence and in particular all mentioned that either they had used the Budapest Convention as a model or that their own review demonstrated that their legislation as drafted appeared to be consistent with Budapest Convention.

- Many mentioned that consistency with the Convention which they mentioned was the only international standard in terms of cybercrime was essential for effective international cooperation in the fight against cybercrime. Some requested further engagement and support from the Council of Europe for assistance in amending their laws in this regard. Fiji was one new and salient participant in this respect which called for such assistance while noting the special assistance Fiji had already received from Mr. Jayantha Fernando of Sri Lanka. Fiji also expressed its interest in engaging with the Council of Europe on accession and with member states present on building bilateral relations for stronger MLAT and cooperation processes. Tonga similarly noted the assistance of the Council of Europe with drafting amendments and Australia's assistance with drafting instructions for such amendments. Tonga advocated more Pacific countries to enact consistent legislation and ensure International cooperation for combating cybercrime. Updates and similar comments were received from Japan, Sri Lanka, Australia, Singapore, Cambodia, Fiji, Laos, Thailand, Tonga, Malaysia, South Korea, Philippines.

- Japan and Sri Lanka stressed that in the fight against cybercrime could not succeed without international cooperation. Sri Lanka noted the support it was inspired by its good friend Japan to accede to the Convention and shared the assistance it had received from the various friendly states in the Council of Europe as well as its own domestic efforts that had led to the island state becoming the second country in Asia and the fastest ever accession to the Convention. In this regard Sri Lanka shared its experience

with the accession process which was recognized as a best practice example for Asian and other countries to be followed with respect to their process for accession.

- Australia shared its recent efforts to introduce a specific format by which service providers had been mandated to collect and maintain information such as subscriber information and other data sets under a under specific format. Australia also shared its efforts to work more closely with the private sector, which as part of its 2016 Cybersecurity Strategy introduced efforts to ensure that the private sector took measures to protect their networks and a cascading system of engagement of government and LEAs, as well as Australia's continued commitment to institutional capacity building which included assistance in drafting laws for developing countries, training and engaging with industry about Cybersecurity and protection of networks.

- Cambodia while giving its update identified the following key challenges that were also shared by other Asia Pacific nations: Legislation challenges to achieve harmonization between international standards and domestic issues, enhancing Technical capability such as forensics, Institutional arrangements, capacity building and greater local and international cooperation

- South Korea also added that it had faced significant challenges due to some court rulings that declared evidence as inadmissible unless when data was copied or seized the lawyer of the owner of the digital evidence is allowed to participate and observe the process of collection. It was also shared that it was getting more and more difficult for South Korea to obtain data or receive cooperation from service providers. Some participants also mentioned adherence to the Budapest Convention as a best practice as an investment imperative in order to provide an enabling environment to investment and improved links with ASEAN.

- Japan also shared its experience in amending its legislation and dilated upon the difficult task any criminal justice legislative reform faces domestically. This underscored Japan's commitment to ensuring its legislation was consistent with best practice enshrined in the Budapest Convention. In this respect some innovative means to establish procedures through new mechanisms as opposed to outright amendments was of much interest and provided much guidance to other participants.

- The case study of Pakistan offered several instances of what not to do in terms of drafting cybercrime legislation and also offered an opportunity to list some basic dos and donts. These included:

    - Avoid usage of unique and language and provisions inconsistent with international standards established by the Budapest Convention and other models such as the Commonwealth Model Law
    - Avoid reinventing language or offense
    - Avoid creating omnibus legislation that combine cybercrime with cybersecurity/national security/telecom issues/cyber war/offences which were better dealt with in other legislations
    - Avoid over criminalisation or under criminalisation
    - Using technology neutral language
    - Be consistent with international best practice and the Convention
    - Using appropriate safeguards and civil liberties protections
    - Engaging international expertise
    - Singapore offered to add to these dos and donts by adding: aim to harmonize, Involve Frontline stakeholders (not just policy maker and legal draftsman) in order to stress test the legislation, Forge partnerships with academia and private sector through the drafting and consultation process

- Philippines also added that it was useful not to simply copy paste from the Budapest Convention. It was added by experts that as a treaty the Convention outlined provisions, principles and State obligations and was never intended to provide legislative language and as such assistance should be sought from the Council of Europe and best practice legislative language found in UK, US, Singapore and the Commonwealth Modal law provided best practice precedents in this regard.

