# CYBERCRIME

DISCUSSION - THE IMPLEMENTATION OF THE CONVENTION ON CYBERCRIME IN BULGARIA

Plovdiv, 17th December 2007

Dr. Marco Gercke



# GENERAL REMARKS

- The requirement of a mental element ("mens rea") is only defining minimum standards
- The member states are free to criminalise even recklessness or negligence

*The purpose of Section 1 of the Convention (Articles 2 - 13) is to improve the means to prevent and suppress computer- or computer-related crime by establishing a common minimum standard of relevant offences.*
**Explantory Report, No. 38**

**Art. 2 - Illegal Access**

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.



# GENERAL REMARKS

- The requirement of acting "without right" leaves the member states much space for interpretation. It is from my perspective no problem with regard to the standards of the Convention if the member states limit the rights ("without the consent of the person administering or using a computer")

*„It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise)."*
**Explantory Report, No. 38**

**Art. 2 - Illegal Access**

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**.



# NATIONAL SOLUTIONS

- Most implementations show at least some difficulties
- Germany has not even ratified the Convention
- The Convention and not a national solution should be the model
- National solutions only relevant with regard to the experiences

**Art. 44 Romanian Penal Code**

The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence

- Damaging
- Suppression = Restriction?

**Art. 4 - Data interference**

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 **damaging, deletion, deterioration, alteration or suppression of computer data** without right.

## ILLEGAL ACCESS

- The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an **undisturbed** and uninhibited manner
- Integrity of Computer Systems

**Art. 2 - Illegal Access**

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. 319a PC**

Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine of up to BGN three thousand.



## ILLEGAL ACCESS

- Access to computer data = Access to a computer system
- Not be be mixed up with data espionage
- Is there any case where accessing a computer system does not go along with obtaining access to computer data
- Same approach in Germany
- Different dogmatic approach / Different legal interest protected
- In 99% of the cases the same result

**Art. 2 - Illegal Access**

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. 319a PC**

Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine of up to BGN three thousand.



## ILLEGAL ACCESS

- Bulgaria did not make a reservation with regard to Art. 2
- The reservation in paragraph 2 shows that the drafters were aware of the possibility to link the act to data by requiring an intent

**Art. 2 - Illegal Access**

(2) 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.



## ILLEGAL INTERCEPTION

- Protect the right of **privacy** of data communication - similar to the protection of other mass communication that is already established
- Only non-public transmissions
- Right to privacy of correspondence is enshrined in Article 8 of the **European Convention on Human Right**
- Listening to, monitoring or surveillance of the content of communications

**Art. 3 - Illegal Interception**

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 **interception** without right, made by **technical means**, of **non-public transmissions** of computer data to, from or within a computer system, including **electromagnetic emissions** from a computer system carrying such computer data.

**Art. 171(3) PC**

becomes aware of the content of an electronic message not addressed to him/her or prevents such a message from reaching its original addressee

## ILLEGAL INTERCEPTION

- Different dogmatic approach as the provision is not focusing on the act of interception but the result (becoming aware of the content)
- Difficulty: Art. 3 does not require that some becomes aware of the content (e.g. encryption)
- 171(3) is first of all a broader approach as it is not limited to the technical interception
- But the application of 171(3) is limited to electronic messages

**Art. 3 - Illegal Interception**

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 **interception** without right, made by **technical means**, of **non-public transmissions** of computer data to, from or within a computer system, including **electromagnetic emissions** from a computer system carrying such computer data.

**Art. 171(3) PC**

becomes aware of the content of an electronic message not addressed to him/her or prevents such a message from reaching its original addressee



## ILLEGAL INTERCEPTION

- Bulgaria did not make a reservation with regard to Art. 2
- Even a reservation would not solve the dogmatic challenges

**Art. 3 - Illegal Interception**

(2) A Party may require that the offence be committed with **dishonest intent**, or in **relation to a computer system** that is connected to another computer system.



## DATA INTERFERENCE

- Provide computer data and computer programs with protection similar to that enjoyed by **corporeal objects** against intentional infliction of damage
- **Integrity** of data and programmes

**Art. 4 - Data interference**

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 **damaging, deletion, deterioration, alteration or suppression of computer data** without right.

**Art. 319b PC**

Anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant, shall be punished by deprivation of liberty of up to one year or a fine of up to BGN two thousand



## DATA INTERFERENCE

- 319b covers the acts of deleting, altering and destroying computer data
- It is not certain if the provision covers the suppression of computer data (similar situation in Romania)

**Art. 4 - Data interference**

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 **damaging, deletion, deterioration, alteration or suppression of computer data** without right.

**Art. 319b PC**

Anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant, shall be punished by deprivation of liberty of up to one year or a fine of up to BGN two thousand

**Art. 44 Romanian Penal Code**

The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence

## DATA INTERFERENCE

- Bulgaria did not make a reservation with regard to Art. 2
- "where the occurrence is not considered insignificant" in the Bulgarian law is in line with the EU Framework decision on attacks against Information systems
- With regard to the Convention a reservation should have been taken into consideration (although not insignificant is not necessary a serious harm)

**Art. 4 - Data interference**

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in **serious harm**.