Octopus Conference 2015
Cooperation against Cybercrime

17 – 19 June 2015
Palais de l'Europe, Council of Europe, Strasbourg, France

Version 23 June 2015

Key messages

Some 300 cybercrime experts from 85 countries, 15 international and 50 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 17 to 19 June 2015 for the Octopus 2015 Conference on cooperation against cybercrime. The Conference was opened by Thorbjørn Jagland, Secretary General of the Council of Europe, and closed by Deputy Secretary General Gabriella Battaini-Dragoni.

Key messages resulting from Octopus 2015 are:

- Cybercrime is a serious threat to human rights, democracy and the rule of law. A survey among participants in the Octopus Conference showed that they do not consider that "cyberspace is basically safe, that crime and violation of rights are the exception and that offenders are brought to justice." The ability of governments to protect society against crime and the rights of individuals in cyberspace is limited.

- More effective international cooperation is needed. Full implementation of the 24 recommendations of the Cybercrime Convention Committee's assessment report on the functioning of mutual legal assistance (T-CY, December 2014) will make a difference. It is encouraging that membership and use of the Budapest Convention on Cybercrime as a legal framework for international cooperation continues to increase. Governments cannot address the challenge alone. More cooperation with a wide range of actors – industry, civil society organisations, academia and others – is necessary.

- Capacity building will remain the most effective way of helping societies address the challenges of cybercrime and electronic evidence. This approach has been promoted by Octopus Conferences for many years and is now recognised as mainstream international policy. In April 2014, the Cybercrime Programme Office of the Council of Europe (C-PROC) became operational in Romania with the sole task of worldwide capacity building. Other organisations are similarly expanding their projects and programmes.

- Criminal justice in cyberspace relies on access to data. Without data, there is no evidence, no investigation, no prosecution and no justice. The issue of access to evidence in the cloud and related questions of jurisdiction must be resolved. The Budapest Convention is the most obvious framework for solutions. The Cloud Evidence Group of the T-CY will hold a hearing for stakeholders on 30 November 2015 in Strasbourg. This may eventually lead to a Protocol to the Budapest Convention.

- The protection of victims and their rights should be put at the forefront in order to ensure the effectiveness of the criminal justice system. The impact of victims is often underestimated. More cooperation amongst law enforcement, private sector and victim services is needed.

- Radicalisation on the Internet leading to terrorism has become a major problem. The case law of the European Court of Human Rights helps define the boundaries between the freedom of expression on the one hand, and xenophobia, racism and other content contributing to radicalisation on the other. Implementation of the Budapest Convention and of treaties such as the Convention on the Prevention of Terrorism is complementary. Parties to the Budapest Convention should speed up ratification of the Protocol on Xenophobia and Racism committed through computer systems.

Octopus 2015, thus, resulted in specific proposals. Follow up by participants in the conference and their respective organisations will contribute significantly to improving the rule of law, the protection of society against cybercrime and the rights of individuals in cyberspace.

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.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Workshop summaries

Workshop 1: Capacity building on cybercrime: good practices, success stories, lessons learnt and upcoming programmes

17 June 2015, 14h00 – 18h00, Room 1 Palais

Moderators: Geronimo Sy (Assistant Secretary of Justice, Philippines)
Cécile Barayre (Economic Affairs Officer in charge of the E-Commerce and Law Reform Programme, UNCTAD, Geneva)

Rapporteur: Bojana Paunovic (Judge, Court of Appeal, Serbia)

Workshop 1 addressed capacity building as an international policy and technical assistance delivered by many international organisations such as the European Union, UNODC and the Global Forum for Cyber Expertise. Furthermore, this workshop examined capacity building in action, ingredients and lessons learnt in OAS, World Bank and project of the C-PROC. Finally, this workshop underlined best practises for judicial training for judges and prosecutors.

CHALLENGES

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

- Technical assistance requires ensuring the non-duplication of efforts. In order to avoid this we need better coordination between organizations.
- It is important to know who else is working on capacity building within specific areas.
- Creating plans for capacity building must include cultural, background and historical differences.
- Every organization should be transparent in what they are doing.

In order to achieve the determined goals, all actors should promote dialog and partnerships at both domestic and international levels. It is important to continue sharing information and define priorities.

GOOD PRACTICES

Good practices were shared by:

- The Commonwealth Secretariat working with National Crime Agency, which plays a leading role in on-line child sexual abuse.
- The Organisation of American States has organised round-tables with national stake holders in order to enforce responsibility of issues and challenges.
- New World Bank 2014 project.
- Lessons learnt from IPA project: 8 courses delivered, 140 trained prosecutors and judges on introductory course integrated; gave results because trained prosecutors/judges are regularly invited in the region to train and contribute to curricula of training institutes.
- Philippines: Institution building rather than capacity building: the institutions themselves must be established or reorganised.
- Under IPA Project establishing in Croatia a pilot centre.
- Global Forum for Cyber Expertise in Netherlands.
- UNODC

- UNCTAD: Impact assessment carried out a year after the delivery of capacity-building activities as one way to measure the impact of training activities and encourage ownership and commitment from beneficiaries.

In respects to sustainability, examples of Morocco, Senegal and South East of Europe countries shows that benefits are visible, sharing information continues after trainings, and cooperation between Judicial Academies can be improved. At the same time, countries are now in the position to synthetize best practice guidance, determining selection for participants. The best training program is one that is very concise, short and to the point.

