COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Octopus Conference & Budapest Convention 10th anniversary meeting

Cooperation against cybercrime

21 – 23 November 2011

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

Version 30 Nov 11

Octopus 2011 – Key messages

Cybercrime experts representing countries from all continents, international organisations and the private sector met at the Council of Europe in Strasbourg from 21 to 23 November 2011 to review the global cybercrime situation, to share experience on effective responses and to enhance cooperation against cybercrime at all levels. On the occasion of the 10th anniversary of the Budapest Convention (23 November), the Conference included a special session on the impact of this treaty. Senior representatives of Australia, the European Union, Hungary, the United Kingdom and the USA expressed strong support for global implementation of this Convention. Experts from Argentina, Senegal, Sri Lanka, Tonga and the private sector underlined its impact and potential in different regions of the world.

Key messages resulting from plenary and workshop discussions include:

1. The challenge of cybercrime continues to increase. It is a transversal threat affecting people and their rights, generating large amounts of crime proceeds, causing major damage, and targeting economic, social, economic and security interests of societies worldwide. Cybercrime should, therefore, be considered a priority concern by all, including by decision-makers in parliaments and governments.

2. Technical assistance helps build the capacities of countries to implement standards, tools and good practices already available. The conference confirmed once more the conclusions of Octopus 2010 and the subsequent United Nations Crime Congress (Brazil 2010), namely, that there is broad consensus on the need for capacity building. Progress was made since 2010 in that new technical assistance programmes have been launched by different organisations. More programmes are required to support countries in all regions of the world.

3. International organisations should reinforce their cooperation with each other to provide a better service and more coherent support to societies worldwide. Technical assistance programmes are conducive for such partnerships.

4. Comprehensive legislation, harmonized with international standards is a key element of the response to cybercrime. The Budapest Convention serves as a guideline in this respect. Progress was made in many countries around the world since Octopus 2010. Nevertheless, the pace of adopting legislation must be accelerated.

5. Responses to the sexual exploitation of children include criminal law measures. The "Lanzarote" (CETS 201) and "Budapest" (CETS 185) Conventions of the Council of Europe provide benchmarks. The legislative engagement strategy proposed by the Virtual Global Task Force and adopted by Interpol in November 2011, will contribute to follow up in cooperation with the Council of Europe. Notice and take down should be an essential part of any overall strategy concerning child exploitation on the Internet. New technologies, such as PhotoDNA facilitate effective victim-centric identification systems. Public awareness

measures - such as the 1 in 5 campaign of the Council of Europe – contribute to preventing sexual violence. Prevention, protection and prosecution reinforce each other.

6. Specialised cybercrime units at the level of police-type agencies but also prosecution services allow for the effective investigation and prosecution of offences against and by means of computers and the forensic analysis of electronic evidence related to any crime. Good practices are available and have been documented. The strengthening of specialized units is essential to address the threat of cybercrime and meet the demand for computer forensic services. 24/7 points of contact have now been established by all Parties to the Budapest Convention. Their effectiveness should be enhanced in line with Article 35 of the Convention.

7. Cybercrime strategies – aimed at crime prevention and criminal justice – may help ensure a comprehensive response to cybercrime and other offences involving electronic evidence. They can provide a framework for a range of different measures and the participation of multiple public and private sector stakeholders. They should be closely linked to cybersecurity strategies.

8. Law enforcement needs to be provided with the powers necessary for effective investigations, but such powers need to be subject to conditions and safeguards as foreseen in Article 15 of the Budapest Convention. This – and the adoption of data protection regulations in line with Convention ETS 108 of the Council of Europe – will help ensure that human rights and rule of law requirements are met when investigating cybercrime and securing electronic evidence. The case law of the European Court of Human Rights is a valuable resource also for non-European countries

9. The Budapest Convention on Cybercrime made an impact during its first ten years. Interventions by senior speakers and subject-matters experts from different regions and the private sector in the special 10th anniversary session on 23 November confirmed that this impact is reflected in stronger and more harmonized legislation worldwide, more efficient cooperation between the Parties, and more investigations, prosecutions and adjudications. The Convention allows for global outreach, serves as a catalyst for capacity building programmes and as a basis for trusted partnerships and multi-stakeholder cooperation. It contributes to human rights and the rule of law and is an essential element of norms of behaviour for cyberspace.

   So far, 55 States have ratified, signed or been invited to accede to the Budapest Convention. With each new Party this treaty will gain in effectiveness. States therefore need to accelerate the process of becoming Parties.

