Cybercrime
Research Institute

THE NEED FOR A COMPREHENSIVE APPROACH TOWARDS CYBERCRIME

Regional Arab Forum on Cybersecurity
Cairo, 19.12.2011
Prof. Dr. Marco Gercke

Cybercrime
Research Institute

DECENTRALISED SERVICES

- Availability of high-speed Internet connections and server infrastructure today enables the development of storage/processing concepts that are not anymore based on local but decentralised storage/processing
- „cloud computing" and „cloud storage"
- New opportunities for industry – but in a contested environment


Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

Cybercrime
Research Institute

DECENTRALIZED SERVICES

- Ability to use low-level end user systems for highly complex operations

Picture removed in print version
Bild zur Druckoptimierung entfernt

IPHONE CLOUD

Cybercrime
Research Institute

DECENTRALIZED SERVICE

- ExampleGoogle Maps,

Picture removed in print version
Bild zur Druckoptimierung entfernt

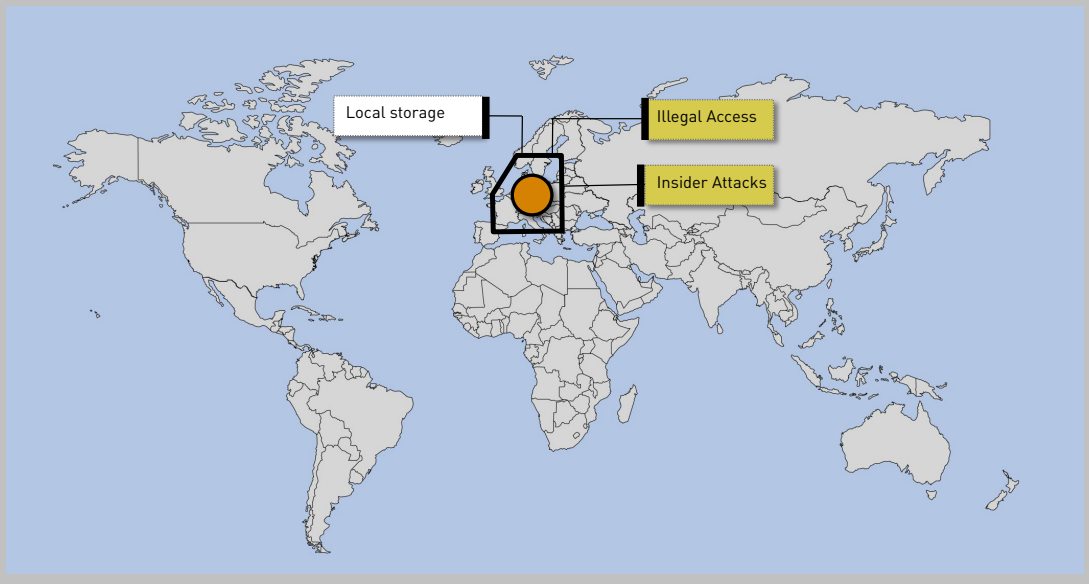
GOOGLE MAPS

Cybercrime
Research Institute

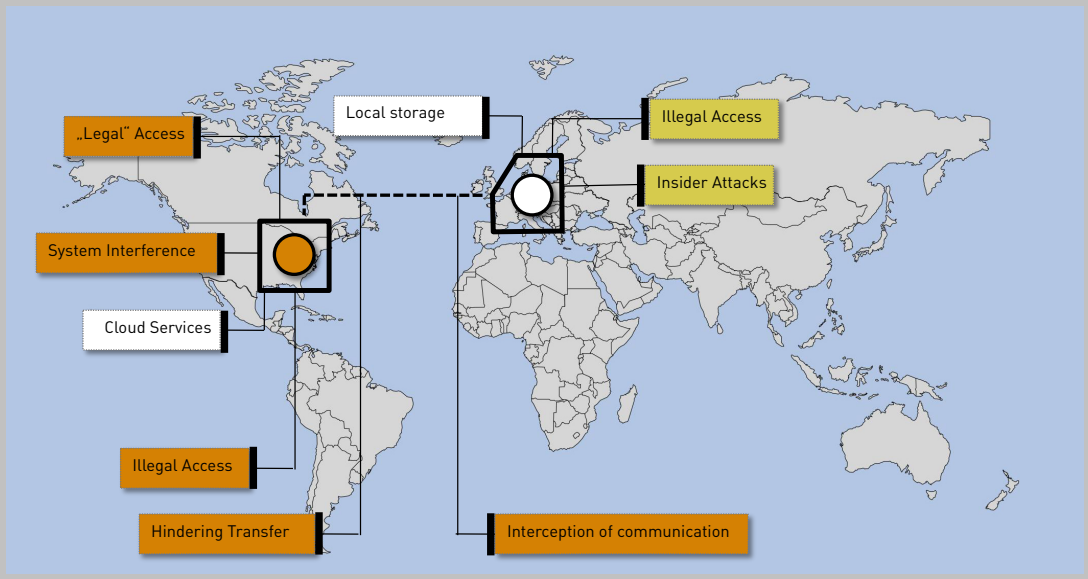
SUBSTANTIVE CRIMINAL LAW

Cybercrime
Research Institute

DECENTRALISED SERVICES



RISKS



SOLUTION

- Within HIPCAR/ICB4PAC/HIPSSA comprehensive regional legal frameworks are developed that address the various crimes
- This includes issues like illegal acquisition of computer data (data espionage), identity-related crime

HIPCAR

(1) If a judge is satisfied on the basis of [information on oath/affidavit] that in an investigation concerning an offence listed in paragraph 5 hereinbelow there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the judge [may/shall] on application authorize a police officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:
(a) suspect of the offence, if possible with name and address, and
(b) description of the targeted computer system, and
