Octopus Conference 2018
Cooperation against Cybercrime

11 – 13 July 2018
Palais de l'Europe, Council of Europe,
Strasbourg, France

Version 19 July 2018

Key messages

Some 360 cybercrime experts from 95 countries, including representatives of 8 international and 75 private sector, civil society organisations and academia met at the Council of Europe in Strasbourg, France, from 11 to 13 July 2018 for the Octopus 2018 Conference on cooperation against cybercrime.

Key messages resulting from Octopus 2018 are:

- The participation of ministers and other senior representative from States of Africa, Asia/Pacific and Latin America underlined the global interest in the Budapest Convention on Cybercrime and related capacity building programmes. Following recent accessions by Argentina, Cabo Verde, Morocco and the Philippines, sixty States are now Party to this treaty which remains the most relevant international agreement on cybercrime and electronic evidence.

- During the past two years, cybercrime has reached even more threatening proportions affecting the security of individuals and core values of societies. Massive worldwide ransomware attacks illustrate the vulnerability of societies to cybercrime. At the same time, examples of good practice are available demonstrating that the successful investigation of transnational cybercrime is possible through enhanced international and public/private cooperation on the basis of agreements such as the Budapest Convention.

- Interference with elections through attacks against computers and data used in elections and election campaigns combined with disinformation operations, as experienced in particular since 2016, violate rules to ensure free, fair and clean elections and represent attacks against, and undermine trust in, democracy. While rules on elections need to be adapted to the realities of the information society and while systems need to be made more secure, greater efforts need to be undertaken to prosecute such interference.

- As the European Court of Human Rights has found, governments have the obligation to protect society and individuals against crime, including through criminal law. Criminal justice authorities need to be provided with more effective means to prosecute cybercrime and secure electronic evidence in specific criminal proceedings, while meeting human rights and rule of law requirements as foreseen in Article 15 Budapest Convention. Failure to reach agreement on effective means to investigate cybercrime and secure electronic evidence carries the risk that competencies will further shift from the criminal justice arena (with strong safeguards) to the national security arena.

- The Additional Protocol to the Budapest Convention – currently being prepared by the Cybercrime Convention Committee – is expected to offer meaningful ways to render mutual legal assistance more efficient while also enabling direct cooperation with providers across jurisdictions and extending searches to access evidence in the cloud with the necessary rule of law safeguards. Consultations during the Octopus Conference with civil society, data protection and industry organisations pointed at avenues to

devise solutions that would be effective while taking into account data protection and rule of law standards. The European Union's e-evidence proposals and the US CLOUD Act are relevant and consistency between all these initiatives should be ensured. Parties to the Budapest Convention may also consider accession to the modernised data protection "Convention 108+" of the Council of Europe to facilitate transborder data flows for law enforcement purposes.

- Domain name registration data is often the starting point for criminal investigations but is also used by other organisations with a legitimate interest, including privacy, consumers protection or cybersecurity organisations. Following changes by ICANN to its policies in view of the application of the EU General Data Protection Regulation in May 2018, important elements of WHOIS registration data are no longer publicly available. This is already adversely affects the ability of criminal justice authorities to investigate crime. Interim solutions are urgently required pending the development of long-term solutions. An international legal basis for requests to WHOIS data may need to be considered.

- Specific legislation, consistent with human rights and rule of law requirements, is the basis for criminal justice action on cybercrime and electronic evidence. Many governments around the world have undertaken legal reforms in recent years, often using the Budapest Convention on Cybercrime as a guideline. Some 95 States, that is, almost half of UN Member States have adopted substantive criminal law provisions in recent years. Although measurable progress is being noted and important lessons can be drawn from this experience, more reforms are still necessary, especially with regard to procedural powers for securing electronic evidence and the ability to engage in international cooperation.

- Capacity building is considered one of the most effective means to address the challenges of cybercrime and electronic evidence. Based on broad international consensus, governments, international organisations, civil society and private sector initiatives in recent years have made resources available and supported programmes in all regions of the world to strengthen legislation, provide training to criminal justice officials, promote public-private cooperation and make international cooperation more efficient. Sufficient experience and tools are now available to ensure that such programmes are designed and implemented in view of sustainable impact.

