Friedrich-Alexander-Universität
Fachbereich Rechtswissenschaft

Cybercrime

SEC LAW 2024
Stockholms Universitet

Dr. Florian Nicolai
Friedrich-Alexander-University Erlangen-Nuremberg

Cybercrime and Forensic Computing
Research Training Group 2475

Stockholm University

Forms of Cybercrime

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

Cybercrime in the narrower sense

- **Crimes with computers, devices and data as a target, e.g.**
  - Phishing
  - Identity theft
  - (D)Dos Attacks
  - Ransomware Attacks

Cybercrime in the broader sense

- Fraud
- Harassment
- Cyberstalking
- Cyberbullying
- Child Pornography
- and much more

Basically every crime can be commited by the aid of IT technology

Forms of Cybercrime

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

Cybercrime in the narrower sense

- **Crimes with computers, devices and data as a target, e.g.**
  - Phishing
  - Identity theft
  - (D)Dos-Attacks
  - Ransomware attacks

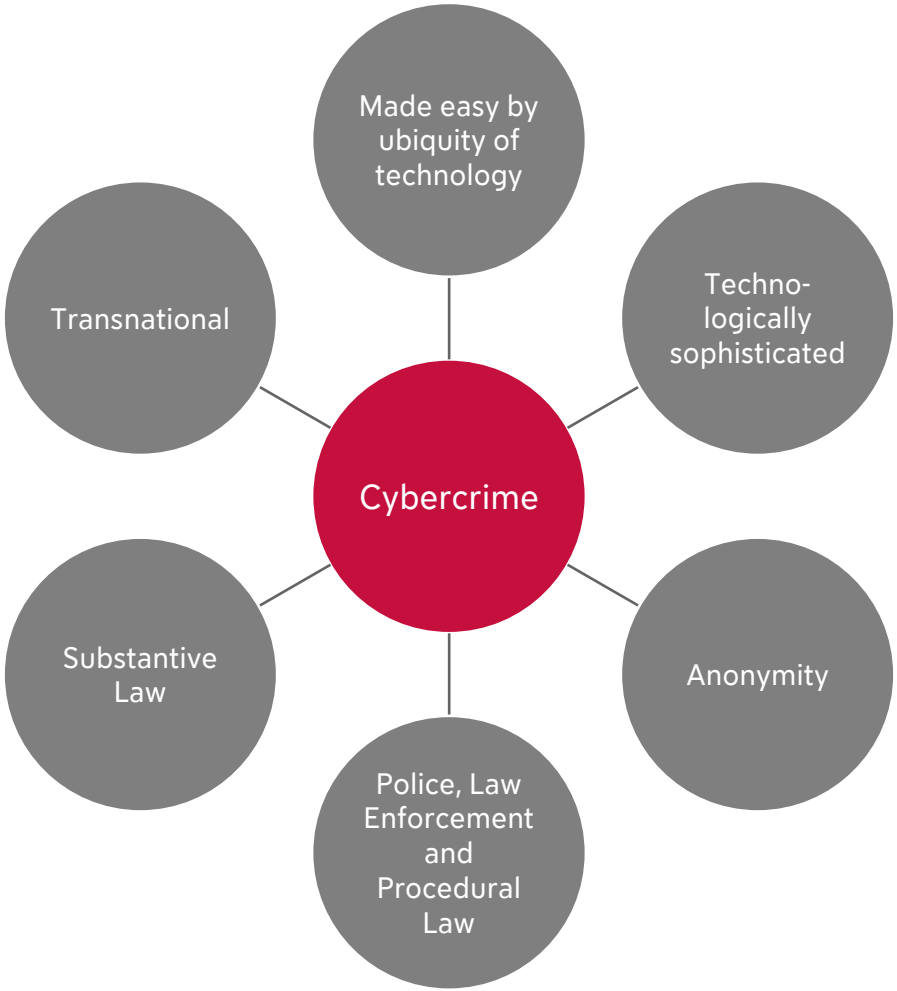
Especially those cases lead to data privacy issues