(c) description of the intended measure, extent and duration of the utilization, and
(d) reasons for the necessity of the utilization.

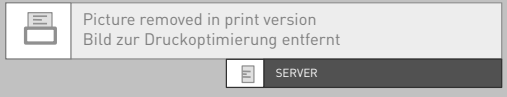
Cybercrime
Research Institute

PROCEDURAL LAW

Cybercrime
Research Institute

DECENTRALISED SERVICES

- Cloud storage provider might host data for thousands of customers
- Traditional approaches like seizing all relevant IT-systems might in this case not be an option as it could affect thousands of businesses



Cybercrime
Research Institute

DECENTRALISED SERVICES

- Law enforcement might not have the possibility to physically seize evidence
- More sophisticated instruments might be required
- Includes activating a computer system

HIPCAR

(16) Seize includes:
a) activating any onsite computer system and computer data storage media;
b) making and retaining a copy of computer data, including by using onsite equipment;
c) maintaining the integrity of the relevant stored computer data;
d) rendering inaccessible, or removing, computer data in the accessed computer system;
e) taking a printout of output of computer data; or
f) seize or similarly secure a computer system or part of it or a computer-data storage medium;

Cybercrime
Research Institute

ENCRYPTION

- In order to avoid some of the above mentioned attacks technical solutions are used
- One example is encryption technology
- Use of such technology can seriously interfere with the work of law enforcement

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE PGP

Cybercrime
Research Institute

SOLUTION

- With regard to the use of encryption technology by offenders solutions for LEA are required
- This includes technical as well as legal solutions
- Within HIPCAR/ICB4PAC/HIPSSA comprehensive regional legal frameworks are developed that address the issue of sophisticated investigation instruments