- Cyberviolence comprises a broad range of conduct that most directly affects the dignity and rights of individuals. It is often gender-based and targeting women and girls. While prevention is essential and should be given priority, criminal justice is part of the response. Better training and awareness raising of criminal justice authorities should be provided and use should be made of the tools available under the Budapest, Lanzarote and Istanbul Conventions of the Council of Europe, as well as the Protocol on Xenophobia and Racism to the Budapest Convention, whether or not States are Parties to those instruments..

- The rapid progress of artificial intelligence and machine learning raises critical questions on the future of humanity but also specific questions regarding benefits and risks related to cybercrime and criminal justice. Artificial intelligence may offer useful tools for law enforcement but may also further automate cybercrime. While criminal justice practitioners and decision makers will need to become involved and closely follow developments, fundamental questions beyond the issue of cybercrime need to be addressed urgently by societies and governments, including the matter of criminal liability and of ethical limits to uses of AI.

Octopus 2018 was the 11th 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, Hungary, Japan, Monaco, Romania, Slovakia, United Kingdom and the USA

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Programme overview

WED, 11 JULY		
Plenary session	*Hemicycle (E/F/S/R)*	
14h00	**Opening session** **Criminal justice in cyberspace: key challenges 2017/2019** **Introduction to the workshops**	
20h00 Social dinner		
THU, 12 JULY		
Workshop sessions	*Hemicycle (E/F/S/R)*	*Room 11 (E/S/F)*
9h00	**Workshop 1:** ► Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention	**Workshop 2:** ► Global state of cybercrime legislation: progress 2013 – 2018
12h30 – 14h00	*Lunch break*	
Workshop sessions	*Hemicycle (E/F/S/R)*	*Room 11 (E/F/S)*
14h00	**Workshop 1** (cont'd)**:** ► Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention	**Workshop 3:** ► Capacity building on cybercrime and e-evidence: what impact?
FRI, 13 JULY		
Workshop sessions	*Hemicycle (E/F/S/R)*	*Room 11 (E/F/S)*
9h00	**Workshop 4:** ► WHOIS: What now?	**Workshop 5:** ► Cyberviolence: challenges and responses
12h30 – 14h00	*Lunch break*	
Plenary session	*Hemicycle (E/F/S/R)*	
14h00	**Plenary:** ► Results of workshops ► Futures: artificial intelligence and cybercrime ► Concluding panel	
17h00	*End of conference*	

Workshop 1 – Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention

12 July 2018, 9h00 – 18h00, Hemicycle, Palais

Moderators: Cristina Schulman (Ministry of Justice, Romania) / Pedro Verdelho (Office of the Prosecutor General, Portugal)

Rapporteur: Betty Shave (Consultant, USA)

Secretariat: Alexander Seger (Executive Secretary, Cybercrime Convention Committee, Council of Europe)

Workshop 1 was an opportunity for the Cybercrime Convention Committee (T-CY) to seek the views and benefit from the experience of civil society, data protection organisations and industry in view of the preparation of the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime.

A discussion guide was made available to structure the workshop and to give participants an idea beforehand of exactly what would be on the agenda. The session was conducted under the Chatham House rule. There was active participation from representatives of all parts of the private sector as well as from country representatives.

The discussion was punctuated by background presentations or remarks to introduce the specific questions. Topics covered in the course of the day were:

- the rationale for the protocol, the long history of preparatory work leading to it, and the overall objective of moving electronic evidence more quickly between countries in accordance with fundamental due process principles

- current European Union proposals regarding e-evidence as well as the "Clarifying Lawful Overseas Use of Data Act," or "CLOUD Act," recently enacted in the United States

- the effort to make classic mutual legal assistance more efficient and, as a corollary, to establish new ways rapidly to move electronic evidence between countries. This corollary is important because of the urgency and indispensability of obtaining electronic evidence in an increasing proportion of cases. The topic was introduced by an explanation of the T-CY Recommendations of 2014 and implementation by Parties. Under this heading, the group discussed the two extant provisional drafts, which relate to emergency mutual legal assistance and the language of requests.

