HACKING A CRIME?

Dr. Marco Gercke

27.12.2005 / 22C3 Berlin

HACKING & CRIMINAL LAW

- Focus on hacking in the 80th (esp. Media)
- Intensive discussion about criminal law aspect of the phenomenon
- Today focus on child pornography, fraud and phishing
- Legislation in the area of cybercrime shows a number of difficult aspects
- “felt inability” leads to ad hoc legislation without integration of technical experts

EXAMPLE „PHISHING“

- Phishing (Password & Fishing?)
- Media and interest groups demand a new “phishing”- provision to be integrated in the national criminal law
- „phishing“can already be prosecuted unter (German) national criminal law
- Instead of legal and technical analyses popular calls for stricter legislation

BITKOM PM 27.04.2005

Das Ausspähen von Kunden-Passwörtern per **Phishing** - also mit Massenmails und gefälschten Webseiten - muss unter Strafe gestellt werden, fordert Peter Broß, Geschäftsführer des BITKOM. Denn bislang gibt es keine strafrechtliche Handhabe gegen diese neue, zunehmende Form der Internetkriminalität.

Sec. 269 (Falsification of Legally Relevant Data) - German Penal Code

(1) Whoever, for purposes of deception in legal relations, stores or modifies legally relevant data in such a way that a counterfeit or falsified document would exist upon its retrieval, or uses data stored or modified in such a manner, shall be punished with imprisonment for not more than five years or a fine.
(2) An attempt shall be punishable.

CYBERCRIME LEGISLATION

- Necessary to protect fundamental values by the means of criminal law
- Network technology offers a number of advantages for offenders (time, speed & certain degree of anonymity) - therefore criminal law needs to be applicable
- Legislation needs to respect technical background (jurisdiction)
- Integration of technical & legal experts
- No stricter legislation than outside the internet (balance)

HACKING

HACKING & NATIONAL PENAL LAW

HACKING & NATIONAL CL

- German penal law applicable
- Obtaining data after circumventing a protection
- Explanation of the draft of the law makes clear that the act of accessing a computer system (hacking) without further action (eg. download of data) shall not be prosecuted under Sec. 202a

Heise News v. 30.12.2004

Es gehört quasi zum guten Ton des alljährlichen Chaos Communication Congress, dass die dort versammelten Hacker einige auserlesene Websites mehr oder weniger dezent umgestalten. Sie wollen damit ihr Können unter Beweis stellen, auf Sicherheits-lücken hinweisen und die allgemeine Schadenfreude befriedigen.

Sec. 202a (Data Espionage) - German Penal Code

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

HACKING & NATIONAL CL

- Comparing it the the “real world”:
  - Unlocking a closed door is no criminal offence
  - Entering the house is a criminal offence
- Restrictive application of the provision with regard to the “first data” received after circumventing the protection

Sec. 202a (Data Espionage) - German Penal Code

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

HACKING & NATIONAL CL

- Alteration of data (even as a proof of success) can be prosecuted
- No limitation to financial damages

Sec. 303a (Alteration of Data) - German Penal Code

(1) Whoever unlawfully deletes, suppresses, renders unusable or alters data shall be punished with imprisonment for not more than two years or a fine.
(2) An attempt shall be punishable.

HACKING & NATIONAL CL

Protected System

Accessing the System	✓
Obtaining Data	✗
Alteration of Data	✗

Unprotected System

Accessing the System	✓
Obtaining Data*	✓
Alteration of Data	✗

Heise News v. 30.12.2004

Es gehört quasi zum guten Ton des alljährlichen Chaos Communication Congress, dass die dort versammelten Hacker einige auserlesene Websites mehr oder weniger dezent umgestalten. Sie wollen damit ihr Können unter Beweis stellen, auf Sicherheits-lücken hinweisen und die allgemeine Schadenfreude befriedigen.