- Capacity building efforts of the Council of Europe, UNODC and South Korea through the World Bank were shared. Also the continued efforts of CCIPS/DoJ of the United States was recognized by Singapore which also mentioned its inaugural annual ASEAN cyber prosecutors meeting as an effort at capacity building in the region as part of Singapore's cyber week.

Workshop 3: Service provider/law enforcement cooperation on cybercrime and electronic evidence

16 November 2016, 14h30 – 18h00, Room 3 Palais (Chatham House Rules)

Moderator: Pedro Verdelho (Prosecutor, Portugal)

Rapporteur: Markko Künnapu (Ministry of Justice, Estonia)

Workshop 6 discussed how to improve cooperation between service providers and law enforcement authorities to disclose subscriber information, including the main mistakes that have been made by formulating and sending the requests. During the workshop, were discussed also the service providers' disclosure policies and the emergency procedures which enable law enforcement agencies to receive necessary information in urgent cases, with the detailed presentation of a real case and lessons learnt. Finally, the workshop discussed the findings of the Cloud Evidence Group and proposed solutions. It was generally agreed that solutions were needed urgently, because practical problems are already impacting the criminal investigations.

CHALLENGES

- The workshop started with an overview of the issues identified by the Cloud Evidence Group in obtaining subscriber information from service providers and the different policies adopted by some of the prominent service providers. The rate of satisfied request is around 60%, which causes concerns in guaranteeing the rule of law in cyberspace.

- Some concerns were raised about how law enforcement agencies could know in advance where to send mutual legal assistance requests.

- As disclosure policies often refer to criminal cases and criminal investigations, a question was raised concerning cooperation with regard to missing persons. It was confirmed that cooperation and disclosure of information was at least with some service providers, possible also in missing persons cases where criminal investigation has not been initiated.

- The workshop also discussed a recent case study concerning possible terrorist attacks and cooperation with one particular service provider. The case study showed that there is still room for improvement, cooperation is not always effective and providers should review their disclosure policies. Emergency situation is understood in different ways, therefore it might be useful to review or harmonize the policies.

- Due to the forthcoming entry into force of the General Data Protection Regulation, the Parties need to look quickly for clear legal basis to address requests after 2018.

GOOD PRACTICES

- The use of common templates and establishment of Single Point of Contacts by one State Parties was mentioned as one of the best practices. It has led to faster and more efficient cooperation and this could be used as a positive example to guide other State Parties.

- The draft Guidance Note on Article 18 received lots of attention. As one of the main preconditions for the service providers to respond, is proper legal basis and lawfulness of requests, States were encouraged to review their national legal frameworks.

- The use of 24/7 contact point is useful both for law enforcement and for service providers, especially for data preservation.

- The service providers see improvement in obtaining information from countries that choose a single contact point.

THE WAY AHEAD

- A future online tool was discussed to make cooperation more effective. In addition to the law enforcement, also service providers could make use of it, because it would contain the relevant information about the State Parties, its competent authorities and requirements for sending requests to the service providers.

- The workshop also discussed the findings of the Cloud Evidence Group and proposed solutions. It was generally agreed that the solutions were needed urgently, because practical problems are already impacting the criminal investigations.

- The workshop welcomed the CEG proposal to continue dialogue and engage in closer cooperation with service providers which include having joint meetings once a year.

- The use of a common database maintained by the 50 Parties and the service providers could be a valuable resource. In this sense, the Parties should maintain and update the information about what are the powers that can issue production orders and the service providers should maintain and update the procedures to address correctly requests to them.

- Finally, it was noted that as the Convention may not provide all the solutions and the scope of the Guidance Note is also limited, an additional protocol, as proposed by the CEG, might solve many problems, including the legal basis for requests, and pave way for more effective cooperation.

Workshop 4: Terrorism and information technology: the criminal justice perspective

17 November 2016, 09h30 – 13h00, Room 1 Palais (Chatham House Rules)

Moderator: Catherine Smith (Australia)

Rapporteur: Andrea Candrian (Deputy Head of Criminal Law, Federal Office of Justice, Switzerland)

This workshop addressed the issue of terrorist misuse of information technology such as cyberattacks against computer systems, including critical infrastructure, or their use for logistical purposes, including the planning of terrorist attacks. The dissemination – often via social media - of illegal contents, including terrorist threats, promotion of or incitement to terrorism, recruitment or training, xenophobia, racism or other forms of hate speech contributing to violent extremism, radicalisation and terrorism was also discussed. The workshop was the occasion for criminal justice authorities and private sector to share their views, look at cooperation mechanisms and discuss improvements and solutions.