THE WAY AHEAD

- There is a clear consensus on the imperative of mainstreaming and linking cybercrime activities to other thematic areas (terrorism, crime prevention, international cooperation).

- It is crucial to establish a registry of information with regard to the institutions and organizations that provide technical assistance.

- We should look into the future and make e-learning materials with regular updates, like Electronic Evidence guide.

- The benefit of training trainers was recognized, yet there are not enough trainers. We should work on creating a larger group of trainers capable of delivering trainings.

- A mechanism must be created for measuring achieved outcomes.

- Support of cooperation between judges, prosecutors and training institutions after training.

- Capacity building efforts will show no results if we do not establish strong links between international partners, criminal justice authorities and private sector.

- Training institutions should make an effort to include modules within their curriculum that contain information about relevant instruments on international cooperation that can be used when dealing with cybercrime cases.

- It is essential to establish the best way to meet national requirements in each country. Workshop 1 promoted acceptable solutions that meet the rule of law and human rights requirements.

Workshop 2: Evidence in the Cloud – Criminal justice access to data

17 June 2015, 14h00 – 18h00, Room 1 Palais

Moderators: Erik Planken (Chair of the Cybercrime Convention Committee, Ministry of Justice, Netherlands)
John Lyons (Chief Executive, International Cyber Security Protection Alliance, UK)

Rapporteur: Mary Jane Lau Yuk Poon (Assistant Solicitor General, Mauritius)

The workshop aimed to help identify solutions regarding the challenges faced by criminal justice authorities in obtaining electronic evidence kept in the cloud. The types of data that the criminal justice authorities require range from subscriber information to traffic data and content data. The political, legal, and technical challenges are numerous and specific focus was placed on the mutual legal assistance process.

An "challenges" report of the Cloud Evidence Group established by the Cybercrime Convention Committee (T-CY) in December 2014 was presented. It deals with the challenges and difficulties in terms of the impact of cybercrime as a threat to the rule of law and democracy. With the continuing advancement in the development of technology, there is an urgent need of finding solutions either through the creation of practical measures, the adoption of good practices or guidelines, or with the introduction of a binding additional protocol to the Budapest Convention. The said interim report has been made available online on order to encourage discussions and enable an exchange of views. The issues raised during this workshop will be further discussed and analysed by the Cloud Evidence Group until the final presentation of the report in the TC-Y meeting of December 2016 with a proposal for options and recommendations which can be adopted.

CHALLENGES

Challenges faced by the criminal justice include:

- The scale and scope of cybercrime, the different types of devices used, the users and victims.
- The technical challenges; (VPN, P2P, anonymisers, encryption, VOIP, NATs etc).
- The territoriality and jurisdiction in relation to cloud computing. Where is data stored and the applicable legal regime.
- Service providers operate under different layers of jurisdiction.
- Unclear as to which provider for which services controls which data.
- Is data stored or in transit? Is there a need for a production order, search or seizure process or interception?
- The challenge of mutual legal assistance.

A list of questions was identified by the Cloud Evidence Group:

- To whom should the request be sent for cloud evidence?
- What governs jurisdiction for criminal justice?
  - Location of data?
  - Nationality of owner of data?
  - Location of owner of data?
  - Nationality of data owner?
  - Location of data controller?

- Headquarters of the cloud service provider?
- Subsidiary of a cloud service provider?
- Territory where the cloud service provider is offering services?
- Laws of the territory where the data owner has subscribed to a service?
- Territory of the criminal justice authority?

- Article 18.1.b of the Budapest Convention makes provisions for empowering competent authorities to order a service provider offering its services in a territory of the Party to submit subscriber information relating to such services in that service provider possession or control is irrespective as to where the data is kept.
- Therefore, if a court authorizes the interception of a communication between two nationals or persons in its territory, would MLA be required even if technically the provider would carry out the interception on a server in a foreign country? Is the sovereignty of that country affected and to what extent are the rights of the defendants unprotected? Likewise for production order regarding content data.
- How realistic are governments efficiently able to attend to the increasing number of requests made under MLA? Would an increase of resources for the process of MLA not only at the level of competent central authorities but also at the level of courts, prosecution, police officers where MLA request are prepared and executed be a solution?
- What would be the reasonable time frame to obtain data from a foreign authority? Should this be defined in a binding agreement?
- Can there be a light regime for subscriber information?
- What additional legally binding solutions could be considered for an efficient criminal justice access to specified data in foreign or unknown jurisdictions within the framework of a criminal investigation?

Issues raised in discussions:

- Several US-based ISPs are willing to assist data requests from foreign LEAs upon a request to service providers, whilst providers in other countries, particularly in Europe, are less cooperative and insist that MLA (via central authority) is used.
- There is also a legal obligation on the company doing business in a specific country to comply with the existing laws in that territory.
- There is a need to rethink current practices. A call was made for a paradigm shift in regards to sovereignty and jurisdiction but is considered doubtful as sovereignty between states is a sensitive issue.
- It was further discussed that to overcome delays in obtaining data via MLA, there could be unilateral actions taken to obtain data. This could lead to a breach of sovereignty as it is difficult to determine the location and alternatives to unilateral action.
- More engagement with industry and other stakeholders is needed to obtain a better understanding of cloud services.
- There were conflicts highlighted in three areas: competing desires to investigate, divergent obligations on service providers and competing nation state interests.
- The MLA process is too cumbersome and a paradigm different from territoriality is needed.