- direct cooperation with providers across jurisdictions; voluntary disclosure [of subscriber information] by service providers (speakers emphasized that subscriber information is crucial to the beginning of most investigations); and preservation requests.

- direct cooperation with providers across jurisdictions; mandatory production orders across jurisdictions.

- access to data in the cloud, often referred to as "transborder access" to data; concepts of jurisdiction. In these connections, the group discussed the types of connections that justify accessing data and asserting jurisdiction, including whether to focus on the location of the data or of the person who possesses or controls the data.

Throughout the session, there was repeated emphasis on attention to human rights as the protocol is negotiated and on data protection, both in general and in the sense specific to the European Union.

Further information and drafts of text and explanatory report sections will be released as the negotiations progress. The next physical consultations are planned for the afternoon of Monday, 26 November 2018, in Strasbourg, and would be open to interested persons as in the 12 July session.

Workshop 2 – The global state of cybercrime legislation: progress and lessons learnt 2013–2018

12 July 2018, 9h00 – 12h30, Room 11, Palais

Moderators: Zahid Jamil (Barrister-at-law, Jamil & Jamil, Pakistan) / Karuna Devi Gunesh-Balaghee (Ag Parliamentary Counsel, Attorney General's Office, Mauritius)

Rapporteur: Jayantha Fernando (Legal Advisor/Program Director – Policy & eLeadership, ICT Agency of Sri Lanka)

Secretariat: Giorgi Jokhadze (Project Manager, C-PROC, Council of Europe) / Cristina Ana (Senior Project Officer – Legislation, C-PROC) / Ana Elefterescu (Project Officer, C-PROC

Workshop 2 aimed at reviewing progress made worldwide during the past five years in terms of legislative reforms on cybercrime and electronic evidence, including examples of good practices and problematic areas, based on findings from background desktop study on the state of cybercrime legislation, completed by the Council of Europe in 2018. Specific legislation, consistent with human rights and rule of law requirements, is the basis for criminal justice action on cybercrime and electronic evidence. Many governments around the world have undertaken legal reforms during the past five years, often using the Budapest Convention on Cybercrime as a guideline; although measurable progress is being noted and important lessons can be drawn from this experience, more reforms are still necessary, especially in the domain of implementing procedural powers for securing electronic evidence and for engaging in effective international cooperation.

Challenges

- Overall, good progress was made between January 2013 and January 2018 in terms of reforms of cybercrime legislation, with almost half of the 193 UN member states (49%) having substantive criminal law provisions largely in place; an additional one third of States had adopted at least some specific substantive criminal law provisions. However, in terms of implementing procedural law powers, only 38% of states had specific powers largely in place by January 2018.

- Using compliance with the Budapest Convention or general context of fighting cybercrime as a pretext of introducing or aggravating offences of libel, defamation or blasphemy should not be acceptable. The recent example of this trend is brought forward by Chatham House study on Cybercrime Legislation in the GCC Countries published in July 2018.

- Criminal justice authorities still tend to rely on traditional procedural powers instead of specialized investigative powers provided by the Budapest Convention. Moreover, there are many jurisdictions where no distinction is drawn between categories of data (subscriber, traffic and content). Governments may be also reluctant to adopt specific procedural powers without the capacity of their authorities to apply them in practice, and further capacity building would be needed to advance.

- The case of Benedik vs. Slovenia was discussed, with inputs from Slovenia and Croatia, to illustrate a specific case of production orders for subscriber information. The discussions showed that, despite different treatment of static and dynamic IPs in some

countries, from both technical and investigative perspectives, the different treatment of the two may be irrelevant, and the judgement itself leaves the question still open for discussion.

- The results of Article 15 Safeguards Study in the Eastern Partnership region were introduced to demonstrate the difficulties for countries to properly implement specific procedural powers and the resulting challenges for keeping balance with applicable rule of law standards.