   The Budapest Convention is a dynamic instrument that can be supplemented to address new challenges such as issues related to cloud computing and jurisdiction.

   The Parties to the Convention are the owners of the treaty and have a particular responsibility to ensure its effectiveness. This includes a stronger role of the Cybercrime Convention Committee, but also stronger political engagement by decision-makers.

10. The future of international cooperation against cybercrime depends to a large extent on the effective implementation of already existing standards and tools, on the removal of obstacles preventing efficient cooperation at all levels, including with respect to public-private as well as international information exchange, and the level of engagement of decision-makers. An effective approach requires cooperation by public and private sector stakeholders at all levels. Meeting the challenge of cybercrime is thus a shared responsibility.

The Octopus conference is part of the Global Project on Cybercrime and has been made possible by voluntary contributions from Estonia, Japan, Monaco, Romania, Microsoft and Visa Europe, as well as from the Budget of the Council of Europe.

Summary of plenary and workshop discussions

Update session

This session provided updates on:

- Threats and trends of cybercrime (Symantec)
- The scale of online sexual exploitation and abuse of children (Interpol)
- Threat assessment of Europol
- The state of information security in Europe (ENISA)
- The role and responsibility of CERTs (CERT-LEXSI)

The session underlined the scale and impact of cybercrime and thus the need to enhance cooperation at all levels. Decision-makers need to be made aware and need to be become more engaged in devising and adopting criminal justice and other responses.

Furthermore it provided an overview of:

- The activities and role of the Cybercrime Convention Committee
- Relevant developments in Argentina, Benin, Botswana, Cambodia, India, Nigeria, Niger, Pakistan, Paraguay, Peru, Philippines, Russian Federation, Tanzania, Tonga and Uzbekistan.

Discussions confirmed the progress made in many countries towards cybercrime legislation and the use of the Budapest Convention as a guideline.

The session also drew attention to new challenges related to cloud computing, roaming services, GEO-location, mobile phones, and others.

Workshop 1 – Capacity Building

The workshop provided an overview of the capacity building activities in the fields of judicial training, law enforcement in different participating countries as well as of the technical assistance delivered by the Council of Europe, the initiative of the Commonwealth and capacity building activities by the UNODC.

Challenges

While most countries are concerned about the growing threat of cybercrime many tools and instruments against cybercrime are already available. However, these are not necessarily implemented in all countries and regions of the world, nor is there necessarily longer-term sustainability built within countries. Common and urgent efforts to strengthen legislative frameworks, criminal justice capacities, international cooperation and public/private cooperation, the protection of children and measures against criminal money flows on the Internet are therefore required based on tools and instruments already available, or easily adaptable. Additional resources will be required and efforts would need to be undertaken to facilitate access to development cooperation funds for measures against cybercrime.

Good practices

In the context of the Global Project on Cybercrime of the Council of Europe and the joint projects with the European Union (CyberCrime@IPA and CyberCrime@EAP), the following aspects were underscored:

- Implementation of different projects need to consider also raising awareness among policy makers and legislators about the need to take measures against cybercrime.
- Technical assistance requires work at different levels and with all institutions responsible in order to make a sustainable impact. This is also beneficial for inter-agency cooperation.

- Sustainable training should be available for police, prosecutors and judges as well as for agencies dealing with anti-money laundering and financial investigations.
- Setting up regional pilot centres for judicial training is a good practice and provides a good basis for a better regional and global cooperation.
- Sharing good practices and tools have provided great benefit for countries.

It is important to create awareness with respect to the urgency that exists for moving forward beyond the talk and urgently implement, in substance, the various tools and capacities required in many countries, especially developing and small countries.

It is good practice for all actors to leverage what is already available including existing legal instruments, resources and tools as opposed to reinventing the wheel. Stakeholders should work collaboratively and cooperatively on the basis of 'many partners – one team'.

Efforts should leverage existing basis and unique compatibility of various forums and the valuable traditions for instance, common language, the common law or other shared values to create awareness, build capacities and assist in the implementation of convergent, consistent and compatible legislation, procedures and legal assistance provisions and work with policy makers, legislators, law enforcement, prosecutors, judiciary and the private sector. An example is the Commonwealth Cybercrime Initiative.