THE WAY FORWARD

Suggestions made, include:

- Law enforcement may consider subcontracting the gathering of evidence so that there need not be a recourse to MLA sovereignty and territoriality issues. Once evidence is gathered, it is handed over for the due legal process.
- Determining the ownership as well as the holder of the data/Location of the data owner will assist in determining the location of the internet service provider.

- Legal certainty is the main driver behind the provision of secure cloud services - otherwise companies find that they are under competing jurisdictional demands. Companies must be able to answer to their customers regarding those important issues.
- The difficulties of investigating cybercrime and obtaining cross border assistance could be compared to international law regulating waterway flows through one or more countries, as well as the open skies principles that regulate the use of satellites overflying territories, or the civil aviation regulations of ICAO.
- Compel the companies operating in concerned territories to give data, as it is subject to territorial or national laws for operating business. Otherwise, companies should be disallowed to continue operating in regions of concern.
- Data protection law should not be an issue in case of law enforcement activity if law enforcement powers are defined by law.
- Transfer of data and consent are not applicable to law enforcement activity.
- Transfer of data within EU is not a problem but only becomes an issue if it is transferred outside of the EU.
- There is a need to use common language and create standard definitions within the MLA process.
- Regards to the capture and access of data by LEAs, procedures need to adapt to incorporate live forensic evidence gathering techniques. For example, when seizing a device that is switched on, it is important to capture all data in RAM and explore any connections to cloud services before switching off the device.

Workshop 3: Victims of cybercrime – Who cares?

17 June 2015, 14h00 – 18h00, Room 1 Palais

Moderators: Betsy Broder (Counsel for International Consumer Protection, Federal Trade Commission, USA)

Rapporteur: Frederico Moyano Marques (Portuguese Association for Victim Support)

This workshop addressed the human rights harms inflicted on victims of cybercrimes. Frequently, cyber and cyber enabled fraud targets fragile individuals who often endure great financial and psychological burdens long after the case is resolved. Workshop 3 discussed the impacts of cyberbullying, romance scams and identity theft on citizens online. Through highlighting the concerns and recommendations of leaders and practitioners who are on the front lines of assisting victims of cyber abuses, this workshop arrives at a set of conclusions for further preventing acts of cybercrime.

CHALLENGES

- Because victims of cybercrime are an invisible constituency, they often are overlooked by policy makers and those who assist victims of traditional criminal offenses. Yet the harms are substantial and deserve greater attention.
- The impact of cybercrime on victims is often underestimated: besides the financial harm, the social, practical and psychological consequences can be devastating. Added to this, many victims tend to not report the crimes. This may be due shame, embarrassment, or a sense of futility. Unfortunately, we learned that their misgivings might be justified, because indeed often the services for victims of cybercrimes are inadequate.
- Additionally, cooperation between law enforcement and victim services is lacking.

GOOD PRACTICES

This Workshop highlighted many projects that were built around the interconnectedness between law enforcement, the private sector, and victim services:

- **ENABLE** (European Network Against Bullying in Learning and Leisure Environments) tackles bullying in all platforms. With the support of industry members, this project builds social and emotional learning skills to help youngsters avoid bullying.

- **The Fraud Help Desk** is a Dutch help lineconsidered the go to place for victims of frauds; it also is leading the charge to protect victims of romance scams. In close cooperation with dating websites, they are raising users' awareness about the dangers that may arise from such sites, and how to detect romance scams at an early stage. .For further information on romance scams, go to the Fraud Help Desk's website to see a documentary on the impact of romance scams on several Dutch citizens.

- **The Portuguese Association for Victim Support** (APAV) launched Project Proteus. Co-financed by the European Commission and with the AG, police and others from Romania and Estonia, this network focuses on identity theft. APAV trains professionals through the creation of a best practice guide, support victims of these crimes and promotes prevention.

- In Italy, the **High Tech Crime Unit at the Public Prosecutor's Office in Milano**, in partnership with the Municipality and the local Bar Association, uses experts in various fields, including cyber, to support victims. They also provide training courses to judges, lawyers and police on new investigative procedures and techniques for law enforcement

regarding cybercrimes and have established a free-of-charge cybercrime victim support advice bureau.

- In the USA, the **FTC's consumer education program** focuses on clear, friendly and easy to follow steps for victims of cyber abuses, using our revised ID theft material as a case study. The FTC's consumer education program merges consumer education/victim support with intelligence gathering through the CSN. This makes consumer complaints available and provides de-confliction tools for qualified law enforcement bodies through a secure website.

THE WAY AHEAD

The workshop concluded with the following conclusions / recommendations:

- Victim assistance provides a valuable but too often overlooked opportunity for cooperation among law enforcement, private sector and victim services. This is an opportunity for the CoE and those here today to promote standards that address cybercrime victims' most immediate needs.

- Because law enforcement is a key point of contact with cybercrime victims, police forces should be prepared to acknowledge the crime, take a report and provide basic information to victims of cybercrime. This might be as simple as directing them to a helpful website or victim assistance program, such as the volunteer program in Milan.

- Academics should be encouraged to conduct more research on cyber victimization. This will help lead us to the best strategies and procedures for both prevention and assistance.