- In terms of cooperation with Internet Service Providers (ISPs), legal regulations necessary for operation of ISPs and in particular data retention requirements do not work in some countries, since the service providers do not know what data to store, or data stored is irrelevant to the cybercrime investigations. Moreover, the liability regime for ISPs is a concept specific to Europe and the US at the moment, with less presence in other regions.

Good practices

On substantive criminal law and protection of human rights, the following examples were noted:

- Stressing the importance of following existing legislative models and conducting comprehensive legislative gap analysis against the Budapest Convention (Botswana);
- Importance of judicial guidelines and practice providing interpretation of laws related to cybercrime that would render the courts more proficient in applying the law (China);
- Importance of establishing and then testing the practice against thresholds (for example, for extraterritorial jurisdiction, what is the "serious harm" justifying extended reach), consulting with wide array of stakeholders, taking into account technological neutrality for definitions, and keeping constant review and improvement of law to keep it aligned with the needs of the investigations (Singapore).

- Introducing definitions of offences that are wide enough to survive the test of time, but not as general as to be applied arbitrarily (Sri Lanka).

- While drafting legislation on cybercrime, including crimes like defamation, harassment and stalking as part of the cybercrime law provisions, analysis against the general criminal law provisions is necessary and moratorium on application can be used as a policy decision (Singapore).

On procedural powers and applicable safeguards/guarantees:

- With regard to production orders the recent T-CY Guidance Note on Article 18 of the Convention, it was emphasized that it is a measure to be applied in specific cases in regard to specified providers (Mauritius).

- Implementing procedural powers in national legislation should also provide for a degree of flexibility, balanced between law requirements that are necessary for a productive investigation and ensuring protection of human rights (Estonia).

- In terms of ensuring cooperation with ISPs, best practices examples provided stressed the importance of proper legislations and clarity of law (e.g. telecommunication laws distinctly specifying what kind of data is to be stored) so that the dialogue with service providers is more efficient (Croatia, Netherlands). Capacity building efforts to start and sustain productive dialogue between the stakeholders may lead to conclusion of cooperation agreement between the parties (C-PROC).

- Introduction of innovative, albeit controversial powers, to search of computer systems and data beyond national jurisdiction is a bold step forward that may serve as basis for further debate and balancing solutions from the viewpoint of safeguards and guarantees (Singapore).

The way ahead

- Good progress has been made in introducing substantive legislation on cybercrime. Introducing definitions of offences in flexible and technologically neutral manner, as well as maintaining constant review to this effect, should contribute to long-term stability, clarity and predictability of law.

- The balance between the need to investigate and prosecute cybercrime and the need to protect the freedom of expression should be maintained, perhaps with the use of policy decisions to minimize criminal law response where applicable.

- Procedural law reforms should focus on introduction and application of specialized powers – as opposed to traditional procedural means – for securing electronic evidence, based on definition and treatment of different categories of data (subscriber, traffic and content).

- There is a dual obligation of the law enforcement and justice system in every country to protect both human rights and fundamental freedoms and to protect its citizens against crime. Balance must be found in all national cybercrime laws between the two obligations;

- Introduction of procedural powers under the Budapest Convention should take into account the context of cooperation and related legal frameworks, addressing international cooperation between state in criminal matters and public-private partnerships with Internet industry to ensure efficient access to data.

- National dialogue and multi-stakeholder approach to both development and review of cybercrime legislation should contribute to its clarity and practical application.

Workshop 3 – Capacity building on cybercrime and e-evidence: what impact?

12 July 2018, 14h00 – 18h00, Room 11 Palais

Moderator: Panagiota-Nayia Barmpaliou (Attorney-at-Law and Cyber Policy Expert, Greece)

Rapporteur: T. George-Maria Tyendezwa (Assistant Director | Head, Cybercrime Prosecution Unit, Federal Ministry of Justice, Nigeria)

Secretariat: Marie Agha-Wevelsiep (Project Manager, CyberSouth, C-PROC, Council of Europe) / Manuel de Almeida Pereira (Project Manager, GLACY+ Project, C-PROC, Council of Europe)

The aim of the workshop was to identify metrics to measure impact of capacity building programmes on cybercrime and e-evidence.