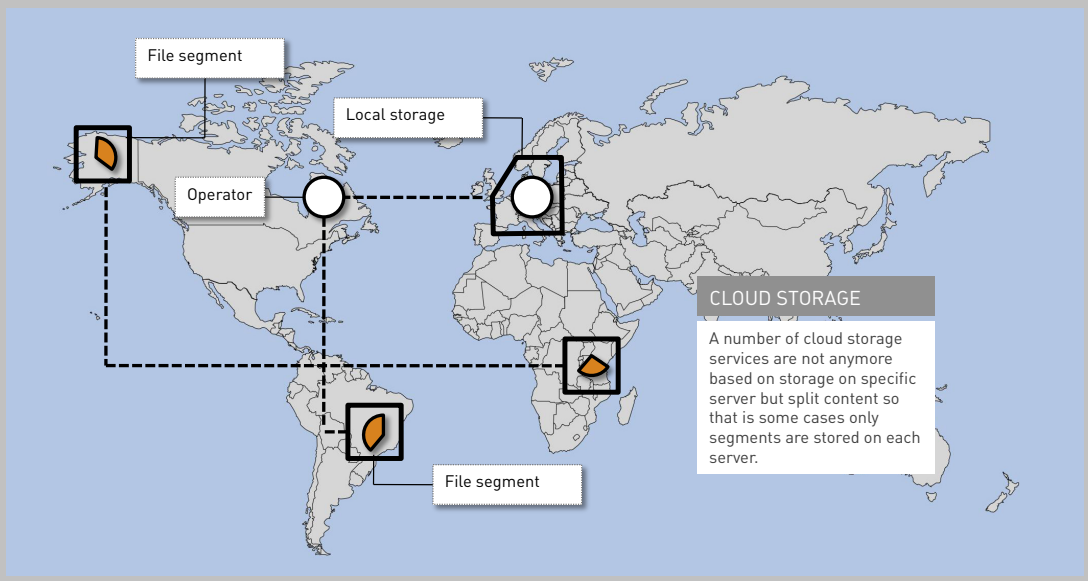
HIPCAR

(1) If a judge is satisfied on the basis of [information on oath/affidavit] that in an investigation concerning an offence listed in paragraph 5 hereinbelow there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the judge [may/shall] on application authorize a police officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:
(a) suspect of the offence, if possible with name and address, and
(b) description of the targeted computer system, and
(c) description of the intended measure, extent and duration of the utilization, and
(d) reasons for the necessity of the utilization.

Cybercrime
Research Institute

INTERNATIONAL COOPERATION

DECENTRALISED SERVICES



CLOUD STORAGE

A number of cloud storage services are not anymore based on storage on specific server but split content so that is some cases only segments are stored on each server.

Cybercrime
Research Institute

ELECTRONIC EVIDENCE

Cybercrime
Research Institute

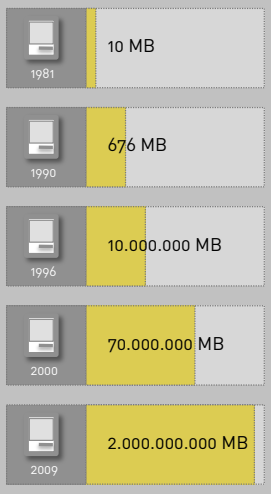
BACKGROUND

- Emerging relevance of digital evidence influences the procedures in court
- It is possible to divide between two different processes:
  1. Substitution of traditional evidence by digital evidence
  2. Introduction of digital evidence as additional evidence
- Influence is not limited to the fact that courts need to deal with digital evidence
- Even the design of courtrooms is influenced

Cybercrime
Research Institute

DIGITAL DATA

- One explanation for the emerging importance of digital evidence is the fact that the number of digital documents are intensively increasing
- Costs for storing one MB of data was constantly decreasing during the last decades
- Today it is cheaper to store information digitally than to keep physical copies



Cybercrime
Research Institute

DECENTRALISED SERVICES

- With regard to cloud computing the presentation of electronic evidence in court might be required
- Essential that there are rules in place that allow such process
- Within HIPCAR/ICB4PAC/HIPSSA comprehensive regional legal framework are developed that address the issue of admissibility of electronic evidence

