Octopus Interface conference on

Cooperation against cybercrime

Council of Europe, Strasbourg, France, 11 – 12 June 2007

Conference summary

More than 140 cybercrime experts from some 55 countries, international organisations and the private sector met at the Council of Europe in Strasbourg from 11 to 12 June 2007 to:

- analyse the threat of cybercrime
- review the effectiveness of cybercrime legislation
- promote the use of the Cybercrime Convention and its Protocol as a guideline for the development of national legislation and encourage wide and rapid ratification and accession to these treaties
- strengthen cooperation among different initiatives by enabling stakeholders to make better use of existing opportunities and to explore new ones.

Plenary and workshop discussions resulted in the following:

1 CYBERCRIME: SITUATION ANALYSIS AND IDENTIFICATION OF NEW THREATS

The challenge

A presentation by the Europol representative, followed by a panel discussion with representatives from France, Microsoft, INHOPE and ICMEC and interventions by other participants suggested the following:

- Societies worldwide are dependent on information and communication technologies. The growth of cybercrimes renders societies highly vulnerable
- Malware – malicious codes and software, including viruses, worms, Trojan horses, spyware, bots and botnets – is evolving and spreading rapidly, and used among other things to commit denial of service attacks, identity theft (phishing and other social engineering techniques), fraud, money laundering and other economic crimes
- Spams, reportedly accounting for the vast majority of email traffic, are not only a nuisance but increasingly carriers of malware
- Offenders are increasingly organising for crime aimed at generating illicit profits
- Botnets are one of the central tools of such criminal enterprises not only for denial of service attacks and extortion but also for the placing of adware and spyware
- An underground service economy is developing, with, for example, botnets being rented out to organised criminals
- A major shift in the "threat landscape" is also confirmed by industry analysts: broad, mass, multi-purpose or even global attacks by viruses, worms and spams which attract attention are replaced by more targeted, smaller attacks on specific users, groups, organisations or sectors while seeking to avoid attracting attention. These attacks increasingly pursue criminal economic purposes
- Small and medium enterprises are particularly vulnerable as they often do not invest the necessary resources to protect their systems
- Online virtual payment systems are becoming a major concern in the USA

- The internet is misused for the sexual exploitation and abuse of children and trafficking in human beings. A large share of child pornography sites and child abuse images now appear to be of a commercial nature generating huge amounts of proceeds
- The risk of cyber-attacks against critical infrastructure (cyber-terrorism) is perceived to be increasing
- The remote storage of data creates problems with regard to the investigation of cybercrimes
- The technologies and techniques used to commit cybercrime develop rapidly and become more sophisticated. Next-generation-networks (NGN), including services such as Voice-over-IP, will pose new challenges to law enforcement.

The way ahead

Proposals made include:

- Global cooperation against cybercrime is required. Countries around the world should adhere to global standards as a basis for information sharing. Widest possible implementation of the Convention on Cybercrime will be an important step in this direction
- Public-private partnerships are an essential cornerstone of such global cooperation. The industry has a strong responsibility to cooperate with law enforcement. The challenge is to find the right balance between privacy rights and security needs
- Encourage victims of cybercrime to report; facilitate such reporting and take measures to protect witnesses
- Improve the quality and consistency of data on cybercrime, for example, through centralised reporting systems, research on cyber offenders and others
- Not just public institutions, but also the industry and other private sector organisations should continue their most valuable threat assessments and analytical work. For example, the forthcoming INHOPE trend report on child pornography and illegal content will provide useful insights
- Criminalise child pornography and child abuse on the internet by fully implementing Article 9 of the Convention on Cybercrime without reservations, unless absolutely necessary
- Also implement other treaties and regulations protecting children from abuse
- Improve education for the secure use of information and communication technologies at all levels, for example through specialised curricula or training institutions. Users themselves (individual users but also companies and public institutions) themselves have a major responsibility to prevent and protect themselves
- Implement measures for the protection of critical infrastructure
- Take steps to find solutions to challenges posed by technological developments such as NGN, including VoIP.