DISCUSSIONS

- The workshop started with an overview of existing international instruments countering terrorism, terrorism related offences and criminal acts that may lead to the commission of terrorist offences both at the Council of Europe level and at the United Nation Counter Terrorism Executive Directorate (CTED) level. These instruments cover different aspects such as recruitment, training or traveling abroad for terrorist purposes. The criminalization of preparatory acts in view of committing terrorist offences addresses this new trend.

- At the practical level, the need to establish central authorities with the adequate capabilities to exchange information in an expeditious manner was discussed. The Council of Europe is establishing currently a 24/7 network for exchange of police information in this matter.

- Ukraine, Estonia and France shared their experiences regarding major threats and difficulties encountered. The panel underlined the seriousness of such attacks causing damages against governments' websites, banking systems or national security and the importance for countries to be prepared for such attacks. Also, it was stressed that further efforts should be undertaken in order to counter such type of attacks. Countries should, where necessary, strengthen their own security system in order to avoid that their own infrastructure is being used for that purpose. One of the threats mentioned is the offer of cybercriminals to sell their services online to terrorist groups.

- The panel also discussed the consequences on the use of encryption from a criminal justice perspective. Increased use of encryption, with end-to-end encrypted messaging systems makes criminal investigation. It was emphasized, however, that effective means of encryption are essential in view of protecting privacy and fundamental rights such as freedom of expression as well as regarding commercial purposes. Private sector is of the opinion that a broader approach should be considered, and stressed that both users and system need to be secured, internet as a secured system helps also under developed economies. Therefore any regulation on encryption should not be seen only from a criminal justice perspective.

- Two perspectives on hate speech versus freedom of expression were briefly presented. Freedom of speech is not considered as an absolute right by the European Court of

Human Rights. Therefore freedom of speech cannot be used to deny the holocaust. From the US perspective, freedom of speech is also not an absolute right and can be restricted, however hate speech should produce imminent violence in order to be criminalized, the speech in itself is not enough.

CHALLENGES

Presentations and discussions during the Workshop made clear that:

- The Internet, social media and means of electronic communication is also used by terrorist groups or groups and organizations supporting the commission of terrorist acts,
- Territorial boundaries are no longer the relevant element for determining jurisdiction and resolving the issue of competence
- Attacks on critical infrastructure do not only have severe consequences on our daily lives, but threaten confidence of the public that is put into the State and its services (in the period of the attacks in France, there was a significant increase of Internet attacks against protected IT-systems, for example in relation to mass media such as TV-stations or public services, in the country)
- Industry: Beside cooperation with LEA, they emphasize the importance of the voluntary provision of information and a regular, established exchange with LEA (in both ways).
- Contribution from practitioners shows that the aspect of juvenile offenders in the context of IT-offences related to terrorism is becoming more significant.
- Encryption may pose one the biggest obstacles in view of a successful criminal investigation.

GOOD PRACTICES

- Welcome the early entry into force of the 24/7-network for the exchange of police information on travelling for terrorist purposes

- Reminding the importance of UN SC Resolutions, especially with regard to the public provocation and incitement via the Internet, taking into account basic principles such as freedom of expression, and the principles of International Human Rights.

- Emphasizing the importance of international cooperation, not only, but also with regard to the efficient implementation of UNSC Resolution 2178 by States.

- Improving cooperation with ISPs, but also taking into account the different nature of Providers and the information and data they are in a position to share.

- Importance of counter narrative.

- Spain has adopted new offences relating to terrorist acts that are very specific regarding the manner they are committed, namely by means of a computer system or via the Internet.

- Technical means (that often are of an intrusive nature) allow prosecuting authorities to read and make available encrypted messages and data. In practice, this is not only feasible, depending also on the degree of encryption. Always keep balance vis a vis civil liberties and basic rights (not competing goals, but add to each other: a balance has to be kept). Encryption is not only essential regarding rights of privacy, but also regarding safety and security of individuals and communities.

- Providers are aware of their role and their responsibilities in order to contribute to an environment that allows both the use of encryption as an essential instrument in

electronic communication and establishes the possibilities to carry out criminal investigations and proceeding, not only in the context of the countering of terrorism.

- The exercise of freedom of expression carries with it duties and obligations, such as the protection of the interest of third parties and maintaining safety and security of individuals and the general public.