HACKING

HACKING & INTERNATIONAL REGULATION ATTEMPTS

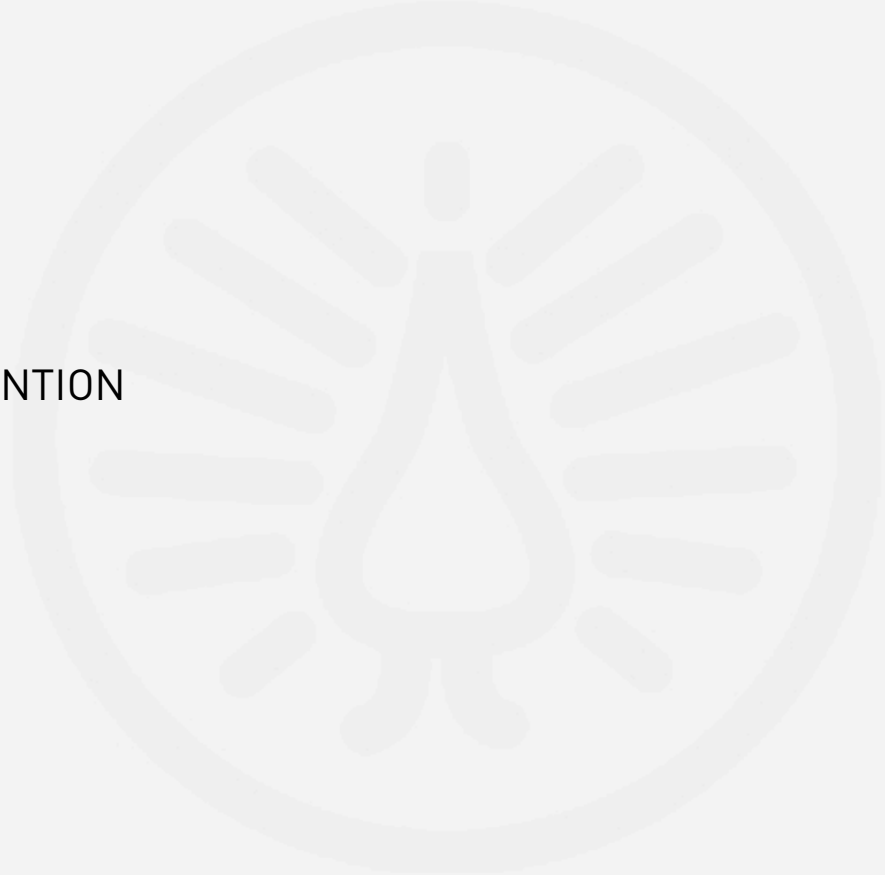
HACKING

1. Council of Europe - Convention on Cybercrime

2. European Union - Framework Decision on attacks against information systems

HACKING

CYBERCRIME CONVENTION



HISTORY OF THE CONVENTION

- Council of Europe (not Council of the European Union)
- Since 1989 the CoE is working to address threats of computer related crimes.
- In 1995 report about adequacy of criminal procedural law in the field of cyber crime.
- In 1997 Committee of Experts on Crime in Cyberspace established to draft convention on Crime in Cyberspace.
- In 2000 draft version 19 was made public.
- Negotiation went on until end of 2001when the convention was ready for signature.

STRUCTURE

- Section 1: Substantive criminal law
- Section 2: Procedural law
- Section 3: Jurisdiction
- International cooperation

- Additional protocol (xenophobic material)

NATURE OF THE CONVENTION

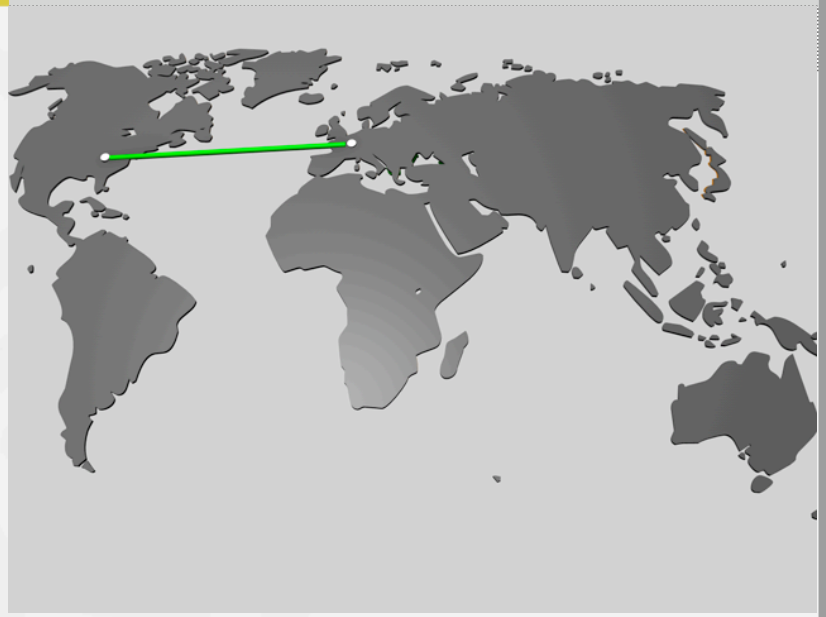
- International Agreement
- Needs to be ratified an implemented to come into effect
- Binding only on a political level
- Various spaces for interpretation and restrictions

MOTIVATION

- Fight against Cybercrimes was very much focusing on a national level
- International Dimension in most cases
- Threat of worldwide illegal activities from a “computer crime haven”
- Within transfer processes illegal contents are passing countries without respect to borders and boundaries. Uncoordinated national regulations are not able to solve this problem.
- Harmonisation - Different regulation on computer related crimes make an international strategy difficult.

