ECONOMIC ASPECTS OF CYBERCRIME

Asia-Pacific Regional Workshop on Fighting Cybercrime
21. – 23.09.2011, Seoul
Prof. Dr. Marco Gercke, Director Cybercrime Research Institute

IMPORTANCE OF KNOWLEDGE

- Knowing about the quantity of Cybercrime as well as the economic impact is vital for both governments as well as businesses
- Especially necessary to be able to adjust legal and regulatory frameworks as well as institutional capacities
EXAMPLE ORGANISED CRIME R.

- An example for quotations without verifiable reference was discovered by the Wall Street Journal in 2006.

- While investigating a quotation that “child pornography is a multibillion business – 20 billion USD a year” - the journalist reported that two main documents containing information about revenues from 3 billion to 20 billion – a publication from NCMEC and one from the Council of Europe - did refer to Institutions that did not confirm the numbers.
DIFFERENTIATION

- It is necessary to differentiate between two economic aspects: Revenue generated by Cybercrime and losses caused by Cybercrime.

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent and impact of crime.
- This is especially relevant with regard to the involvement of organized crime.
- Available information from the crime statistics therefore not necessary reflect the real extent of crime.
- Different motivations of private users and businesses not to report Cybercrime.

The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. “It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack,” explained Mark Mershon, acting head of the FBI’s New York office.
IMPACT OF CYBERCRIME

- As a result the extent and impact of Cybercrime is uncertain

Examples:
- Losses in German based on numbers provided by Federal Police: 75 million USD
- Losses in Germany based on Symantec: 33 Billion USD
- Number of “data manipulation” in Germany in 2010 based on official statistics: 2,000
- Number of Germans affected by computer virus: 12,000,000

AUTOMATE

- Automation enables offenders to generate high profit by committing various offences with rather small amounts each
- Background: Victims that have just lost rather small amounts tend not to report the crime
**LOSSES**

- What is known is that the losses caused by Cybercrime can be significant.

- Losses are not only related to direct financial losses but also necessary investments in Cybersecurity and loss of reputation when incidents happen.

- It is important to give guidance in this regard.

- Eg: Reporting obligation / establishment of reporting mechanisms (complaint center).

**REVENUES**

- Without doubt committing Cybercrime can generate large profits.

- One of the key motivations of organized crime to get involved in this form of crime.

- Current investigations show that even operating an illegal "free-of-charge" website with copyright protected movies can generate millions of USD in less than a year through advertisement.
**CHILD PORNOGRAPHY**

- Child pornography is widely recognised as illegal
- Exchange does not necessarily take place on a commercial basis
- Statistics even show a decreasing number of commercial child pornography websites
- Possible success of several initiatives to prevent the use of financial services with regard to child pornography
- Commercial nature is especially relevant with regard to the determination of the extend of organized crime

**EXAMPLES**

- “Math virus” stopped the computer after 30 steps and displays a simple addition or subtraction questions
- Execution of the program is denied unless the correct answer is given by the user
Currently there are more viruses that were designed with the intention to generate profits.