THE WAY AHEAD

- Increase the capacity of law enforcement authorities to monitor social media
- Use of positive counter narrative with the help of private sector
- Treat the question of encryption with all economic actors involved, find practical and partial solutions with additional safeguards
- Increase CERTs capability
- Develop law enforcement guidelines on how to cooperate with private sector with an online resource to access to providers' policies.
- Encryption: One might think of drafting a general legal basis (on a national or international level) regulating the use of encryption and the means of LEA in order to overcome such impediments. This is not limited to the countering of terrorism. Partial solutions may be appropriate, depending on the specific area.
- Public safety and national security have to be dealt with on a policy level and cannot be left to developments that are subject to specific events or technological or commercial changes.
- Avoid polarization in the discussions regarding the use of emergency procedures by LEA and ISPs, not only in terrorism related cases, but also in other cases of criminal investigations and cases of missing persons, particularly children.
- Regarding hate speech, duties and responsibilities of internet portals should be engaged

Workshop 5a: Legislation on cybercrime and electronic evidence in Africa

17 November 2016, 09h30 – 11h00, Room 2 Palais

Moderator: Irene Kabua, Kenya Law Reform Commission

Rapporteur: Patrick Mwaita (United Nations African Institute for the Prevention of Crime and the Treatment of Offenders, Uganda)

Workshop 5a discussed good practices on legislation on cybercrime and electronic evidence in Africa and shared information on problems encountered.

Participants were guided through their country status regarding cybercrime legislation and the following observations were noted:

- There is a notable increase in ICT applications and internet penetration in the African region and consequently, on-line and computer related criminality has become a reality, with the youth being targeted as victims. Considerable efforts and commitment should be geared toward control the emergence of cybercrime in Africa using available legislative frameworks. Concerns were raised regarding the effectiveness of available legislation in a number of countries. From the country reports, it was evident that African countries were at various stages in the development of their cybercrime legislation, with some countries in bilateral cooperation arrangements by which they give necessary legal assistance to each other as appropriate, thereby setting a precedent for a wider regional/global programme of cooperation.

- Citing national legislations, the workshop recognized the efforts of national cyber-control mechanisms (*in some cases, institutionalized*) which have been set up to specifically address the challenges of deficiency in available legislation and ineffective policy, all attributed to focused consultations with the Council of Europe. All presentations expressed satisfaction with the relevance of the Budapest Convention to their cybercrime legislation.

- Based on its suitability, the Budapest Convention coupled with the available technical support from the Council of Europe through expert interventions was cited as significant and appropriate measures which should guide the review of available control measures as well as facilitate legislative reforms for effective cyber-security. The Budapest Convention was further commended for the opportunities for enhanced collaboration; including in-built mechanisms for international cooperation focused on provision of technical support and expert interventions available from the Council of Europe. Additionally, supportive measures covered in mandates of partner agencies/institutions such as UNODC, UNAFRI, AUC and ITU were readily available to provide necessary technical interventions to African countries on request.

- The workshop also recognized regional efforts in the formulation of relevant cybercrime legislation. At regional level, the African Union Convention (Malabo convention) was acknowledged for its encompassing outreach with the specific attention it gives to addressing the cybercrime challenges. Utilising the findings of a case study both the Budapest Convention and the Malabo Convention, while formulated in diverse geographical entities were noted for their complementarity to each other. At sub-regional level, reports indicated that the Budapest Convention was increasingly being used as a basis for countries' cybercrime legislations. However, considering the dynamic and borderless nature of cybercrime and the challenges attributed thereto, it was implicit that the African Union may have to consider widening the scope of coverage of the

Malabo convention to address concerns regarding modalities for international cooperation (*as opposed to regional cooperation*), harmonization of practices (*consistent with set standards*). It was also mooted that the African Union may consider making additional protocols in order to operationalize crucial initiatives in respect of mutual legal assistance, exchange of information and means of cooperation in order to bring the aspirations of the African region in line with international benchmarks regarding definition, type of offences, procedural law and international cooperation.

- The country reports mirrored the need for legislative review where legislation is available to match and address the current trends of online challenges.

- Similarly, the workshop underscored the need for legislative reforms to strengthen current inappropriate and ineffective legislation in order to align it with specificity requirements to address cybercrime.

- Regarding functionality of cybercrime legislation, it was imperative to engage with key decision makers to gain their support in drafting legislation.

