Happy Birthday to the European Cybercrime Centre (EC3)

10 February 2014

On the first anniversary of the launch of the European Cybercrime Centre (EC3) within Europol, the Commission (DG Home Affairs) organised a half-day event last week in Brussels to take stock of EC3’s achievements so far, to look at current threats and trends in the field of cybercrime and to define future priorities. 120 stakeholders representing Member States Law Enforcement Agencies (LEA), Academia, Civil Society, the Private Sector and European Institutions joined the event, chaired by Reinhard Priebe, Director Internal Security, DG Home Affairs.

In her keynote address, Commissioner Malmström congratulated EC3 on considerable achievements so far, including key involvement in botnet takedowns, disruption and investigation of criminal forums, Ransomware, credit card fraud and malware attacks against financial institutions. She also noted the significant progress in the fight against online sexual exploitation of children.

Despite this, criminal behaviours and patterns are evolving fast, exploiting technology developments and existing legal loopholes. ‘Cybercrime as a service’ and rapid adoption of the Internet worldwide through a multitude of devices is leading to more criminal activity. More effective investigation and prosecution, and deterrent sanctions are needed to complement preven-
tion in this domain. Effective cooperation with our international partners is also key, and the Commissioner re-affirmed that the Budapest Convention remains the model for national legislation on cybercrime, as well as the framework of reference for international police and judicial cooperation.

Troels Oerting, the head of EC³, presented a report on EC³’s first year of activities. He underlined that EC³’s central priority continues to be the support for EU Member States’ law enforcement agencies on the front line. The borderless nature of cybercrime and its rapid expansion necessitates a coordinating role for EC³. Cybercrime prevention can be stepped up with an emphasis on ‘Security by design’ and awareness raising amongst all stakeholders. Continued active disruption will also deter criminals.

Emma McClarkin MEP expressed her strong support to EC³’s contribution to protecting the vulnerable from cybercrime. She called for more awareness raising and for striking the right balance between privacy and accountability.

Representatives of law enforcement authorities and of ENISA subscribed to the need for EC³ to provide a single voice for the common European fight against cybercrime and to play a key role in coordinating a European approach, along with other agencies. Speakers concurred in highlighting barriers to existing investigative and prosecutorial practices: the ‘loss of location’ of criminal activity online, an insufficient legal framework for remote search and seizure, jurisdictional complexity and complications in cooperation with service providers. Private Sector representatives provided further cause for alarm in highlighting new threats from more sophisticated encryption and malware that will affect the ‘Internet of Everything’.

In terms of possible solutions to the mounting threat of cybercrime, speakers focused on three elements in particular: the right legal framework needs to be put in place, also from a procedural perspective; public-private partnerships, which already exist in some Member States, have proven beneficial and should be expanded; and Member States need to ensure that the police can keep up with the technical knowledge required and have access to the right tools. To achieve these aims, decision-makers have to be convinced of the need to prioritise cyber issues.

In his conclusions, Director Reinhard Priebe highlighted the need for a continuous exchange between the EC³ and all of its stakeholders to ensure that priorities set by the Centre are always closely matched with the needs of the communities that it serves. He invited all participants to continue the conversation.