Capacity building is considered one of the most effective means to address the challenges of cybercrime and electronic evidence. Based on broad international consensus, governments, international organisations, civil society and private sector initiatives in recent years have made resources available and supported programmes in all regions of the world to strengthen legislation, provide training to criminal justice officials, promote public-private cooperation and make international cooperation more efficient.

Challenges: how to measure impact?

The challenge of capacity building programmes was identified from different perspectives: the delivery of ad hoc trainings without any consistency and any balanced approach, the lack of coordination within donor networks and the absence of aligned policies between implementers. Redundancy and non-aligned policies result in dead-aid, therefore metrics are important both in the project design and project implementation phases. Further, countries receiving these capacity building programme should also have a political commitment to use these projects to fill in identified capacity gaps.

Many organisations are trying to address these challenges such as the Global Forum on Cyber expertise, the World Bank, the Government of Netherlands, Chatham house, the Council of Europe, the European Union and Interpol.

From the perspective of donors

International organisations have been working in the past years to create tools to help to measure capacity building impact.

The World Bank and the European Union presented their tools:

The World Bank developed a Toolkit on "Combating Cybercrime: Tools and Capacity Building for Emerging Economies" (www.combattingcybercrime.org). The Toolkit provides countries best practices in terms of policy, legal and criminal justice aspects in the fight against cybercrime. The Toolkit has also an assessment tool to allow countries to self-assess their current capabilities on cybercrime and hence identify their own priorities.

- The Tool has 9 dimensions using about 100 indicators on policy framework, legal framework, Substantive Criminal Law, Procedural Criminal Law, e-Evidence, Jurisdiction, Safeguards, International Cooperation and Capacity-building to allow to assess the level

of readiness of capacity building. The tool helps to have a baseline to analyse the situation at a point in time and then measure the progress made. The tool has been used to stimulate debates in the countries: results might be different if the assessment is done by a legislator or law enforcement. Thus, the contestability of the tool allows countries to have a more constructive debate to which non-governmental actors to whom the tool is also accessible can have a more substantial contribution.

- The ethos of this tool is not to duplicate and replicate and thus to have an evidence-based approach to measuring capacity building impact.

The **European Union Institute for Security Studies** presented the Operational Guide on the EU international cooperation on Cyber Capacity building which will be available online at the EC portal during this summer, that gives an overview of cyber policy, provides guidance on the design of project interventions and also proposes some metrics and indicators to measure the result of cyber capacity programming and provides concrete examples of result chains and 20 tools that organize the existing knowledge and provide a roadmap on how to think about cyber capacity building.

- The design of the project at very early stages with stakeholder analysis, conflict and policy analysis and drawing lessons from previous projects are essential to prevent redundancy and replication of capacity building programmes.

- Though helpful in the project design, some challenges remain in the implementation perspective:

    - the link between what is implemented and the outcome to be achieved.
    - the difficulty of merging different aspects such as security and rights.
    - the issue of different definitions on similar concepts.

These tools are only guiding tools and cannot be used as automated systems neither do they aim to assess the quality of legislation *per se*, so the human evaluation and decision-making remains key.

From the perspective of practitioners (judiciary, law enforcement and academia) participating in the implementation of these programmes

Practitioners confirmed the followings in terms of how to measure impact:

- The importance for countries to adopt cybersecurity policies and strategies to allow for donors to identify the priorities for each country and thus propose targeted actions.

- In terms of training, motivation is also important for future trainers for career development and the management of staff in order to ensure they keep using and grow the knowledge gained. The training of trainers approach to empower local capacities was underlined.

- UK National Crime Agency – on Measuring Law Enforcement´s Cybercrime Outputs suggests that when designing the metrics on performance and impact of technical activities we need to pose and find answers to 3 questions:

    - Are we raising the risk to cyber criminals?
        - Are we deterring UK-based individuals from attacking the UK because they fear arrest or disruption of their group?