- We all need accessible, friendly and proven tools to promote awareness on cyber threats to consumer well-being.

- Discuss whether or not victims of cybercrime should be considered among the beneficiaries of the Budapest Convention. Establishing an international and multidisciplinary steering committee on assisting victims and promoting further workshops to encourage the identification and sharing of proven approaches was also discussed. The consideration of implementing a multi-year project to identify best practices to support the victims at the epicenter of cybercrime was also discussed

Workshop 4: Cybercrime legislation and implementation of the Budapest Convention

18 June 2015, 9h00 – 12h30, Room 1 Palais

Moderators: Zahid Jamil (Pakistan)
Irene Kabua (Kenya Law Reform Commission)

Rapporteur: Francisco Salas Ruiz (Informatic Law Prosecutor and Director of the Law in Effect System, Procuraduría General de la República, Costa Rica)

CHALLENGES

- Use the three fundamental pillars to build a solid legislation on cybercrime: basic criminal laws, procedure laws and international cooperation.

- Review different countries' legislation to see if their legal systems include the concept of "functional equivalence". See whether electronic evidence is accepted. If not, countries should elaborate on a legislative framework to accept electronics evidences and review it's effectiveness.

- Select a narrow scope or concrete criteria when defining criminal offenses.

- Analyze the European Court's sentence that limits access to evidence in order to elaborate on new laws or new accepted practices that could obtain legal access of evidences while respecting the Court's criteria.

- Tracking the effectiveness of legislation. Build a review process into legislation.

GOOD PRACTICES

- Involve all stakeholders (ministries, police, investigators, prosecutors, private sector, citizens) in a consultation process when developing legislation. Publish draft laws for comments as in Finland and the Netherlands.

- The Budapest Convention is an important guideline and source of concepts for the development of legislation. Paraguay and South Africa are good examples.

- Use technology-neutral language when drafting laws but still be specific when describing conduct to be criminalized.

- When drafting law, take into consideration case law and court decisions along with the experience and good practices of other countries.

THE WAY AHEAD

- Development of a serious national strategy against cybercrime with the participation of lawyers, legal operators, technicians and politicians. Involve and give roles to all relevant sectors as no single sector can address this alone. South Africa, Costa Rica and Japan are examples of such policies and efforts.

- Approval of accession should be part of the legislative process. Seek support to the Budapest Convention in particular in those institutions that are responsible for sending draft laws to Parliaments. Seek approval at an early stage. Sri Lanka is a good example. In Costa Rica, Paraguay and South Africa this is in process.

- Parties to the Budapest Convention need to further improve and adapt their legislation. In Sri Lanka, Belgium and Croatia this is in process.

- Identify actors that should be involved in cybercrime legislation, including procedural law. Special working groups, task forces or commissions should be established.

- Make available online resources for the training of ministries, agencies, prosecutors, judges, magistrates and other legal professionals, including possibly formal recognition or degrees for training. South Africa is training legal professionals.

- Multiply efforts to explain the need for legislation and other measures against cybercrime to politicians and decision-makers in simple language.

- Consider specialised prosecution offices for cybercrime. Argentina and Paraguay are good examples.

- Consider a common cybercrime glossary to facilitate common understanding of the phenomenon.

- Review if criminal codes already types of crimes that can be applied to cybercrime cases to avoid the need for new criminal offences.

Workshop 5: International cooperation: workshop for 24/7 points of contact and MLA authorities

18 June 2015, 9h00 – 12h30, Room 1 Palais (restricted to criminal justice authorities)

Moderators: Betty Shave (Assistant Deputy Chief for International Computer Crime, Computer Crime and Intellectual Property Section, Department of Justice, USA)
Cristina Schulman (Vice-chair Cybercrime Convention Committee, Ministry of Justice, Romania)

Rapporteur: Claudio Peguero (National Police, Dominican Republic)

The workshop examined the issues faced in the efficiency of international cooperation, which is essential for the investigation and prosecution of cybercrime and other offences involving electronic evidence. Thisincludes police-to-police cooperation, mutual legal assistance, and expedited measures to preserve electronic evidence.

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.

CHALLENGES

- MLA process is inefficient and many investigations are abandoned.
- Opportunities of existing agreements are not yet fully utilized.
- Data/statistics on MLA are not available.

DISCUSSION / THE WAY AHEAD

- There was support for establishing direct relationships with providers that are important to each country, including the major US providers. Several countries have been successful in establishing contact, setting up meetings, visiting the providers, setting up templates.
- Develop templates to use amongst the 24/7 network and with the ISP's to ensure adequacy and using the same structure in different languages.
- There was support for creating a portal for the 24/7 contact point network in which there are automated templates to generate requests in all the different languages. This would be sent through a portal via encrypted e-mail, and provide a secure discussion forum to figure out if more than one country is working in the same case or dealing with the same threats.
- There was broad support for more training for the 24/7 contacts points, make them aware of their role and what they can do.
- Develop Standard Operating Procedures (SOP) for contact points.
- Prepare a T-CY note on the role of 24/7 contact points which contact points could refer to when exercising their functions.

- Contact points change quite often. Need to make sure that when trained people are no longer 24/7 contact points their replacements are properly trained by them.

- Some support for direct passage of MLA requests between judicial authorities (where the law allows it).

- Taking small steps:
  - Numbering requests.
  - Establishing a mechanism for knowing if requests will be replied.