MOTIVATION

- 42 States signed the Convention, among them 4 non-members of the CoE



MOTIVATION

- 12 Ratifications
- Albania, Bulgaria, Cyprus, Denmark, Estonia, France, Croatia, Hungary, Lithuania, Macedonia, Romania, Slovenia,

MOTIVATION

- Convention is a historical break through in the fight against cyber crimes.
- It enables an effective cooperation an coordination of international task forces.
- Chance for an effective Fight against Cybercrime?

IMPLEMENTATION

- Some of the Members do already have at least some internet related provision
- Translation
- Different legal systems and legal traditions (US influence)
- Different opportunities within the expert groups (convention and additional protocol) were indication for the need of a discussion during the implementation phase.

CRITICISM

Formal aspects:

- Procedure of the negation ("secret negotiation")
- No broad discussion with independent expert groups

Substantive criticism :

- Some provision of the convention (eg. real time collection of traffic and content data) are criticised because of a certain misbalance between freedom/privacy protection and fight against cybercrime.
- Technical aspects (real time collection)

ROAD MAP

- Translation (done in Germany)
- Draft of Law
- Negotiation about “fine tuning”

- Negotiation about the Conventions in general are **over** at this time
- In order to achieve a harmonisation of the various criminal codes it is necessary not to create new instruments but **keep the focus on the Convention**
- Convention leaves in some provisions space for different national solutions

ART 2: ILLEGAL ACCESS

- Protecting the **Integrity** of a computer system
- Without right: Ordered testing is no offence
- The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an **undisturbed** and uninhibited manner.
- A criminal prohibition of unauthorised access is able to give **additional protection** to the technical system and the data as such and at an early stage.
- Complete ban on hacking?

Art. 2

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the **access** to the whole or any part of a **computer system** without right.

ART 2: RESTRICTIONS

- Convention leaves space for national adjustment
- Prosecution of hacking can be limited

Question: Will it be limited?

- Evidence (easier to proof access than alteration)
- Claims under Civil Law

Art. 2

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

A Party may require that the offence be committed by **infringing security measures**, with the **intent of obtaining** computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

ART 9: MISUSE OF DEVICES

- "Hacking tools"
- Separate and independent criminal offence
- Intentional commission and **possession** of specific illegal acts regarding certain devices or access data
- A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting
- Restricted to those which are designed primarily for committing offences
- Does not necessary excluding dual-use devices

Art. 9

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
the **production, sale, procurement for use, import, distribution or otherwise making available** of:
• a device, including a computer program, designed or adapted **primarily** for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
• computer password, access code, or similar data by which the whole or any part of a computer system is **capable of being accessed,**
with **intent** that it be used for the **purpose of committing any of the offences** established in Articles 2 through 5; and
• the **possession of an item[...]**

ART 9: MISUSE OF DEVICES

- Restriction within the Convention
- Software tools necessary to ensure the protection of computer systems are not covered by the provision
- Authorised testing only

Art. 9

This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article **is not for the purpose of committing an offence** established in accordance with Articles 2 through 5 of this Convention, such as for the **authorised testing** or protection of a computer system.

HACKING

EU FRAMEWORK DECISION

FRAMEWORK DECISION

- Council Decision from the 24th February 2005
- **Implementation until** 16th March 2007
- Adds the existing Attempts to protect Information Systems (eg. Conditional Access Services Protection Act)
- Aim: Harmonisation of the National Legal Systems with regard to the protection of Information Systems in the EU
- Only Substantive Criminal Law
- Limited to EU Member States
- Limited to grave violations

- Cybercrime Convention follows a broader concepts

ART 2: ILLEGAL ACCESS

- Comparable to the Convention on Cybercrime
- Complete ban on hacking?
- Possible restriction: minor cases

Art. 2

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

ART 2: ILLEGAL ACCESS

- Possible restriction: committed by infringing security measures
- Conflict: Protection of unprotected Systems (eg open Webpage)
- Compared to the Convention on Cybercrime less reservations are possible (eg. intent to obtain computer data)

Art. 2

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.
2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

CONCLUSION

THANK YOU VERY MUCH FOR YOUR ATTENTION

QUESTION & REMARKS

gercke@cybercrime.de