- Are we deterring overseas-based individuals from attacking the UK because they fear arrest or disruption of their group?

- Are we raising the cost to cyber criminals?
  - Are we taking out criminal infrastructure (technical or supporting criminal groups) on which the cyber criminals usually rely?
  - Are we raising the barrier to entry to cybercrime? Are we stopping people becoming cyber criminals in the first place?

- Are we reducing their gains?
  - Are we reducing cyber vulnerabilities and protecting our assets?
  - Are we improving the response to victims?

- The metrics for all these 6 questions can be amalgamated (activity, output, key performance indicator) to see the direction of travel for each question. The currency of success, measured as Major, Moderate, Minor, or No Impact – for each individual tactical success, based on the impact on either the criminal group or the wider community. This can be across all criminality – and a regular evaluation meeting ensures consistency.

- The measuring of impact should be done at the policy/governance and technical/operational levels. At the policy/governance level, countries should have inter-ministerial coordination to bring key actors together and at the technical/operational level, the number of cases should serve as metrics to measure impact.

- Increased training and awareness does not always lead to immediate increase in number of cases, because depending on countries theses type of crimes are under reported.

From the perspective of international organisations as implementers of capacity building programmes

Both UNODC and Council of Europe and European Union Project GLACY+ underlined the importance of the strategic approach in capacity building programmes and their support to a process of change in each country rather than imposing pre-defined objectives. Thus, the number of trained staff, the measurement of effectiveness of legislation through case laws, as well as the deterrent effect of preventive measures were mentioned as possible indicators of capacity building impact.

Response to some of the challenges

The Global Forum on Cyber Expertise (GFCE) www.thegfce.com is seen to be a good venue to support a holistic approach on cyber capacity building by providing a global platform for countries, international organizations and private companies to exchange best practices and expertise. The global agenda for cyber capacity building (GACCB) of the GFCE focuses on five dimensions Cyber security policy & strategy, Incident management & infrastructure protection, Cybercrime, Cyber security culture & skills, Cyber security standards encapsulated in The *"Delhi Communiqué"* adopted at the GCCS in India in November 2017 which includes cybercrime amongst the different vectors that are part of such document. GFCE could be used as a facilitator among all international initiatives.

The way ahead

- Measuring impact is crucial, though not always as easy and quantifiable. Everyone agreed that impact of capacity building programmes does not lie only in the hands of

one actor but is equally the responsibility of donors, implementers and beneficiary countries.

- We are not starting from scratch, nothing out there is a myth. There is a lot of information and resources out there, nonetheless, many officials are unaware that the methodologies presented at the workshop exist.
- Maintaining a policy dialogue and having clear metrics in place for projects helps to show the direction to take and allows to prioritise the resource's available. In that sense, statistical figures remain key to help raise funding.

- When talking about awareness and prevention, figures are not always relevant to demonstrate impact. Thus, lowering expectations in terms of project objectives and outcomes will help to identify more practical metrics to help to answers to these three questions: "are we raising the cost for cybercriminals, are we raising the risk to cybercriminals and are we reducing the gain of cybercriminals".

Workshop 4 – WHOIS: What now?

13 July 2018, 9h00 – 12h30, Hemicycle, Palais

Moderators: Jayantha Fernando (Director/Legal Advisor, ICT Agency, Sri Lanka)

Rapporteur: Tjabbe Bos (Policy Officer Cybercrime, European Commission)

Secretariat: Matteo Lucchetti (Project Manager, C-PROC, Council of Europe)

For many years, public access to WHOIS data has been an important tool for criminal justice authorities to identify registrants of websites misused for criminal purposes. For many years, questions regarding the compatibility of this public WHOIS register with data protection requirements have also been raised.

In view of the European Union's General Data Protection Regulation (GDPR), ICANN – the organisation responsible for Internet Protocol address space allocation and management of the domain name system – put in place Temporary Specification for gTLD Registration Data effective 25 May 2018 which restricts access to the part of WHOIS information considered personal data. Consultations have been underway for some time to find solutions to permit access to WHOIS data for law enforcement and other legitimate purposes while at the same time meeting data protection requirements. ICANN is now leading a multi-stakeholder consultation aiming to adopt a consolidated policy by May 2019.