- Each country should promote their 24/7 contact points within their own country, including through national training academies (police, prosecutors, judges).

- There was broad support for establishing secure communication channels and encryption, including the use of PGP, to ensure information does not fall in the wrong hands.

- Several countries said they already could get traffic and subscriber information on an expedited basis.

- There was a discussion of whether foreign law enforcement can contact providers directly or not in the different countries.

- There was discussion about creating an "international production order" for subscriber or basic information.

- Some support for an additional protocol, although some people recognized it will be challenging.

Workshop 6: SOP working group on standard operating procedures for electronic evidence

18 June 2015, 14h00 – 18h00, Room 3 Palais

Moderator: Nigel Jones (United Kingdom)

Rapporteur: Steve Brown (Project Manager, Cybercrime Programme Office of the Council of Europe (C-PROC), Bucharest)

This was the first meeting of the Electronic Evidence Standard Operating Procedures Working Group under the GLACY Project that had already been established under the Octopus Community. The working group is focused on digital forensics procedures as information and advice is already available in the CoE Electronic Evidence Guide.

The workshop was restricted to criminal justice professionals.

In short, there was consensus on the need for standard operating procedures, but the infinite variation of forensics situations, local conditions and legal jurisdictions means that it is not possible to produce a universally applicable SOP. Instead, we should concentrate on producing a guide to creating an SOP with a menu of options and possibilities that can be adapted for local use. There was a lot of debate as to whether or not a documented SOP is possible. A number of experienced forensics examiners felt there needed to be more room for creativity and innovation. There is a risk that if an SOP is too prescriptive, it could become an unnecessary constraint on the investigative search for evidence. Even so, there was general agreement that digital forensics is a science with objective standards and realities.

The workshop started off by looking at a definition of an SOP and what should be contained in such a document. Suggestions were offered with the able assistance of Victor Voelzow from the German police on how to define and map the processes as well as on functional and administrative content.

It was recommended that SOPs should be clear about the training needed by people conducting certain types of examinations and that procedures need to be both understandable and defensible in court (not just juries, but judges and prosecutors too). The point was also well made that SOPS promote international confidence for evidence transmitted to other jurisdictions.

The need for training in the SOPs was also highlighted as well as the need for managers to be better trained in the content and application of SOPs for digital forensic examination.

The results of practical experience in developing SOPs internationally was presented by Mick Jameison who highlighted the importance of knowing the scope and boundaries of whatever SOP is devised. He emphasized the need to see this in the context of an overall system of management and quality. This included the need for validation of any SOP by the justice system.

Nigel Jones spoke about the role of a forensic regulator in establishing standards and of IS0 17025 on quality standards for forensics laboratories in general.

We were also fortunate to have Stephan Duguin from EC3 who was able to give a brief summary of work that ENFSI is doing with Europol on and EU funded project on a best practice manual in digital forensics. Caroline Goemans-Dorny from Interpol also mentioned the work being done on another EU funded project (the 'Evidence Project') that was discussed in Workshop 7. And we benefited from the wisdom and contributions from Eric Freyssinet who is a special advisor to the French Ministry of Interior on cybercrime. He made some valuable interventions on practical matters.

However, a special thanks goes to Sanjay Balgobin from Mauritius, Kaniskha Yap from Sri Lanka and Levy Lazado from the Philippines who shared their national experience and details of their approaches to laboratory procedure. In the Philippines we heard that the National Police have rolled out a suite of 27 comprehensive SOPs to their 7 regional forensic labs. This catalogue of SOPS is expanded as and when experience dictates. Assistant Secretary Sy also mentioned the initiative and efforts of the Philippine Cybercrime Office in developing common reporting templates.

The workshop ended with an interesting technical presentation on file analysis from Yves Vandermeer from ECTEG and the Belgian Police. The presentation illustrated his point about allowing for some creativity when confronted by a difficult set of forensic data. Vandermeer proposed that procedures should include the seizure of 'every E-thing' and suggested also that it would be useful for some kind of central repository of knowledge on the forensic characteristics of different file systems and artefacts.

Following this meeting, the CoE, with the help of various volunteers, will begin to develop a supplement to the Electronic Evidence Guide that will provide advice on the content, structure and design of SOPs related to the capture and processing of digital forensic evidence.

Workshop 7: Policies, activities and initiatives on cybercrime of international and private sector organisations

18 June 2015, 14h00 – 18h00, Room 3 Palais

Moderators: Jean-Christophe Le Toquin (SOCOGI, France)
Aminiasi Kefu (Acting Attorney General and Director of Public Prosecutions, Tonga)

Rapporteur: Norberto Frontini (Ministry of Justice, Argentina)

This workshop examined the issues faced in the cooperation and dialogue between international and private sector organizations. The workshop began with a case study on cross-border investigation, information sharing and prosecution involving Nigeria, Spain and the USA. This led the way to other presentations approaching similar issues from different angles. From all of them, the following challenges are derived.

CHALLENGES

The multiplication of initiatives and measures on cybercrime is a positive development. While attempts to "coordinate" initiatives may hinder initiatives, better dialogue and consultation between public and private sector organisations as well as between international organisations would foster synergies and effective use of resources and prevent that organisations work against each other.