Capacity building should also address the various structures adopted by cybercriminals including distributed networks, which may not necessarily fall within traditional definitions, such as organised crime, and may range from lone wolves, loose associations and organised groups. Capacities need to be collaboratively developed and implemented by all actors to address these aspects and enable speedier global cooperation, which should also include the private sector.

Developing capacities of prosecutors to present 'virtual evidence' for the better understanding of juries and the judiciary can play an important role in improved prosecution of cybercrime. Establishment of databanks that share information about points of contact and other resources from centralised repositories such as GPEN play an important role in contributing to international cooperation for combating cybercrime.

Capacity building efforts can also facilitate advancement of policy, legislative, regulatory and harmonisation efforts for specific nations through collaboration of various stakeholders of participating nations such as the outcome of the Regional meeting in Colombo.

The way ahead

- The scope and size of the problem is vast enough that no one entity can alone address it. All actors have a role to play and should cooperate with each other within their respective mandates on an urgent basis.
- The only way to adequately address this challenge moving forward is for many partners to work as one team.
- It is important to address all elements (LEA, prosecution, judiciary, policy makers and the private sector) of combating cybercrime thereby avoiding 'weak links'.
- Capacity building should focus on harmonisation and on a convergent, compatible and consistent basis using existing legal instruments, resources and tools rather than reinventing the wheel.
- Capacity building is not a one-off endeavour but requires sustainable, layered, phased and continued efforts.
- Public-private partnerships should be encouraged to effectively deliver capacity building.
- Efforts should include both developing as well as developed countries.

Workshop 2: Specialised services

The workshop examined the issues faced in the development of specialised law enforcement cybercrime units and the 24/7 points of contact provisions and requirements as set out in Article 35 of the Budapest convention. The workshop heard case study presentations that highlighted some of the challenges of dealing with cross-jurisdictional malware investigations and received a report from the authors of the cybercrime units good practice study conducted by the Council of Europe.

Challenges

Case study presentations highlighted the following issues:

- The challenge of being able to deal with investigations that transcend many international borders, including identifying appropriate and knowledgeable contacts in other countries.
- The dilemma about when and how to take down Botnets and the identifying the legal and practical considerations
- How to deal with victims of crime, for example those that may not aware that they have been infected by malware.
- The challenges of investigations involving countries where some have ratified the Budapest convention and others have not.
- The importance of having access to a judiciary knowledgeable of cybercrime issues.
- The challenges faced by countries that are seeking to develop cybercrime strategies and LE units, with no experience to call upon.
- The effect of time-consuming and sometimes frustrating cooperation with third countries. In particular the pressures on countries that are either often the recipients of attacks or jurisdictions which receive large numbers of requests due to the prevalence of attacks from their countries
- The potential issues raised by countries that do not fully implement the 24/7 points of contact requirements.

Good practice

A number of good investigative practices were identified within the case studies and these include:

- The importance of the creation of effective law enforcement cybercrime units in countries.
- The importance of having specialised cybercrime prosecutors and/or prosecution units.
- The benefits of joint working of law enforcement and prosecutors throughout the investigation process.
- The importance of having clear lines of communication between investigators/prosecutors in different countries.
- The advantages that may be accrued during investigations by having established relationships in place with the Internet industry, CERT's and other public and private parties.
- The set up of cybercrime units same organizational level as economic crime and other similar units rather than being subordinate to one or more of those units.

The good practice study on specialised cybercrime units was created to help public authorities create or further strengthen specialised cybercrime units as a key element of the response to cybercrime. It is recognised that both law enforcement and prosecution authorities require a specialised response to the issues raised by cybercrime. The study concentrates on the development of police type of law enforcement specialised units; however it is of value to prosecution departments that are seeking to create their own units or seeking to up the skill of staff within existing offices to deal with cybercrime. The study provides examples of different types of units that may be created and will be of value to the target audience.

The way ahead

The workshop made the following recommendations as a result of the consideration of the issues raised by the presentations and following discussions:

