Octopus Interface conference on

Cooperation against cybercrime

Council of Europe, Strasbourg, France, 10-11 March 2009

Conference summary

Some 300 cybercrime experts from more than 70 countries, international organisations and the private sector met at the Council of Europe in Strasbourg from 10 to 11 March 2009. The extensive materials and presentations made available are evidence of the high quality and variety of the discussions (see conference site at www.coe.int/cybercrime).

1. The conference provided an update on:
   - The implementation of the Convention on Cybercrime. More than 100 countries worldwide use the Convention as a guideline for their legislation. Progress has been made in terms of ratifications and accessions but countries are encouraged to accelerate the ratification/accession process. Ratification of the Convention by Germany on the day before the Conference was very much appreciated as encouragement to others.
   - The guidelines on law enforcement – ISP cooperation in the investigation of cybercrime adopted at the last conference have been taken up by the European Union, France and other countries.

2. Phase 2 of the global Project on Cybercrime was launched. It will last from March 2009 to June 2011 and will be available as a tool to support countries worldwide in the implementation of the Convention on Cybercrime but also of standards related to data protection and the protection of children. The results of the conference will very much influence the work programme of this project. Initial funding is provided by the Government of Romania, Microsoft and McAfee. This is highly welcome and other public and private sector donors should follow their example.

3. Access to training resources: The conference showed what training on cybercrime is on offer for law enforcement, prosecutors and judges. The conference in particular saw the launch of the "2centre", a joint action of law enforcement and industry for cybercrime training. With regard to prosecutors and judges proposals have been discussed to further improve training materials and institutionalise judicial training. The Lisbon Network of the Council of Europe and the Global E-Crime Prosecutors Network (GPEN) offer opportunities in this respect. CYBEX has developed a model training course for judges. Common issues are the question of certification of training and trainees, the different levels of knowledge required by different people and the sustainability and replicability of training.

4. Criminalising child pornography and sexual exploitation and abuse of children on the Internet: Article 9 of the Convention on Cybercrime 9 and the Convention on the Sexual Exploitation and Abuse of Children (CETS 201) provide a comprehensive normative framework in this respect. However, only a few countries have so far fully implemented Article 9. Many other countries should therefore review and improve their current provisions in line with this Article. Countries should update their country profiles to facilitate such reviews. Consideration should also be given to the implementation of the new offences introduced by Convention 201. With regard to the obligations or liability of ISPs for child abuse materials there are differences regarding access, hosting and content providers. A number of issues require further debate: Should these obligations be governed by contract, self-regulation or formal legislation? To what extent do ISPs have the obligation to prevent crime or only to support investigations? What are the

consequences of a failure to comply? It may be useful to further study good practices regarding different approaches and their implications.

5. Following criminal money on the Internet: The conference helped share experience, good practices and opportunities for cooperation in terms of (a) typologies of proceeds generating crime, money flows and money laundering, (b) strategies, techniques and tools to search, follow, seize and confiscate such proceeds, and (c) opportunities for multi-stakeholder action to follow criminal money and prevent cyber-fraud and cyber-laundering. The conference pointed at the need to establish trust between different public and private sector stakeholders involved in anti-cybercrime and anti-money laundering and terrorist financing measures, and to build bridges between the anti-cybercrime and anti-money laundering communities, between law enforcement, internet industry, financial services and others. Examples discussed included the Financial Action Task Force, Moneyval, the Anti-Phishing Working Group, the London Action Plan, the Advance Fee Fraud coalition or the Hi-tech Crime Forum in Ireland. Countries should also make sure that different types of cybercrime are predicate offences for money laundering. Countries should also be aware of the risks of networks such as VoIP that may need further regulations.

6. Effectiveness of international cooperation: the conference discussed proposals to make international cooperation against cybercrime more effective. For example, contact points need to become more proactive and make themselves known, and help facilitate mutual legal assistance. The Council of Europe and the G8 High-tech Crime Subgroup should organise their management of the 24/7 network of contact points. Solutions need to be found to expedite mutual legal assistance (article 31 of the Convention). As a minimum, countries should make use of possibilities for direct cooperation between authorities that are provided for in a number of European instruments. The network of 24/7 points of contact is primarily for urgent measures. For other, less urgent cases, other channels are used, in particular Interpol. The strengthening of law enforcement – ISP cooperation remains a concern in many countries. The Project on Cybercrime could study good practices and further possibilities regarding a contact list for law enforcement and Internet Service Providers to facilitate cooperation not only at the national but also international level.

7. The future of cybercrime – challenges and solutions: The conference stimulated the debate on "jurisdiction, national borders and law enforcement in the times of cloud computing". Computer data and services will increasingly move from specific, identifyable computers in a specific location to the "clouds", that is, they are hosted in data centres in unspecified locations. And different technologies will become increasingly interconnected. This has implications for security and law enforcement, and creates legal uncertainties and inconsistencies. These and other questions raise a number of challenges related to data protection and identity management. The Council of Europe should further study the implications of "cloud computing" on jurisdiction, law enforcement and national borders. It may also be necessary to review in this light the adequacy of data protection instruments that have been in place for more than 25 years.

Strasbourg, 11 March 2009