GOOD PRACTICES

- The Octopus conferences serve as a platform for the promotion of cooperation and synergies between organisations and initiatives.
- A number of initiatives pursue multi-stakeholder approaches to address cybercrime (East/West Institute).
- Other activities on cybersecurity and cybercrime are based on a multidisciplinary vision and facilitate the sharing of good practices and knowledge (Cybersecurity Advisors Network).
- International organisations assist and facilitate communication between their member states (Commonwealth).
- Collaborative security and its principles are valuable tools to address the issues regarding cybercrime (Internet Society).
- Training not only regarding cybercrime but also in related matters such as e-commerce laws and data protection should be part of a comprehensive approach, especially in developing countries (UNCTAD).
- Developing online tools such as libraries, forums, contact databases, etc. are needed in order to facilitate capacity building among law enforcement agencies, prosecutors, judges and lawyers (GPEN).
- Recent research and development underline the need of harmonization of criminal and procedural law, of international procedures regarding cooperation and of languages used in the forensic field in order to facilitate criminal investigations and validity of electronic evidence (Evidence Project).

THE WAY AHEAD

- Additional spaces must be created in order to strengthen the cooperation and dialogue between private sector and international organisations.

- The intervention of generalists is needed in order to transmit concepts and knowledge from multidisciplinary approaches to different stakeholders. There is also is an urgent need to involve politicians in cooperation and dialogue regarding cybercrime.

- Principles discussed in forums should be applied to concrete issues; vague initiatives should be avoided.

- Isolated and compartmentalized work should be avoided.

- Although having a wide menu of options of collaboration and dialogue is productive, a specific mechanism should be elaborated in order to help developing countries understand where to start when dealing with cybercrime.

Workshop 8: Radicalization on the Internet: the criminal justice perspective

18 June 2015, 14h00 – 18h00, Room 3 Palais

Moderator: Andrea Candrian (Ministry of Justice, Switzerland)

Rapporteur: Ehab Elsonbaty (Judge, Egypt/Qatar)

This Workshop addressed the use of information and communication technologies (ICT) and their contributions to the dissemination of further radicalization online. While ICT's offer an unprecedented means of facilitating freedom of expression worldwide, such technologies may also be misused for the dissemination of racist and xenophobic materials, racist and xenophobic motivated threats and insult or the denial, gross minimization, approval or justification of genocide or crimes against humanity. Through discussing the increasing concerns of radicalization online, this Workshop strategized further recommendations for preventing and/or diminishing acts of racism, xenophobia, and hatred on the Internet.

Challenges

- The Workshop began with a brainstorming session on the connection to ICT's and the rising phenomenon of radicalization online. Questions were proposed as to whether or not more radicalized content is spread in the digital era and whether or not this content has become increasingly more violent. Further, the panel established that although ICT's are neither the creators nor instigators of radicalization, they do contribute to the speed of the radicalization process. Due to the development and speed of electronic mediums, large amount of materials have the opportunity to be circulated on a very large scale. Thus, there is a rising phenomenon of radicalization due to the increasing quantity of materials and the accessibility of radicalized content online. Self-radicalization was also discussed in this brainstorming session. The panel notes that although self-radicalization may happen online, it does not happen independently. Self-radicalization is further increased with the interactions to materials, interviews, videos, etc. done by others. Thus, terrorists acting alone through digital radicalization leads to increasing challenges for law enforcement.

- In this discussion, racism and xenophobia were highlighted as major contributing factors to further radicalization online. Social media was also highlighted as playing a significant role in the radicalization and recruitment of foreign terrorist fighters. For example, many radical groups such as ISIS successfully promote their groups online. In the context of criminal law, judges are reluctant to convict criminals of racism and intolerance because of the strong protections granted to freedom of speech. Thus, an obvious tension exists between freedom of expression and the enactment of xenophobia and racism online. These tensions were discussed as well as other criminal justice measures in order to combat radicalization on the internet.

- Increased propaganda was also debated within the context of digital radicalization. A question was proposed as to whether or not easier access to propaganda information and further digital anonymity has led to amplified radicalization. The example of foreign fighters, the Individual Jihad, and the Mujahedeen brotherhood online were discussed.

Good practices

- The Council of Europe's Protocol on Xenophobia and Racism committed through Computer Systems (ETS 189) was discussed. An action plan was adopted by the Committee of Minsters in May 1995 which included the implementation of the Convention on the Prevention of Terrorism and the Additional Protocol on Foreign Terrorist Fighters. When the Budapest Convention was established, a separate protocol was created in order to fight

Xenophobia and Racism online. There are currently 46 parties to the Budapest convention. 24 of these parties have ratified and 14 have signed the protocol to Xenophobia and Racism online. Further, the ECRI monitoring mechanism to the Council of Europe has used this protocol for its monitoring reports on member states. These General policy recommendations provided by ECRI aim to develop standards to combat racism and intolerance online. In this context, issues of territoriality, international cooperation, freedom of expression, and criminal legislation were discussed.

- The panel proposed a platform for citizens to report such crimes to an external authority. This would encourage self-regulation of xenophobic and racist material online. A discussion was also made on the effectiveness of blocking offensive content online and whether or not it was considered a preventative or reactionary strategy. Blocking was also discussed in the context of religion and freedom of expression online. This was defined as the "paradox of tolerance" due to the contention in determining hate speech online. Further, case law of the European Court of Human Rights and other instruments of the Council of Europe will help to balance freedom of speech versus racism and intolerance online.