- Taking into account the issues faced in the Netherlands case, consideration should be given to the implementation of legislation that authorises law enforcement and/or industry with appropriate criteria to take measures to warn users and/or remove botnets. Appropriate guidelines measures detailing actions that may be taken, should also be developed.
- The Council of Europe should consider providing advice and guidance workshops for countries/regions setting up units with others who have set up units. The potential for virtual workshops should be considered. A specific request for such a workshop was made on behalf of the East Africa region.
- The Council of Europe should consider developing a guide setting out the steps on how to establish or update a cybercrime unit.
- Development of a document dealing with a structure for fighting cybercrime. This should enable discussion on the evolution of technology and criminal trends how to fight cybercrime in the future.
- The Council of Europe should conduct a study on the creation of cybercrime units specifically aimed at prosecution services.
- Emphasis should be made on the importance of cascading knowledge and skills across law enforcement in order that responsibility for investigations may be spread more efficiently.
- The Council of Europe should continue its efforts in encouraging countries to create effective 24/7 points of contact with particular emphasis on the importance of organisations being nominated rather than individuals. The organisation should be responsible for managing access to individuals. Regular checks on the 24/7 points of contact list should be made by the Council of Europe to ensure that redundant information is not present, as well as ensuring the effectiveness of the network of contact points. Countries should also be encouraged to use the 24/7 regime in advance of the issue of letters rogatory; as well as a resource for identifying experts within country.
- Countries should also consider developing 24/7 processes such as appropriate contacts with industry, CERTS and other relevant public/private parties on that basis.

Workshop 3 Cyber Crime Strategies

The workshop discussed the cybercrime strategies and provided an overview/comparison of how cybercrime strategies and Cybersecurity strategies interact with one another in the effort of governments and private sector to tackle cybercrime.

An overview of what was meant by Cybercrime and Cybersecurity strategies was presented through the Council of Europe Discussion Paper, including fine distinction between the two and cases where they overlap. The general conclusion from the presentations was that while the main aim of the Cybersecurity strategies was to ensure the confidentiality, integrity and availability (c-i-a) of computer data and systems and to protect against or prevent intentional and non-intentional incidents and attacks, the cybercrime strategies provide a criminal justice response to c-i-a attacks against computers and thus complement technical and procedural cybersecurity responses. In addition Cybercrime strategies also deal with offences committed by means of computer data and systems, ranging from the sexual exploitation of children to fraud, hate speech, intellectual property rights (IPR) infringements and many other offences.

Challenges

The discussions and presentations highlighted the following issues:

- Considerations whether countries should adopt Specific Cybercrime strategies in addition to Cybersecurity strategies

- Creation of overall strategies that would encompass both Cybercrime and Cybersecurity components;
- Ensure that criminal justice/rule of law principles – including safeguards – are taken into account, also in Cybersecurity strategies
- Need to increase the level of technical assistance to countries that don't have capacity to create such strategies
- Due to the nature of cybercrime the Cybercrime and Cybersecurity Strategies should take into account the need for greater international cooperation, including here the consideration for harmonized legislation (Consider the Budapest Convention on Cybercrime as the tool for such harmonization);
- Capacity to "expedite" cybercrime investigations

Good practices

A number of good practices were presented, and these include:

- Holistic approach to establishing strategies that contain both the Cybercrime and Cybersecurity components
- Establishing of Offices with authority to coordinate the efforts against cybercrime activities (example from Canada)

The way ahead

The workshop made the following recommendations:

- Increased cooperation between the governments, NGOs and private sector in the establishing and implementing the cybercrime and Cybersecurity strategies.
- Increased cooperation through Public Private Partnerships as well as improved cooperation between players in the private sector
- Enhance Cybercrime components within Cybersecurity strategies.
- Mainstreaming of law enforcement response to cybercrime.
- Within the Global Project against Cybercrime the Council of Europe will continue to support countries in their efforts to tackle cybercrime through the establishment of effective cybercrime strategies. Attention should be given to West and East African countries.

Workshop 4 Responses to the sexual exploitation of children

The workshop examined the legislative, technological impacts and limitations (that is, notice and take down) and preventive aspects of the responses to the sexual exploitation of children.

The Council of Europe together with INTERPOL, European Commission, Virtual Global TaskForce, International Center for Missing and Exploited Children, European NGO alliance for child safety online, Association des Fournisseurs d'Acces at de Service Internet, InHope and Microsoft all agree on the importance of developing and harmonising national legislations in place with the relevant international legal instruments.

Challenges

The presentations highlighted the following issues:

- There are international instruments providing the standards to develop and harmonise legislation in place, in particular the conventions on cybercrime ("Budapest Convention") and on the protection of children from sexual exploitation and sexual abuse ("Lanzarote Convention"). These treaties are open to any country to accede, and countries were encouraged to make use of them as a foundation for creating national legislation.