Picture removed in print version
Bild zur Druckoptimierung entfernt

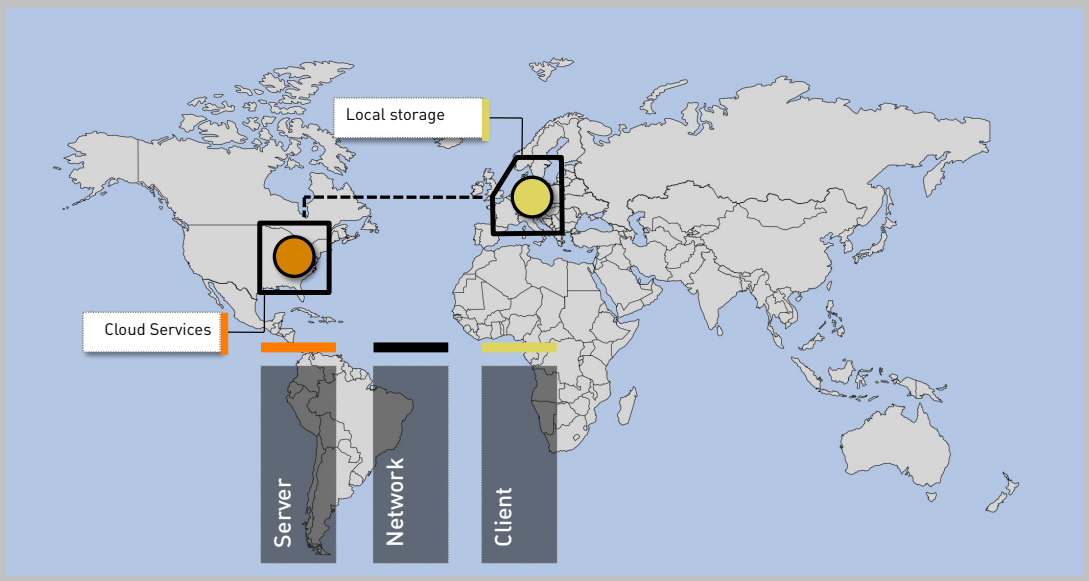
EXAMPLE: AMAZON CLOUD COMPUTING

Cybercrime
Research Institute

LIABILITY OF ISPS

Cybercrime
Research Institute

DECENTRALISED SERVICES



Cybercrime
Research Institute

SOLUTION

- The involvement of Internet Service Provider at various stages raises the question of liability
- Within HIPCAR/ICB4PAC/HIPSSA comprehensive regional legal frameworks are developed that address the issue ISP liability

HIPCAR

(1) A hosting provider is not criminally liable for the information stored at the request of a user of the service, on condition that:
(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court of law to remove specific illegal information stored; or
(b) the hosting provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

SOLUTION

	Subt.	Proc.	Int.	Evid.	ISP
Council of Europe Convention on Cybercrime	✔	✔	✔		
European Union Frameworks	✔	✔	✔		✔
Commonwealth Model Laws	✔	✔	✔	✔	
HIPCAR Model Laws	✔	✔	✔	✔	✔

Cybercrime
Research Institute

SOLUTION

	Ill. Access	Ill. Remaining	Ill. Interception	Data Interfer.	Data Espionage	System Interfer.	Illegal Devices	Comp. Forgery	Comp. Fraud	Child Pornogr.	ID-Theft	SPAM
Council of Europe Convention	✔		✔	✔		✔	✔	✔	✔	✔		
European Union Frameworks	✔		✔	✔		✔	✔		✔	✔		
Commonwealth Model Laws	✔		✔	✔		✔	✔	✔	✔	✔		
HIPCAR Model Laws	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Cybercrime
Research Institute

TRAINING

Cybercrime
Research Institute

MORE INFORMATION

- Legislation is just one component of an anti-cybercrime strategy
- Other aspects include training for law enforcement, judges, lawyers and others
- HIPCAR/ICB4PAC/HIPSSA in-country support includes capacity building
- One example is the ITU publication **Understanding Cybercrime** that is available in Arabic language


الاتحـــاد الدولـــي للاتصـــالات

فهم الجريمة السيبرانية:
دليـــل للبلـــدان الناميـــة

شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني
دائرة السياسات والاستراتيجيات
قطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات

مشروع أبريل 2009

ITU GUIDE

Cybercrime
Research Institute

PUBLIC PRIVATE PARTNERSHIP

Cybercrime
Research Institute

WHO WILL BE RESPONSIBLE

- Compliance with regard to Cybercrime is a key topic
- More responsibility of private sector as well as infrastructure provider is likely
- Question of allocation of risks (client/ provider)

Cybercrime
Research Institute

Cybercrime Research Institute
Prof. Dr. Marco Gercke

Niehler Str. 35
D-50733 Cologne, Germany
gercke@cybercrime.de
www.cybercrime-institute.com