- Article 17 of the European Convention of Human Rights prohibits the abuse of the rights of others. This is another important provision against racism, xenophobia, or hate speech.

- Three case studies were presented (Germany, France and Norway) to illustrate the criminal justice approach to xenophobia, racism and other hate speech.

- In Germany, important measures are taken against hate speech leading to radicalization. The question was raised whether a stronger counter-narrative was needed to counter radicalization.

- In France, the Pharos platform was established to facilitate public reporting on illegal contents already in 2009. Between the terrorist attacks of 7 January 2015 and 30 January 2015 some 29,000 reports were received related to terrorist events. Reports received are analysed, cross-checked and forward to law enforcement for follow up.

- In Norway, cases have proven that the Internet plays a role but is not the only reason for radicalization. The cases of Anders Behring Breivik and Hassan Abdi Dhuhulow were discussed. Norway has adopted an action plan for preventing radicalization and recruitment through the internet through knowledge and expertise, cooperation and coordination, prevention in the growth of extremist groups.

- In total, each representative from the panel emphasized the need for a multi-party approach in order to combat xenophobia and racism online. Through education, civil society participation in monitoring, governmental support, and the enhancement of police presence on the internet, radicalization must be effectively addressed.

The way ahead

- The panel came to the conclusion that in order to combat radicalization, racism and xenophobia online, the implementation of the Additional Protocol to the Convention on Cybercrime concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) should be promoted. Further, the findings and recommendations presented by the European Commission against Racism and Intolerance (ECRI) must be considered. Individual states should provide guidance and support to criminal justice authorities to deal with radicalization, xenophobia and racism online.

- The panel established that strengthening the criminal justice system is crucial in combatting illegal racist and xenophobic content online. However, the panel also acknowledges that the criminal justice system is not the only area of concern and States should look at this matter from all angles. Further, government should allocate more resources to monitoring racism and intolerance online. A balance must be achieved between security and liberty, whilst not compromising established human rights such as freedom of speech, pluralism, tolerance, open-mindedness, etc. Further, all actions must be prescribed by law, accessible by the accused persons, and be compatible with the rule of law. A court shall evaluate if measures taken are necessary and proportionate.

Survey results summary

Octopus Conference 2015
Cooperation against Cybercrime
Strasbourg, 17-19 June 2015

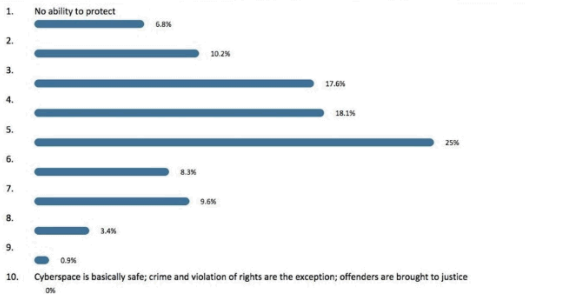
What about the rule of law in cyberspace – Survey results

- Question 1: To what extent are governments able to protect individuals/societies against crime and to defend their rights in cyberspace? (from 0 [no ability to protect] to 10 [cyberspace is basically safe; crime and violation of rights are the exception; offenders are brought to justice])
- Question 2: What are currently the key threats in cyberspace? (List in order of priority)
- Question 3: What are the main obstacles to ensuring the rule of law in cyberspace?

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

To what extent are governments able to protect individuals/societies against crime and to defend their rights in cyberspace?



Survey rule of law in cyberspace / summary of responses

2. What are currently the key threats in cyberspace?

Survey rule of law in cyberspace / summary of responses

- investigative capacities and access to rapid MLA -
- law cert cooperation
- Be member of Budapest Convention Strong law against cyber offender
- Uniformisation des dispositions législatives en matière de cybercriminalité
- insufficient policies
- criminalization ie jurisdiction, extradiction and mla
- Uncoordinated legislation and law enforcement,
- Over liberalisation
- siloed response by government and industry to cyberth
- Local law enforcement versus globally operating cyberc
- Lack of will from both government and industry to stop organise exchange of information at international level
- Lack of collaborative cyber situation awareness in most
- Inadequate laws. Bad governance.
- Consumer protection
- Lack of accountability and trust in the basic internet means that most nations don't have resources or skills to combat the threats
- Lack of data retention
- Lack of cooperation by providers, US companies
- Impossibility to trace connections
- Protection of private data, whilst admitting the necessity for law enforcement to be able to intervene in cases of criminal justice issues

Lack of policies, rules, laws, capacities

Survey rule of law in cyberspace / summary of responses

- Collective ignorance and lack of understanding at executive level
- Ignorance and carelessness,
- public awareness
- Lack of cyber security awareness
- la sensibilisation de la population sur la culture de cybersecurité
- lack of users education
- Lack of public awareness and education at high schools, universities, in-service training on a regular basis. in addition, less than 25% of countries worldwide have ratified this Convention

Awareness

Survey rule of law in cyberspace / summary of responses

- Phishing, hacking, ID theft, fraud, financial crimes
- Malware, DDOS
- Infrastructure attacks
- Offences against dignity, integrity, rights of persons
  - Child abuse, human trafficking
  - Radicalisation, xenophobia, racism, hate speech
  - Cyberbullying
  - Prostitution
- Terrorism
- Organised crime, online extortion
- Money laundering
- Darknet
- Bad hosting
- Privacy violations
- Espionage
- Use of Internet to overthrow governments

