The Hague, 3rd October 2011

File no. 2510-320

Committee on Civil Liberties, Justice and Home Affairs hearing on Cyber Attacks and Information Systems – Europol intervention (V. Baines)

I would like to thank the LIBE Committee and the Rapporteur for inviting Europol to participate today. Our position is that both this hearing and the proposal are particularly timely in light not only of the increasing threat from attacks against information systems, and cybercrime more generally, but also of an increasingly coordinated and collaborative response which is currently gathering pace in the EU.

Europol is the EU's principal centre for law enforcement expertise and operational support on cybercrime. Amongst our services, we provide specialist on the spot forensic support to investigations in Member States, coordinate joint investigations based on identified cross border issues, and give strategic direction to response measures through the EU Cybercrime Task Force. We also serve as Europe's criminal information hub, identifying key target groups and providing crucial insight into cybercriminal behaviour by means of our operational Analysis Work File Cyborg, and our strategic threat assessments. In addition, our unique on site network of 140 liaison officers from law enforcement agencies in the EU and third countries is to be strengthened by a number of specialist liaison officers dedicated to cybercrime, most notably from the UK Serious Organised Crime Agency (SOCA) and the FBI.

Last year Europol published a threat assessment on Internet Facilitated Organised Crime, the iOCTA. This highlighted the key role of botnets in industrialising cybercrime, significantly increasing its profitability, but also in enabling large scale attacks on information systems. Our recommendation that their dismantling should be an international policing priority is very much in line with the current proposal.

Recognising that the same cybercriminal tools are often used for a variety of ends, and having observed that the distinctions between different types of Internet facilitated criminal activity are increasingly blurred, both Member States and EU agencies are adopting a more collaborative approach to fighting cybercrime. Active partnership with the private sector is a high priority, as is the formation of closer working relationships with other EU agencies.

In terms of judicial cooperation, Europol and Eurojust naturally work in very close proximity. Eurojust is a member not only of AWF Cyborg, but also the EU Cybercrime Task Force and the European Cybercrime Training and Education Group, co-founded by Europol. The two agencies therefore collaborate directly on operational and strategic issues, and in capacity building throughout the EU. While the majority of operational examples relate to ongoing cases, instances from the wider cybercriminal environment include:

- An investigation coordinated by Eurojust into frauds committed via the EU Emissions Trading System. In this case analysis of information submitted by Member States to Europol enabled the identification of the money flows concerned, and gave the Member States valuable added insight into the criminal behaviour of the groups involved.
- A project coordinated by Eurojust on "e-muling", the process by which money derived from cybercrime is turned into hard cash. Also in this case, Europol's analysis of information supplied by Member States enabled prosecutors to commence a cross-border investigation into specific offences.

Our collaboration with ENISA is more recent but no less important. As we speak Europol and ENISA are co-hosting a workshop in Prague to foster closer working relationships between Member States law enforcement authorities and Computer Emergency Response Teams.

Recognising key synergies between our missions, especially those between the work of ENISA on resilience and that of Europol on crime prevention, and complementary in strategic insight, together we are currently exploring further opportunities for collaboration, including joint reporting on threats and risks, and joint awareness raising measures.

Looking ahead, the proposed establishment of European Cybercrime Centre in 2013 is an important and timely step forward. As the EU's law enforcement agency, Europol aspires to play a role in the intelligence and investigative work of this centre, and sees potential benefit in the embedding of specialists from Eurojust, ENISA and other relevant agencies. It is anticipated, for example, that there will be close links with the nascent EU-CERT, the computer emergency response team for EU institutions.

To return to the proposal if I may, Europol commends the penalisation of the production, sale, procurement for use, import, distribution or otherwise making available of cybercriminal devices and tools, and the inclusion of aggravating circumstances relating to these offences. The organisation is also in accord with the introduction of illegal interception as a criminal offence, and with the introduction of measures to improve criminal justice cooperation and strengthen the existing 24/7 contact points, including the 8 hour time limit for responding to requests for assistance.

With regard to the collection of statistical data on attacks against information systems, Europol humbly suggests that further consideration is given to whether this would relate to all such attacks, or merely those considered "large scale" or "serious" by Member States. Since the current proposal states that "Member States may determine what constitutes serious damage according to their national law and practice", this may result in inconsistent reporting, in turn precluding an accurate overview of the scale of attacks. Finally, for your information, I draw your attention to a project currently underway to streamline reporting of cybercrimes from Member States authorities to Europol, The Internet Crime Online Reporting System or ICROS, which could be used to collect such reports, and may therefore deserve an explicit reference in the legislative proposal.