- The workshop stressed the need for wide consultations and the significance of research-based findings to address realities in the process of drafting legislation and to align emerging legislation with best practices, utilizing available expertise in the process.

THE WAY AHEAD

- It is expected that the success of Africa in cyber-security will hinge in large measure on appropriate legislation.

- The offer of collaboration and reach-out by the Council of Europe is a chance the region should take up so that it can tap into available technical support.

- Consistent with its provisions, the Budapest Convention offers Africa a choice to secure its cyber space as a part of a global project securing the region's interests better by sharing into the international framework that the Council of Europe has provided.

Workshop 5b: Cybercrime legislation in Latin America – the problem of procedural law

17 November 2016, 11h00 – 13h00, Room 2 Palais

Moderator: Rodolfo Orjales (Chair, REMJA Working Group on Cybercrime, Organisation of American States)

Rapporteur: Pablo Castro (Subdirector para Seguridad Internacional Ministerio de Relaciones Exteriores Dirección de Seguridad Internacional y Humana)

Workshop 5b addressed the difficulties encountered by the Latin American countries with regard to the adoption of procedural law powers.

DISCUSSION

A brief overview of the state of cybercrime legislation in Latin America was presented and some important questions identified and discussed

- Do LATAM countries have current cybercrime legislation?
- Who are the stakeholders involved in that process?
- What have been the impediments?

- When the law would be presented in Congress?
- Does the law cover the procedural part?
- What would be the needs to carry out the process?

Regarding Argentina, Chile, Colombia, Costa Rica, Dominic Republican, México and Guatemala, the following issues were raised:

- Incomplete legislation in place
- Diverse internal process to accede to the Budapest Convention depending on the convergence of several political actors.
- Therefore, some countries have decided to accede first to the Budapest Convention and then to work on a cybercrime law (Chile).
- The Budapest Convention is still a good model of law to apply for a new legislation

ISSUES OF PROCEDURAL LAW POWERS

- Importance of the "Law culture" in Latin America. Technological changes impacted first on the criminal codes with the idea of applying by analogy physical evidence norms to digital evidence.
- Change of paradigm in the criminal process because of the change to digital evidence. In 5 years all complex criminal process will be defined by digital evidence.
- The advent of democracy in Latin American countries contributed to a change of procedural laws and a cultural change.
- The central axis of these codes is moving to an accusatory system. The protection of individual is now guaranteed compared to abuses during military governments.
- The similarity of the procedural codes in LA – many of them adopted with the advent of democracy following military rule – will allow a common approach in this region.

THE WAY FORWARD

- The Budapest Convention should be used as guidelines for developing substantive, procedural and international cooperation rules. These measures should apply in relation to any crime involving electronic evidence.
- On this basis, the new codes should include data assurance, data production orders, and make use of the Guidance Notes, and also of more innovative measures such as big data, etc., advance in standards of the Budapest Convention plus the importance of institutional changes.

Workshop 6: International cooperation: workshop for 24/7 points of contact and MLA authorities

17 November 2016, 09h30 – 13h00, Room 3 Palais (restricted to criminal justice authorities)

Moderators: Claudio Peguero (Director Planning, Development and International Cooperation, National Police, Dominican Republic)
Ioana Albani (Deputy Chief Prosecutor, DIICOT, Romania)

Rapporteur: Aleksandra Tukisa (International Cooperation Bureau, State Police, Latvia)

The participants in this workshop discussed about the strengths and weakness of international cooperation for cybercrime and electronic evidence related issues. The workshop was divided in three main parts: the first one dedicated to the functioning of 24/7 contact points, the second one dedicated to mutual legal assistance and the third one to the presentation of the online tool on

international cooperation developed by the Council of Europe under the Octopus Community platform.

The first panel addressing the issue of 24/7 contact points gathered representatives of the main three POC's networks that are handling cybercrime and/or electronic evidence related issues, that is the Budapest Convention Network of 24/7 contact points, the G7 Network and the Interpol Network. Developing practices by Canadian and Italian authorities were also shared with the participants to this workshop.

The workshop also discussed the conclusions and recommendations of the Cybercrime Convention Committee (T-CY) assessment of the functioning of the mutual legal assistance provisions completed in December 2014, which seeks to make MLA more efficient, strengthen the role of 24/7 points of contact and provide for direct cooperation across borders, promoting follow up to these recommendations. The results proved that the assessment and recommendations are relevant and up-to-date.

