Octopus conference
Cooperation against Cybercrime

Update on EU developments

JulieRUFF,
EC HOME A2, Fight against Cybercrime

European Commission
Home Affairs

Overview of 2013 Developments

- *Launch of the European Cybercrime Centre (EC3) (11 January)*
- *European Strategy for Cybersecurity (7 February)*
- *Adoption of Directive on Attacks on Information Systems (12 August)*
- *Deadline for transposition of Directive on the sexual abuse and sexual exploitation of children and child pornography (December 18)*

European Strategy on Cybersecurity

- Cybercrime Priorities:
  - **Strong and effective legislation**
  - **More operational capabilities (EC3)**
  - **Fight against Child sexual abuse (Global Alliance)**
  - **Capacity building (training, centres of excellence)**

More capacities and better coordination: EC3

- EU focal point in fight against cybercrime
- data analysis and fusion
- operational support to MS investigations
- streamlining R&D and training
- bridging of LE/CERT communities, public-private cooperation
- collective voice of cybercrime investigators

Dir. On Attacks against information systems

- *Directive adopted on 12/08/2013, based on existing Framework Decision 2005/222/JHA…*
- *…But takes into account recent developments, especially the growing number of large-scale cyber attacks against businesses and government organisations.*
  - *Recent cases: Estonia 2007, Lithuania 2008, EU institutions 2011, PL and US governments 2012*

New Elements Introduced by the Directive

- *Criminalisation of the use of tools (such as malware – e.g. 'botnets' – or unrightfully obtained computer passwords) for illegal access, system interference and data interference;*
- *Illegal interception of information systems defined as a criminal offence.*
- *Higher criminal sanctions for basic offences (max of at least 2 years), and in aggravating circumstances (max of at least 5 years - org. crime, use of botnets, and when serious damage caused)*
- *New aggravating circumstances when ID-theft is used;*

Improved European criminal justice/police cooperation

- Strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent request;

- Including the obligation to collect basic statistical data on cybercrimes.

Directive on the sexual abuse and sexual exploitation of children and child pornography

- *Adopted in December 2011*
- *Replaces Council Framework Decision of 2004*
- *Member States have two years to transpose the directive into national law:*

  *deadline **18 December 2013***

Central elements of the directive

- *Sexual abuse of children: minimum maximum penalties ranging from 1 to 10 years*
- *Sexual exploitation of children: penalties ranging from 2 to 10 years*
- *Child pornography: minimum penalties also for viewing without downloading*

New elements of the directive

- *Criminalisation of newer offences:*
  - Grooming of children, e.g. via internet chat rooms;
  - Abuse of webcams
  - Live viewing without downloading

- *Preventive measures, such as access to helplines for potential offenders and awareness-raising campaigns for children*

The Global Alliance against Child Sexual Abuse Online

- *Launched as a joint EU-US initiative on 5 December 2012, four central targets:*
  1. **improving victim identification and assistance;**
  2. **improving investigation and prosecution;**
  3. **raising awareness; and**
  4. **reducing the amount of child sexual abuse material available online.**
- *52 countries, including the EU 28. Newest Members: Armenia, Bosnia and Kosovo*

Global Alliance Next Steps

- *European Commission aiming to publish first report in November 2013*

- *US to take over secretariat role in 2014, with a conference provisionally scheduled for Oct 2014*

Support for capacity building, research and training (ISEC and new ISF from 2014)

- *Co-funding of MSs' activities (operational) in the fight against organised crime, incl. cybercrime*
- *Since 2001, development of cybercrime training materials for LE (ECTEG hosted by Europol)*
- *Since 2010, creation of an EU network of national centres of excellence for cybercrime training, research and education). Already in IE, FR, BE, EE, UK, EL, RO, BG and soon in CZ and PL.*

Looking Forward

- Proposed Directive on Network and Information Security

- 1 year reviews of EU Cyber-strategy and EC3

- Cross-sector cooperation - research/academia, CERTs, LE practitioners and the private sector

-'Post-Stockholm programme'

THANK YOU

Questions?