2 IMPLEMENTATION OF THE CONVENTION ON CYBERCRIME AND THE PROTOCOL ON XENOPHOBIA AND RACISM

The challenge

Cybercrime is extensive, increasing rapidly, becoming more and more dangerous and crosses frontiers without difficulty. Clearly it must and can be fought at a global level. In order to do so countries must not only have compatible and – to

the extent possible - harmonised substantive and procedural criminal laws but they also must all work more closely together in order to achieve effective international cooperation.

The Convention on Cybercrime provides workable and well-received guidelines for the development of national laws and sets up a framework for international cooperation. To date the Convention has been ratified by 21 States and signed by another 22. The Additional Protocol on Racism and Xenophobia has been ratified by 11 and signed by another 20 States.

The challenges include:

- increasing the number of Parties to the Convention and the Additional Protocol. In particular, States having already signed these treaties should speed up the ratification process
- promoting the Convention at a global level. In addition to the six non-European States that signed or ratified the treaty or have been invited to accede, other States should be encouraged to seek accession
- ensuring and promoting the effectiveness of the Convention and its Additional Protocol between Parties.

Good practices to be shared

As a result of the importance of the Convention, which is the only binding instrument on cybercrime in the world, its provisions have been frequently used a model for draft laws. This widespread support for the Convention in the different regions of the world has resulted in virtually all new legislation or draft legislation following very closely the provisions of the Convention. Such reforms are currently underway, for example, in countries such as Argentina, Brazil, Egypt, India, Nigeria, Pakistan and the Philippines.

This ensures, at a world level, the compatibility of laws and provides a solid and effective basis for countries to work together.

The way ahead

- Countries that have already signed the Convention or the Protocol or have been invited to accede should complete the ratification process as soon as possible
- Countries that have implemented the Convention should share their experience. The "Country profiles on cybercrime legislation" prepared by the Council of Europe under the Project on Cybercrime may be helpful in this respect[1]
- The Council of Europe and other partners are prepared to assist interested countries to provide advice on cybercrime legislation
- The Consultation of the Parties – through the Cybercrime Convention Committee, T-CY – will provide advice and assistance in the implementation of the Convention and its Protocol.

[1] See www.coe.int/cybercrime

3 THE EFFECTIVENESS OF CYBERCRIME LEGISLATION

The challenge

Countries need to criminalise certain conduct (substantive criminal law), provide law enforcement and criminal justice with the means to efficiently investigate, prosecute, and adjudicate cybercrimes (procedural law), including the need to rapid action to preserve volatile evidence, and make provisions for efficient international cooperation. Any country is encouraged to use the Convention as a guideline in this respect. Some countries which are already Party to the Convention may need to take further steps to bring their legislation fully in line with this treaty.

The main challenge is that countries adopt national legislation in terms of substantive and procedural criminal law as well as international cooperation in line with the Convention on Cybercrime.

In addition, the question of jurisdiction continues to pose major problems for law enforcement around the world.

Good practices to be shared

Representatives of the following States made a presentation of their domestic law concerning cybercrime and related issues: Italy, Romania, Russia, Norway, the Netherlands, Portugal and Azerbaijan, all of which are member States of the Council of Europe.
Further presentations were made by India, Argentina, Brazil, Mexico, Egypt and South Africa. In addition an overview of present cybercrime legislation and legislative initiatives in States in the Asia-Pacific area was presented by Microsoft.

The merits of the Cybercrime Convention and its First Additional Protocol were commonly recognized and appeared to be largely supported.

Most speakers provided an overview of the provisions of their present domestic law in the field of cybercrime. Signatory States and States that may seek accession to the Convention pointed at pending Bills and further legislative efforts to be undertaken. It may be concluded that implementation of the Convention in most cases has lead to a major review of existing legal provisions and the enactment of new laws. From the information given it may be concluded that a substantial number of ratifications and also of request for accession may be expected in 2007.