Offences

Survey rule of law in cyberspace / summary of responses

3. What are the main obstacles to ensuring the rule of law in cyberspace?

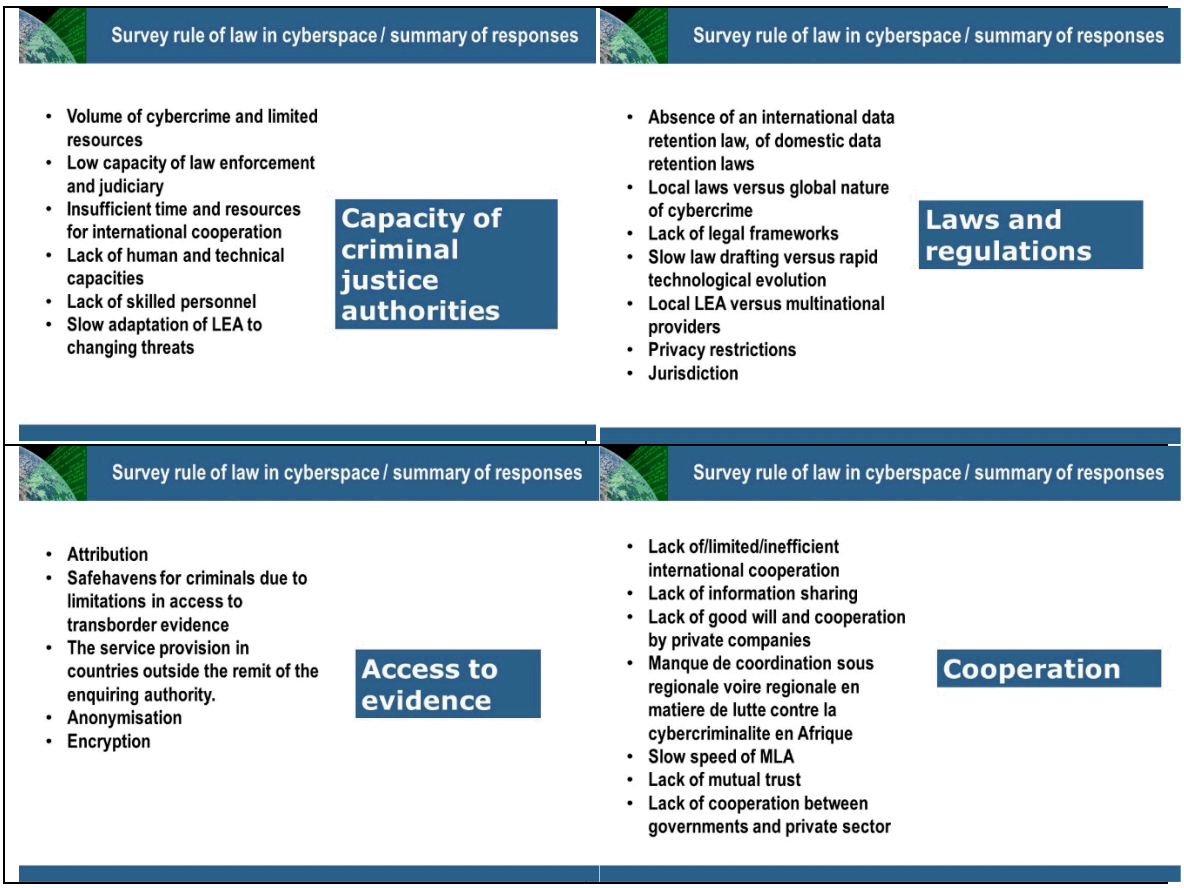
- Highly specialised cybercriminals
- Underreporting of cybercrime
- Too much crime, users, content

Scale and scope of cybercrime

Survey rule of law in cyberspace / summary of responses

- Lack of political will
- Absence de volonte politique
- Differences in policy objectives
- Sovereignty
- People exaggerating intentionally the complexity of the rule of law
- People and organisations whose interest is not to promote rule of law

Politics


Survey rule of law in cyberspace / summary of responses
Capacity of criminal justice authorities
• Volume of cybercrime and limited resources
• Low capacity of law enforcement and judiciary
• Insufficient time and resources for international cooperation
• Lack of human and technical capacities
• Lack of skilled personnel
• Slow adaptation of LEA to changing threats
Survey rule of law in cyberspace / summary of responses
Laws and regulations
• Absence of an international data retention law, of domestic data retention laws
• Local laws versus global nature of cybercrime
• Lack of legal frameworks
• Slow law drafting versus rapid technological evolution
• Local LEA versus multinational providers
• Privacy restrictions
• Jurisdiction
Survey rule of law in cyberspace / summary of responses
Access to evidence
• Attribution
• Safehavens for criminals due to limitations in access to transborder evidence
• The service provision in countries outside the remit of the enquiring authority.
• Anonymisation
• Encryption
Survey rule of law in cyberspace / summary of responses
Cooperation
• Lack of/limited/inefficient international cooperation
• Lack of information sharing
• Lack of good will and cooperation by private companies
• Manque de coordination sous regionale voire regionale en matiere de lutte contre la cybercriminalite en Afrique
• Slow speed of MLA
• Lack of mutual trust
• Lack of cooperation between governments and private sector