- Notice and take down is an essential part of any overall strategy for dealing with child exploitation on the Internet and therefore part of any broader child protection policy. It can be used independently of or in conjunction with any blocking strategy based on National legislation or any other technical solutions, such as PhotoDNA, disruption or arrest and prosecution of offenders.
- Prevention has a massive role to play in the protection of children. Prevention is always better than cure thus awareness raising activities are key instruments of preventive.

Good practice

Good practices were introduced during the workshop including:

- The use of the Budapest and Lanzarote Conventions as legislative benchmarks.
- The work of the Virtual Global Taskforce, including its legislative engagement strategy.
- PhotoDNA, which is designed to improve detection and reduce availability of CAM is a very good example of a technical solution. Developed by Microsoft it makes the finding of CAM easier on networks. Microsoft makes the source code available for free and encourages other companies to implement it on their networks.
- The Council of Europe has developed the ONE in FIVE campaign to stop sexual violence against children. This age-appropriate, easy-to-use, and comprehensive material is available in 25 different languages. It allows for awareness raising at all ages, not as a scare tactic but as a preventative measure.

The way ahead:

Law-enforcement, Government and Non Governmental Organisations must cooperate and leverage their disparate skills to influence change at all levels in society and to have increase awareness in this area. Awareness and empowerment of children remains the most effective means of protecting them and every opportunity to raise awareness should be encouraged and grasped.

Speakers and participants called on everybody to acknowledge that child sexual abuse is a societal issue and that the use of the Internet by those who have a sexual interest in children is a growing part of that problem.

- Create and develop national legislation and associated procedures to underpin all activities in this area.
- Develop new technologies to assist with this ongoing problem.
- Develop a victim-centric identification system within their territories and to link it to the existing International effort.
- Develop a hotline or other reporting mechanism to allow their citizens to report online, any issue which causes them concern.

Panel: Article 15 – protecting you and your rights in cyberspace

The panel explained the purpose and requirements of article 15 on conditions and safeguards of the Budapest Convention on Cybercrime.

The report on the Internet case law of the European Court of Human Rights illustrated that this case law is a valuable resource also for non-European countries.

The discussion of the report on Article 15 by Professors Henrik Kaspersen (Netherlands) and Joseph Schwerha (USA) showed that Article 15 of the Convention on Cybercrime does not set new safeguards and conditions but instead requires that countries apply the safeguards and conditions foreseen under their domestic legislation and in international treaties that they are Parties when implementing the procedural powers of the Budapest Convention.

Article 15 specifically mentions that State Parties should provide for the protection of human rights and liberties pursuant to obligations undertaken by ratifying the 1950 CoE convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political rights and other applicable international human rights instrument. The most pertinent article from the European Convention on Human Rights relating to the implementation of Article 15 of the Convention on Cybercrime are Article 8 (protection and retention of personal data falling within private life) and Article 10 (right to hold opinion without interference, right to freedom of expression, freedom to seek, receive and impart information), a structured approach to these two articles provides for key safeguards against state interference.

Countries should also be encouraged to implement data protection standards, such as those of the Data Protection Convention 108 of the Council of Europe.

It was agreed that questions related to Article 15 should be addressed in capacity building programmes.

Panel Cooperation against cybercrime – what future

The panel focused in particular on the cooperation between public and private sector entities and the need for a holistic approach to tackling cybercrime. While governments are tackling cybercrime with the goal of protecting citizens against crime, the interest of the private sector in investing in the fight against cybercrime is the protection of their businesses and customers. Complementary of interests favours cooperation.

As the number of internet users is growing very fast in all parts of the world there is a need for a greater focus of efforts to support developing countries through technical assistance. There is a great need for increased international cooperation especially in providing technical assistance and training in low income countries. Such training could provided online to ensure cost effectiveness. In addition there is a need for increased coordination in efforts made by international organisations to reduce overlap and ensure results. A specific need for training centres for French speaking countries of West Africa was expressed.

One of the best ways for expedited international cooperation is the use of the 24/7 network of contact points. However, there is a great number of countries that are not yet members of the network.

EU member states have established several mechanisms for cooperation and the European Commission is currently studying the feasibility of an EU Cybercrime Centre. Although this centre is being created for member states, third countries may also benefit from the coordinated effort of EU countries.

All speakers agreed that there is a need for increased cooperation between the many stakeholders including the consideration of public-private partnerships. Panellists called on the private sector to increase their support for initiatives undertaken by the public sector to tackle cybercrime. While some major companies are very much involved already, other major private sector players seem to lack engagement.