A number of complexities met by domestic legislators when implementing the text of the Convention were brought forward, e.g. concerning article 2 (illegal access), article 3 (illegal interception), article 9 (child porn), article 32 (transborder access) and article 35 (24/7). In addition several speakers – including those who already signed or ratified the Convention – referred to specific forms of cybercrime that are criminalized under domestic law, but are not (explicitly) defined under the Convention like identity theft, cyberstalking and cyberdefamation. Abuse of other features of ICT (such as Wifi, biometric identification, RFID) should be studied for further criminalisation.

A number of investigative problems relating to the gathering of electronic evidence was raised, in particular evidence that is outside national territory. The Convention provides for expedited mutual assistance in order to secure electronic evidence in another Party.

Difficulties have been encountered in the cooperation between member States of the Council of Europe and non-member States. For example, classical MLA-procedures for the transfer of the requested material in general take a relatively long term which may jeopardize the investigation and prosecution of the crime involved. In addition, it was brought forward that it may be difficult to determine the physical location of a computer server, which prevents law enforcement to request for mutual assistance.

A brief debate was held about the need to provide for a coercive power to order ISP's to block internet traffic originating for particular sources because of its content. Some countries have such a power, in other cases the blocking is effectuated in cooperation with the ISP.

Most representatives stressed the need for specialized investigating and coordinating bodies at national level, as well as permanent education and training, in particular of the prosecution service and the judiciary.

Some representatives drew attention to the fact that in their developing economies sufficient funds may not be available to provide law enforcement and the judiciary with necessary equipment and expertise. Support of other States and the private sector is needed.

The session was concluded by providing details about the procedure and conditions for accession and consequent ratification.

The way ahead

- A more thorough assessment of the effectiveness of cybercrime legislation may need to be carried out and examples of good practice should be shared. The "country profiles on cybercrime legislation" prepared by the Council of Europe may facilitate this
- Countries that are in the process of drafting cybercrime legislation may request the Council of Europe or authorities of State Parties to the Convention or also the private sector for assistance in the preparation of cybercrime legislation
- The capabilities of criminal justice and law enforcement authorities to enforce cybercrime laws need to be strengthened
- The question of jurisdiction may be further examined in relevant fora, including the Cybercrime Convention Committee (T-CY).

4 INTERNATIONAL COOPERATION AND THE FUNCTIONING OF THE 24/7 NETWORK OF CONTACT POINTS

The challenge

Cybercrime is international crime which implies the need for efficient and immediate international cooperation to preserve volatile evidence across borders. The network of contact points available 24 hours a day, 7 days a week is an important tool is this respect. The creation of such contact points has been promoted by the G8 High-tech Crime Subgroup since 1997 and is also foreseen in Article 35 of the Convention on Cybercrime.

Challenges include:

- Not all Parties to the Convention have established functioning contact points
- The risk of different networks of contact points, such as one of the G8 and one of the Council of Europe

- The legal basis for contact points to act is not fully provided in a number of countries (e.g. with regard to the expedited preservation of data)
- Need to back up cooperation among contact points with functioning judicial cooperation

Good practices

Considerable experience has been gained within the network of the G8 High-tech Crime Sub-group during the ten years since its creation. Guidelines and other documentation are available. The "Protocol Statement" may help countries set up contact points. The "Checklist for use of the G8 24/7 Network" may help contact points formulate requests in a format which contains all necessary information for the requested contact point to act.
Examples of functioning contact points discussed were Italy, USA, France and Romania.

The way ahead

- All countries that have ratified the Convention should establish functioning contact points as required under Article 35. Members of the G8 Network and the Council of Europe should provide support in this respect if necessary
- Contact points established under the Convention are encouraged to also register with the network of the G8 High-Tech Crime Sub-group
- The G8 High-tech Crime Subgroup and the Council of Europe should cooperate to maintain and update a combined Directory of Contact Points (restricted to law enforcement purposes). This proposal should be discussed at the next meeting of the G8 Sub-group
- In order to facilitate cooperation among contact points, standardised formats for requests may be useful, such as the "Checklist of use of the G8 24/7 network"
- Italy is planning set up – subject to the availability of funds – a secure portal for use of the network of contact points. This may help keep the Directory updated but also share other information, such as templates for requests
- Following training conferences for contact points organised by the G8 Subgroup in Rome, Italy, in 2004 and 2006, another G8 training conference could be envisaged for 2009. In order to maintain the momentum, the Council of Europe should consider organising a training workshop for contact points already in 2008
- Network or ping tests may be carried out to verify whether contact points are operational
- Efforts should be undertaken to further expand the network. This should involve an examination of the composition, working methods and competences of already existing networks in this area such as that of Interpol.

