

CYBERCRIME

“PUBLIC-PRIVATE PARTNERSHIP”

Octopus Interface Conference
Cooperation against Cybercrime
12th of July 2007
Strasbourg, France

Dr. Marco Gercke
Lecturer at the University of Cologne, Germany

NEED FOR COOPERATION

- Internet investigations do often require the support of private companies

Example

- Identification of suspects on the basis of an IP-address or bank account information (credit card number)
- Identification of illegal content
- Removal of illegal content

PRINCIPLE

- “Fight against Cybercrime as a joined interest of private companies and law enforcement agencies”
- The ability and obligation of private companies are currently intensively discussed
- Very few regulation until now

Art. 19 - Search Seizure

(4) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

DISCUSSION

- Data Retention (EU Data Retention Directive)
- Obligation to register subscriber information with regard to public internet terminals (Italy)
- Restriction of Encryption Technology
- Obligation of Service Provider to assist in the secret installation of investigation tools

EXAMPLE



DISCUSSION

- Use of keylogger by law enforcement
- Reports that the FBI is already using a keylogger for investigation purposes
- German Federal Prosecution requested permission to secretly install an investigation software
- Federal Court refused the request with regard to the missing legal basis

EXAMPLE



DISCUSSION

- Where is public-private partnership necessary?
- What are limitations?
- What is the motivation and what are expectations from the private companies?
- What is the motivation and what are expectations from the law enforcement agencies?