The second panel, addressing the issue of rendering the mutual legal assistance process more efficient gathered representatives of EUROJUST, European Commission and UNODC who shared their current developments on this subject.

Gareth Sansom, T-CY Bureau member presented the final results of the Cloud Evidence Group (CEG) with regard to the identified solutions to address the new challenges for criminal justice authorities to obtain electronic evidence in foreign jurisdictions, these solutions including making MLA process more efficient.

Giorgi Jokhadze (Cybercrime Programme Office of the Council of Europe) presented the new online tool on international cooperation currently developed by the Council of Europe under the Octopus Community network.

CHALLENGES

- MLA process is inefficient and many investigations are abandoned;
- Gathering electronic evidence from a different jurisdiction with the use of MLA requests is time consuming, not effective and it prevents the investigation, pursuit and adjudication of crime;
- 24/7 contact points are used less than expected and not for all the purposes for which they have been created;
- The succession planning for the 24/7 points of contact is limited;
- There is a distance between the 24/7 contact points and the MLA process.

DISCUSSION/THE WAY AHEAD

- The participants agreed that the functioning of 24/7 contact points needs to be further enhanced; the contact details for the POC's must be kept up-dated, with POC 's proactively communicating any modifications of their details; good practices need to be shared between POC's – a proposal of an annual meeting of 24/7 contact points was discussed and will be analyzed by the Council of Europe;
- It was agreed that the 24/7 contact points should be more used, where domestic legislation permits, for executing or facilitating the execution of MLA requests; the Romanian POC could be used as an example for this;

- There was broad support for more training for the 24/7 contacts points and for the promotion of the 24/7 contact points within their own country, including through national training academies (police, prosecutors, judges);

- The participants considered that, through the MLA process, prior informal consultations between the sender and the receiving competent authority, relative to the requirements that the request needs to fulfill, would prevent a lengthy and inefficient process;

- It was agreed that an additional protocol to the Budapest Convention on cybercrime would represent a solution for the new challenges regarding the mutual legal assistance process and could make this process more efficient.

Workshop 7: Seeking synergies: Policies and initiatives on cybercrime of international and private sector organisations

17 November 2016, 14h30 – 18h00, Room 1

Moderators: Cecile Barayre (Economic Affairs Officer, E-commerce and Law Reform Programme, UNCTAD)

Rapporteur: Joyce Hakmeh (Chatham House)

This workshop provided a platform for organisations at different levels to present their cybercrime initiatives with the aim to favour synergies and multi-stakeholder interaction.

CHALLENGES AND THE WAY FORWARD

- All actors are actively looking in their initiatives to avoid the duplication of existing efforts; they are rather synthesizing and building on these efforts each according to their specific mandate. This is proving to be challenging for the organizations, however, working towards similar goals and having an overarching objective of fighting cybercrime is helping in overcoming this challenge and is leading to a rich content.

- This being said and given the nature of cybercrime, coordination between the actors must be a continued effort, there is a constant need to bridge the gap between different actors through further exchange and through multi-stakeholders' approaches.

- A one size- fits -all approach should be always avoided and the focus should rather be on each country/ region's needs when designing and implementing cybercrime initiatives while building on regional synergies for the maximization of impact.

- Awareness raising, information exchange and capacity building continue to be main priorities around which organizations are partnering.

GOOD PRACTICES

- Organizations are working towards providing open databases and portals to governments and other stakeholders through including other organizations' resources in addition to their own (UNODC, World bank, UNCTAD)

- More tools are being made available for governments enabling them to identify their needs, develop their counter-cybercrime strategies and establish baselines to measure their progress (ITU, OAS)

- New partnership initiatives between international/regional organizations, civil society and the private sector aimed at developing joint action plans are being forged (INTERPOL, AU, CoE, CYAN, City of Milan)

- International organizations are supporting and facilitating communication between their member states (Commonwealth).

- More in-depth studies are being developed aimed at bridging the gaps between policy and technology experts and at keeping stakeholders abreast of how cybercrime develops (Chatham House)
- Online tools for capacity building are being made available for law enforcement agencies, prosecutors and lawyers able to guarantee sustainability and a wider reach (GPEN)

- Organizations are working towards harmonization and the creation of common grounds on cybercrime issues with the aim of facilitating criminal investigations (Evidence Project)

Workshop 8: Targeting proceeds from cybercrime

17 November 2016, 14h30 – 18h00, Room 2 Palais

Moderator: Dave O'Reilly (FTR Solutions)

Rapporteur: Hein Dries-Ziekenheiner (Vigilo Consult)

Workshop 8 addressed the issue of crime proceeds generated on online. The Council of Europe prepared a detailed study on this question on 2012, and in 2016, the Council of Europe and the European Union launched the iPROCEEDS project. INTERPOL, EUROPOL, the UN Office on Drugs on Crime, the Council of Europe and other organisations are developing training materials to link up financial, anti-money laundering and cybercrime investigations, often with a specific focus on "darkmarkets".