5 INITIATIVES OF OTHER ORGANISATIONS AND STAKEHOLDERS: OPPORTUNITIES FOR COOPERATION AND SYNERGIES

The challenge

In recent years, international organisations, States, public and private stakeholders have multiplied the initiatives demonstrating a global engagement to tackle cybercrime and find appropriate solutions. As a result, the momentum on this question is very high but the risk of duplication (with the natural inclination to work in isolation and limit coordination to the others) represents a major challenge. All actors have a unique and common objective which calls for a further harmonisation and centralisation of efforts and actions in particular at the international level. This coordination should function like the internet: cells linking up with each other as appropriate, creating synergies and new dynamics. Meetings like the Octopus Conference, combined with an official coordination between stakeholders, may serve as an Interface to facilitate such cooperation.

Good practices to be shared

Various actions and programmes were presented which represent good practices to be shared and further expanded such as: the co-operation between law enforcement and the private sector as a common platform to exchange information and define the roles and expectations of each other, the coordinating role of the European Network and Information Security Agency (ENISA) with industry, international organisations, third countries and academia and its project of creating a European Information Sharing and Alert System targeting citizens and small and medium enterprises, the Anti-spam Toolkit prepared by the OECD, the International Advisory Group created in the framework of the UNDP Programme on Governance in the Arab Region (POGAR) to support actions aimed at training criminal justice to cope with high-tech crime, the creation of additional Internet Hotlines in Africa and Asia within the INHOPE Association which facilitates and coordinates the work of Internet hotlines in responding to illegal use and content on the Internet, the development of global campaigns against child pornography such as the one launched by the International Center for Missing and exploited Children.

The way ahead

Among the proposals for joint efforts and to enhance cooperation at international level:

- Internet Governance Forum: the Council of Europe will contribute to the next meeting in Rio (November 2007) and underline the need to make sure that the Internet is safe and that human rights and the rule of law are respected in cyberspace as well
- Organisations such as European Digital Rights will continue to observe whether cybercrime laws unduly infringe privacy rights and the freedom of expression on the Internet
- European Commission: the Communication of the Commission of May 2007 may serve as a good basis for further cooperation. The Commission expressed its commitment to promote the Convention and its Protocol, encourage third countries to accede to the Convention and consider accession of the European Communities to the Convention. Council of Europe is prepared to participate in the activities indicated in the Communication

- Organisation of American States (OAS): will further support its member states to accede to the Convention and is ready to explore additional possibilities of cooperation with international organisations. The Council of Europe will continue its fruitful cooperation with the OAS and possibly consider a joint training event to assist OAS member states in the drafting of cybercrime legislation
- Interpol: encourages all its member states to use the tools (24/7 network, databases) it offers in the field of high-tech crime. Council of Europe is prepared to support the meetings of the Near and Middle East working group and of the African working group later in 2007
- Asia Pacific Economic Cooperation and ASEAN: will further promote the Convention among its member states and the strengthening of cybercrime legislation. Council of Europe prepared to work through APEC and ASEAN with countries of Asia and Pacific to achieve this objective. Ready to contribute to the next APEC TEL working group meeting in Chile as appropriate
- Organisation of the Islamic Conference (OIC): will continue to act against the defamation of religion on the Internet. The Council of Europe should cooperate with the OIC against intolerance and discrimination on the basis of the Cybercrime Convention and its additional Protocol on the criminalisation of Acts of a Racist and Xenophobic Nature
- UNDP POGAR: Council of Europe will contribute to the next training conference for prosecutors of the Arab region on cybercrime organised by UNDP POGAR in Casablanca on 19 and 20 June 2007. Further Council of Europe/UNDP POGAR cooperation may be envisaged.

