Background on 'Home Affairs' elements of the Strategy

7 February 2013

European Cybercrime Centre: boosting the EU's capacity to fight cybercrime

Investigations into online fraud, child abuse online and other cybercrimes regularly involve hundreds of victims at a time, and suspects in many different parts of the world. Operations of this magnitude cannot be successfully concluded by national police forces alone.

To help protect European citizens and businesses against cyber-criminal threats, the EU launched the European Cybercrime Centre (E3C), which started operations on 11 January 2013 (IP/13/13 and MEMO/13/6).

The EC3 will focus on illegal online activities carried out by organised crime groups, especially attacks targeting e-banking and other online financial activities, online child sexual exploitation and those crimes that affect the critical infrastructure and information systems in the EU.

Equipped with state-of-the-art technology and a strong team of highly-qualified and specialised personnel offering a wide spectrum of services - from helping Member States analyse complex digital forensic evidence to forecasting trends and scenarios, the European Cybercrime Centre will become the focal point in the fight against cybercrime in the Union.

Some figures:
Around one million people worldwide fall victim to some form of cybercrime every day. Estimates indicate that victims lose around €290 billion each year worldwide as a result of cybercriminal activities (Norton, 2011).

In Europe Internet users remain very concerned about cyber security. According to a recent Eurobarometer survey:

- 12% of EU citizens have experienced online fraud
- 74% agree that the risk of becoming a victim of cybercrime has increased in the past year
- 61% are concerned about experiencing identity theft
- 43% are concerned about not being able to access online services because of cyber attacks

Combating sexual abuse of children online: a Global Alliance for greater results

It is estimated that more than one million images of children subjected to sexual abuse and exploitation are currently online. According to UNODC 50,000 new child abuse images are added each year.

No country can fight this horrible phenomenon alone, as the criminal networks behind it know no boundaries and exploit the lack of information exchange and the legal loopholes that exist within and between countries. This is why international cooperation is crucial to effectively investigate cases of child sexual abuse online and to better identify and prosecute offenders.

The initiative aims to unite decision-makers all around the world for more intensive and better coordinated action worldwide.

To date, 49 countries have joined the Global Alliance: the 27 EU Member States, as well as 22 countries outside the EU (Albania, Australia, Cambodia, Croatia, Georgia, Ghana, Israel, Japan, Moldova, Montenegro, New Zealand, Nigeria, Norway, the Philippines, Serbia, Republic of Korea, Switzerland, Thailand, Turkey, Ukraine, United States of America, and Vietnam).

The countries of the alliance are committing themselves to a number of policy targets and goals (Declaration on the Launch of the Global Alliance and Guiding Principles), notably:

- enhancing efforts to identify victims and ensuring that they receive the necessary assistance, support and protection;
- enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders;
- increasing children's awareness of online risks;
- reducing the availability of child pornography online and the re-victimization of children

**Fighting more effectively large-scale attacks against information systems**

To deal more efficiently with the growing number of large-scale and highly sophisticated cyber-attacks, the Commission put forward in 2010 a proposal for a Directive on attacks against information systems (IP/10/1239 and MEMO/10/463).

The main novelty of the proposal is the criminalisation of the use, production and sale of tools (now mostly known as "botnets") to commit attacks against information systems.

As such it introduces new aggravating circumstances and higher criminal sanctions, in particular for the use of so-called "Botnets" (i.e. networks of infected computers that serve as the universal tool of the cybercriminal and can be remotely controlled for a wide variety of activities, such as staging coordinated attacks, disseminating spam or malware, or committing online banking fraud, to name but a few examples). It also aims to facilitate the prevention of such attacks and to improve the cooperation between member states' authorities in this field.

The proposal is now being discussed in the European Parliament and the Council.

Once adopted the Directive on attacks against information systems will repeal the Council Framework Decision 2005/222/JHA. Member States will have an obligation to comply with the new Directive and transpose it into national legislation within two years from its adoption at the latest.