The aim of this workshop was to share experience / good practices with respect to targeting crime proceeds online, including on training programmes.

CHALLENGES

- Significant increase in commercially/economically motivated cybercrime. Private sector is the main target.
- Growing importance of virtual assets. New (eMoney) methods are faster and more convenient for users. Payment Service Providers are often cheaper; Electronic Money Institutions and virtual currencies offer anonymity. There are more and more non-face-to-face transactions.
- Many typologies of proceeds generating crime were identified – such as: Ransomware, MITM-attacks, CEO fraud or Business email compromise attacks, Banking malware, Phishing (and resale of details), Advanced Persistent Threats, Fraud, Child abuse material (CAM) made to order or streamed live, Data Breaches, ID theft and account takeover, Mass marketing fraud, Selling and trading in BIN (stolen credit card) lists, Advance Fee Fraud, Payment card and card-not-present fraud, Fraudulent websites – such as fraudulent copies of ecommerce, charity or Payment Provider website), Money mules (targeting also vulnerable groups).
  All these generate proceeds in virtual or regular currencies. An underground economy (especially on the dark web) is developing where these proceeds can be converted.

- Transactions are real-time both in banking and in virtual currencies. All proceeds (and obtained information) can be siphoned out to other jurisdictions very swiftly.
- New indicators for online laundering are needed.
- Money Laundering (ML) trends, typologies and crime scenarios are changing rapidly. There is a need for these to be continuously updated and put into regulatory guidelines/suspicious transaction indicators.
- ML/Financial Investigation (FI) functions and Cybercrime Investigation capabilities and policies/strategies are often not aligned.
- The Budapest Convention and the Warsaw Convention (on ML and Terrorism Financing) have great potential but are not effectively used.
- Increasing fraud and especially financial fraud against vulnerable groups, targeted as money mules.
- Need to clearly and unambiguously define the online crime proceeds and mechanisms to distinguish this phenomenon from more traditional laundering typologies. Online crime proceeds investigations (FI with a view to search, seize and confiscate) and the ML offence are sometimes hard to tell apart and need to be demystified for some practitioners.
- Lack of metrics to allow accurate measurement of the scale of online crime proceeds and lack of awareness of tools and training in the areas of cybercrime and on financial investigations and asset recovery.
- Need for preparation on the prosecution side to build investigative capabilities. FIUs need expertise in online (asset) investigations.
- Need for the development of continuous (CPD) training, not just for police, but also for the judiciary.
- Finding appropriate training might be difficult as the area is new and various trainings are in development.

GOOD PRACTICES

- ML/FI and Cybercrime capabilities are increasingly connected at a national level. Practical solutions are needed, such as integrating FI/Cybercrime investigations in joint teams.
- National and international cooperation with industry is used as a method to receive information better and faster.
- ML can sometimes be leveraged if Cybercrime legislation is difficult to apply (or absent)
- Some parties impose increased KYC requirements in cases where there is no face-to-face contact.
- FIU's quick intervention is often keeping the damage of a crime to society limited as transactions can be frozen and assets recovered quickly.
- As investigative strategy the following best practice was mentioned: Follow the money (fast), alternatively trace cyberattack source (secondly); and execute all warrants quickly.
- Immediate assistance from banks needs to be secured up front in a joint investigation, using single points of contact in banks and other financial organisations is preferable.
- Setting up a task force with banks, ISPs, CSIRTs, security vendors for sharing malware and threat information (UK NCA identified cases up to 1M pounds in a 3h meeting with banks).
- Using FIU powers in cybercrime investigations:
  - CAM cases where payment is made for material (live shows or made to order CAM material).
  - Linking bank accounts from anonymous actors to "real" identities on the basis of Bank intelligence on accounts (using cookies or Device ID from Bank systems) through the use of FIU intelligence gathering powers.
  - Bitcoin intelligence is often well developed in FIUs, many have analysis software for Bitcoin transactions. FIUs can also disseminate intelligence on suspicious transactions