6 PUBLIC-PRIVATE PARTNERSHIPS

The challenge

The Investigation of Internet Crimes does very often require a strong cooperation between private companies (such as Internet Service Provider) and law enforcement agencies. The cooperation covers aspects like:

- Identification of suspects on the basis of an IP-address or bank account specification
- Submission of subscriber information
- Identification and access to stored illegal content.

For the private sector the cooperation with law enforcement agencies can lead to conflicts in those cases where a legal framework for the cooperation is not established. The public-private partnership is therefore especially important with regard to two aspects:

- Improvement of the cooperation within the existing legal framework
- Development of principles for the implementation or improvement of procedures of public-private partnerships

Public-Private partnerships in Internet investigations cannot be extended without limits. The limitations do for example result from the fact that key elements of criminal investigations do – at least in most jurisdictions – need to remain under complete control of the competent law enforcement agencies.

Good practices to be shared

The importance of public-private partnership was and is the motivation for the implementation of a number of initiatives. With regard to the fact that many global players in Internet business have their headquarter in the US those companies are playing an important role. Good practices presented during the Conference include:

- The Council of Europe/Microsoft partnership supporting the Project on Cybercrime and thus helping to promote the Convention on Cybercrime worldwide
- The child exploitation tracking system developed by Microsoft in partnership with the Canadian law enforcement authorities which is now being implemented in a number of different countries
- The London Action Plan which is aimed to promote international Spam enforcement cooperation
- The Anti-Phishing Working Group (APWG) which is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types. It now comprises several thousand members, agencies and companies worldwide
- The G8 High Tech Crime Subgroup: encouraged countries to join the 24/7 High Tech Points of Contact Network and to take advantage of the work of the Subgroup in industry-law enforcement cooperation, critical information infrastructure protection, data preservation and other issues. Documents and best practices in these areas are posted on www.coe.int/economiccrime
- The cooperation between law enforcement agencies and private sector companies in Serbia.

The way ahead

- Public-private partnerships should be further developed and expanded
- At the same time, limitations for public-private partnerships should be further evaluated
- Regional players should be identified and included in addition to the global player
- Guidelines or rules for PPP should be developed on the basis of good practices.

7 THE ROLE OF SERVICE PROVIDERS

The challenge

The Service Providesr play an important role with regard to the future success of the network. Without the services made available by Access Provider the aim of enabling as many people as possible to access Internet sources cannot be achieved. Without the storage capacities that are made available by Hosting Providers – often without charge on an add-based level - Internet users in developing countries would loose an important instrument to share information with other users. If the interests of users are to be protected and supported, legislation needs to give due consideration to the protection of the work of access providers. This includes discussing the limiting of criminal responsibility for offences committed by their clients.

Apart from securing Internet connections Service Providers play a major role in Internet investigations. They can especially assist police and law enforcement agencies to:

- Block websites
- Identify and remove illegal content
- Identify offenders
- Assist in the installation of investigation tools
- Collect Data (Data preservation / Data retention)
- Prevent crimes (copyright violation, spam)

Good practices to be shared

- The discussion about the adjustment of the obligations and rights of Service Providers which has just started again
- EU E-commerce Directive which contains basic principles
- The Convention on Cybercrime with regard to the obligation of Service Providers to assist law enforcement agencies

The way ahead

- Open discussion about the role of the Service Provider and the related legal framework should be continued. Good practices should be documented in view of developing common standards or guidelines.

In short:

1. Improve the analysis of cybercrime, facilitate reporting by victims, enhance awareness and promote measures to prevent and protect individuals and public and private sector users as well as critical infrastructure
2. Implement the Convention on Cybercrime and the Protocol, and provide all necessary support in this respect
3. Share information on cybercrime legislation and analyse its effectiveness
4. Take measures to further enhance the functioning of 24/7 points of contact
5. Pursue a pragmatic approach to cooperation between different initiatives and organisations; network and make use of existing opportunities
6. Take steps to further enhance public-private partnerships
7. With regard to the role of ISP: document good practices and consider developing common guidelines taking into account the careful balance between security needs and privacy rights

In sum: Cooperate.

Strasbourg, 12 June 2007