The purpose of this workshop was to help stakeholders obtain a better understanding of issues at stake in order to make informed contributions to solutions.

Challenges

- ICANN presented the revised temporary policies for access to WHOIS registration data for generic Top Level Domains (gTLDs), which also include the important [.com] and [.net] domain names.

- Participants clarified that WHOIS registration data is often an important starting point for criminal investigations, but is also used by other organisations with a legitimate interest, including cybersecurity organisations.

- It was reiterated that the GDPR, which applies to all natural persons residing in EU and to all EU citizens, does not significantly change the general principles of data protection that were already in place and that were already at stake in the original implementation of the WHOIS service. It appears though that the introduction of high levels of penalties has triggered a response from ICANN, registries and registrars.

- On the basis of temporary rules issued by ICANN, registries and registrars of gTLDs that are subject to the GDPR are obliged to redact certain elements of WHOIS registration data, which subsequently are no longer publicly available.

- In the absence of specific guidance provided by ICANN, registries and registrars have taken different approaches on how to implement these new rules, not only in how to grant access to redacted information, but also in in what information is collected from a new registrant. This has been already proven to have hampered access to redacted WHOIS data for law enforcement authorities and other legitimate users, also beyond the European Union.

- Participants to the workshop underlined a sense of urgency and provided examples of how these developments have affected their ability to investigate crimes, including cases of terrorism.

Solutions under consideration

The workshop provided an opportunity to explore possible options for solutions:

- Participants considered the effort of ICANN to work with stakeholders to provide for a permanent solution as particularly important.

- Existing practices of registries and registrars of ccTLDs were considered as a source for inspiration.

- Interim solutions that provide for access to WHOIS registration data on the basis of direct agreements with certain registries and registrars were also discussed.

- Important aspects of these solutions, including the accreditation and authentication of law enforcement authorities at national, regional or international level, were explored. The necessity for cyber security organizations to also put in place an accreditation system was discussed and possible solutions presented.

- In addition, participants discussed the possibility to have WHOIS publicly available in view of its public interest, for which a legal basis may be necessary.

- Finally, participants agreed on the importance of having a legal basis for requests to registries and registrars for WHOIS registration data, which may also be considered during the negotiation of the 2nd Additional Protocol to the Budapest Convention.

Workshop 5 – Cyberviolence: challenges and responses

13 July 2018, 9:00-13:00, Room 11, Palais

Moderator: Betty Shave (Consultant, USA)

Rapporteur: Briony Daley Whitworth (Senior Legal Officer A/g National Security Policy Branch, Department of Home Affairs, Australia)

Secretariat: Nina Lichtner and Mariana Chicu (Cybercrime Division, Council of Europe)

The workshop reviewed challenges posed by cyberviolence from a criminal justice perspective and domestic and international responses, including improved cooperation and possible synergies. This included better use of the tools available under the Budapest, Lanzarote and Istanbul Conventions of the Council of Europe, as well as the Protocol on Xenophobia and Racism to the Budapest Convention.

Concepts of cyberviolence

Discussion of cyberviolence and the types of conduct that are captured focused on several crime types and the particularities of these crime types online:

- The typology of offences that would fall under the concept of cyberviolence is wide and includes a large spectrum of forms of illegal conduct.
- There is significant concern about cyberviolence against children particularly online sexual abuse and exploitation.
- Trends of online violence also significantly target women, including technology facilitated abuse, harassment, and extensions of intimate partner violence into the online space.
- Image based abuse (revenge porn) is an example of an emerging crime type, as is self-generated images (videos) of sexual content and behaviour by children.
- Cyberviolence is a continuation of the spectrum of offline violence, and should not be treated differently dependent on the means.
- The Mapping study on cyberviolence prepared by the Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG) proposes the following definition: cyberviolence is the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.