ex officio (spontaneous dissemination) and may be able to assist in localising perpetrators.
  - Joint training and sharing intelligence between Cybercrime, Financial Investigation and Financial Intelligence Units is preferable.
- Training on cyber currencies and Darkweb using Train the Trainers approach and case studies.
- Detecting structured transactions (so called mixers) and patterns in the Bitcoin (or other cryptocurrency) blockchains to identify the source and destination of transactions.
- Mentorship programmes in capacity building and training; interagency training in the area of cybercrime and ML and especially cryptocurrencies. This could include banking authorities.
- Use of the same software platform between FIU and Cybercrime units for sharing information and reporting, like UNODC GoAML software.

THE WAY AHEAD

- Increased international cooperation and interagency cooperation domestically.
- Better training for judges, prosecutors, FIU analysts and (cybercrime) investigators to speak the same language and understand the challenges.
- Protect victims (multi factor authentication, separation of duties in payment of invoices).
- More cooperation with banks and industry by law enforcement. Trust and regular feedback are required as is regular contact.
- Cybercrime units working alongside banks and integrating with FI/FIU at the operational level.
- FIU cooperation in cybercrime cases and increased use of transaction freezing powers in cybercrime cases.
- More use of FIU powers to trace assets and identify account holders in cybercrime cases.
- Raising awareness of possibilities of the use of FIUs powers (especially in urgent cases) with the police.
- Closer international cooperation and increased trust between service providers and international partners in cybercrime investigations should be developed.
- Increased identification, seizure and confiscation of proceeds from cybercrime, capacity building in this area, national and international cooperation.

□

Workshop 9: Crime and jurisdiction in cyberspace: access to electronic evidence

17 November 2016, 14h30 – 18h00, Room 3 Palais (Chatham House Rules)

Moderator: Erik Planken (Chair, Cybercrime Convention Committee, Ministry of Justice and Security, Netherlands)

Rapporteur: Betty Shave (USA)

After introductory remarks, the jurisdiction group discussed the challenges and frustrations of obtaining data legitimately and with appropriate speed. These challenges had been discussed repeatedly in the course of the week, but among those noted in the session were:

- The availability of data
  - Does it still exist, is it encrypted, can one get access to it?
- The reliability of data
  - Is it authentic, has it been collected according to high forensic standards, has it retained its integrity?
- Conflicts of law (a problem for providers and for governments)
- Unclear and changing law and provider practices

- Data that moves, that is stored in more than one jurisdiction, or whose location is unknown
- Globally, a system that is partly voluntary and discretionary and not predictable
- Increasingly, providers rather than governments seem to make the decisions about disclosure

The group then moved to new views of the problem, particularly academic views but also practitioner and private sector comments.

The group spoke at length about a discrete issue, a possible agreement between the United States and the United Kingdom that would remove the prohibition that prevents US providers from voluntarily disclosing content to foreign government requesters.

- Next the group discussed whether traditional philosophies of sovereignty continued to be valid. It was suggested that:

  - State sovereignty differs from jurisdiction to investigate, States are not *obliged*, even according to traditional theory, *automatically* to assert their interests, and older views of territoriality are breaking down in the areas of climate protection, human rights, and elsewhere, and therefore could reasonably be challenged in the cyber sphere.

Throughout this part of the session, the group debated the pros and cons of basing jurisdiction on possession and control, location, or a balancing test.

- Some solutions discussed were relatively clear and finalized. These included:

  - the detailed recommendations in previous reports for improving mutual legal assistance, increasing direct cooperation with providers, and establishing emergency procedures in more countries;
  - the incoming European Investigations Order;
  - and insistence that basic subscriber information is crucial to initiating investigations and minimally intrusive of privacy.

- Another solution, a new protocol (with discussion of possible elements), marked out a new path to follow. There is broad support within the T-CY for a protocol.

- Themes emphasized throughout the session included that the issue has been studied for a very long time and that countries must move ahead at last, creatively, to address it. The trend of states creating their own solutions could be addressed by a common resolution, taking into account the interests of other states, civil society, and the private sector.

- Finally, the group was reminded twice about a decision of the European Court of Human Rights on K.U. versus Finland that is instructive for all regions of the world. In this decision, the ECtHR found that countries have an affirmative obligation to protect their citizens' safety, and that laws that prevent electronic investigations per se can violate human rights.