National and international experience and responses to cyberviolence

- NGOs provided information on on-going international campaigns and studies related to abuse and violence against women online. Findings show that internet violence is not gender neutral, and cyberviolence identified in these studies targets women in the majority cases, particularly women in the spotlight such as MPs, journalists, activists and bloggers. Users who have more than one commonly-targeted characteristic – for example, people of color, members of minority religions, or people who identify as LGBTQ – may be attacked more frequently. Abuse includes direct or indirect threats of

physical or sexual violence, discriminatory abuse targeting one or more aspects of a woman's identity, targeted harassment, and privacy violations such as doxing or sharing sexual or intimate images of a woman without her consent.

- Of particular concern is the potential chilling effect that cyberviolence has on women. Violence and abuse online may thus limit their right to express themselves equally, freely and without fear, women are often silenced. In many instances the impact on victims that experienced online abuse or harassment is major such as lower self-esteem or loss of self-confidence as a result to stress, anxiety or panic attacks after experiencing online abuse or harassment.

- International standards offer valuable guidance and tools to states in tackling cyberviolence. The Lanzarote and Istanbul conventions provide guidance on substantive criminal laws that protect children and women from abuse and violence, including in the online environment. Both conventions are based on the 4Ps: prevention, protection, prosecution and partnerships. Countries outside the Council of Europe may join both conventions.

- The procedural rules and international cooperation rules in the Budapest Convention can be applied for investigation of offences related to cyberviolence, allowing for preservation and collection of electronic evidence, as well as international co-operation. Cyberviolence, by its nature, occurs online, which means that often the evidence required to investigate and prosecute these offences is controlled or located in another jurisdiction. This requires effective international cooperation.

- The Protocol on Xenophobia and Racism entails an extension of the Budapest Convention's scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist or xenophobic propaganda.

- States have a positive obligation to protect individuals from the potential harms of the internet while ensuring human rights are protected (K.U. v. Finland). It is therefore essential that states manage to strike a fine balance between sufficiently interfering in order to protect persons from cyberviolence and harassment on one hand, and respecting the freedom of expression and right to privacy on the other hand.

- Existing domestic legislation may in some circumstances be adequate to capture cyberviolence, or specific cyber offences may need to be introduced. Drafters should consider making offences technologically neutral so as to ensure they can be applied to emerging technologies and forms of cyberviolence.

- The success of international co-operation for emerging crime types can be influenced by the level of adequate criminalisation of cyberviolence domestically.

Role of service providers

- Service providers play crucial role in detection, prevention, investigation and prosecution of cyberviolence. They also play a key role in combatting forms of cyberviolence that involve illegal content, by providing mechanisms for reporting and removing illegal content from platforms.

- Participants discussed the possibility of blocking content, however industry highlighted that blocking does not offer a solution as such, whereas removal can better address the underlying abuse.

- The CoE Committee of Minister's recent recommendation on the roles and responsibilities of internet intermediaries calls on all states to provide a human rights and rule of law-based framework that lays out the main obligations of the states with respect to the protection and promotion of human rights in the digital environment, and the respective responsibilities of intermediaries.

Lessons learnt: good practices and challenges

- Education and training are thus crucial in combatting cyberviolence. Education should be provided for investigators, judiciary and prosecutors on the types of cyberviolence and how to investigate and collect evidence.

- Education is also important as a preventative tool – children, teachers, parents and the elderly must understand the risks of internet use.

- Ancillary support for victims, including counseling services, easy reporting tools, legal assistance, and financial support was identified as important by participants.

- The International Association of Internet Hotlines, INHOPE, is a collaborative global network of reporting hotlines against illegal content online and represents an example of good practice for reporting, detecting and combatting child sexual abuse online. It allows for submission of anonymous reports of illegal content and quick removal at source due to close cooperation with ISPs and LEAs, an exchange of know-how and best practice models, as well as raising awareness for illegal material.

- EU-Initiative a better Internet for Kids (BIK) is a portal for information, guidance and resources, which aims at creating awareness and information for, and providing assistance in dealing with online risks for children, adolescents, adults, youth workers and teachers.