Cybercrime in the broader sense

- Fraud
- Harassment
- Cyberstalking
- Cyberbullying
- Child Pornography

Basically every crime can be commited by the aid of IT technology

Challenges


Made easy by ubiquity of technology
Techno-logically sophisticated
Anonymity
Police, Law Enforcement and Procedural Law
Substantive Law
Transnational
Cybercrime

The Convention on Cybercrime – A treaty to fight those challenges

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

Convention on Cybercrime (2001)

- Convention of the Council of Europe
- Ratified by almost every member of the Council and other countries as well
- Harmonisation / Establishing ground standards

Substantive Law

Procedural Law

Mutual Assistance

The Convention on Cybercrime – Substantive Law

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

- States have to implement offences that sanction:
  - Illegal Access
  - Illegal Interception
  - Data Interference
  - System Interference
  - Misuse of Devices

Computer, devices and data as target of the crime (Cybercrime in the narrower sense)

  - Computer-related Offences
  - Content-related Offences
  - Copyright-related Offences

Challenges – Substantive Law

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

Section 202a German Criminal Code
Data espionage

(1) Whoever, without being authorised to do so, obtains access, by circumventing the access protection, for themselves or another, to data which were not intended for them and were specially protected against unauthorised access incurs a penalty of imprisonment for a term not exceeding three years or a fine.

The Convention on Cybercrime – Procedural Law

- States have to implement rules that allow, *e.g.*
  - Art. 16 – Expedited preservation of stored computer data
  - Art. 19 – Search and seizure of stored computer data
  - Art. 20 – Realtime collection of traffic data
  - Art. 21 – Interception of content data

But

- The fight against Cybercrime raises privacy issues itself
- Fundamental Rights
- Human Rights

Transnational Investigations

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

- Transnational Investigations to fight transnational Cybercrime?
  - Volatile data stored in other countries
  - No acces via national law
  - No acces via international customary law

- Transborder Access without legal basis?
  - Diplomatic conflicts
  - **Exclusion of evidence**

➔ Mutual Judicial Assistance

Transnational Investigations

- Transnational Investigations to fight transnational Cybercrime?
  - Volatile data stored in other countries
  - No acces via national law
  - No acces via international customary law

Territoriality / Sovereignty

- Do it anyway?
  - Diplomatic conflicts
  - **Exclusion of evidence**

➔ Mutual Judicial Assistance

Transnational Investigations

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

Mutual judicial assistance

- Various legal bases ➔ confusing mesh of European and bilateral agreements
- Time-consuming while risk of losing digital evidence
- Several approaches of unification within Europe, e.g.
  - European Evidence Warrant: failed
  - Now: European Investigation Order (EIO)
  - European Prosecution Office (EPPO)

The Convention on Cybercrime – Mutual Assistance

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

- Art. 29: Expedited preservation of stored computer data (quick-freeze)
- Art. 30: Expedited disclosure of preservered traffic data
- Art. 31: Mutual assistance regarding accessing of stored computer data
- Art. 32: Trans-border access to stored computer data with consent or where publicly available
- Art. 33: Mutual assistance in the real-time collection of traffic data
- Art. 34: Mutual assistance regarding the interception of content data
- Art. 35: 24/7 Network

The Convention on Cybercrime – Mutual Assistance

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

- Art. 29: Expedited preservation of stored computer data (quick-freeze)
- Art. 30: Expedited disclosure of preservered traffic data
- Art. 31: Mutual assistance regarding accessing of stored computer data
- Art. 32: Trans-border access to stored computer data with consent or where publicly available
- Art. 33: Mutual assistance in the real-time collection of traffic data
- Art. 34: Mutual assistance regarding the interception of content data
- Art. 35: 24/7 Network

The Convention on Cybercrime – Mutual Assistance

Cybercrime and Forensic Computing
Research Training Group 2475

FAU

Art. 29: Expedited preservation of stored computer data (quick-freeze)

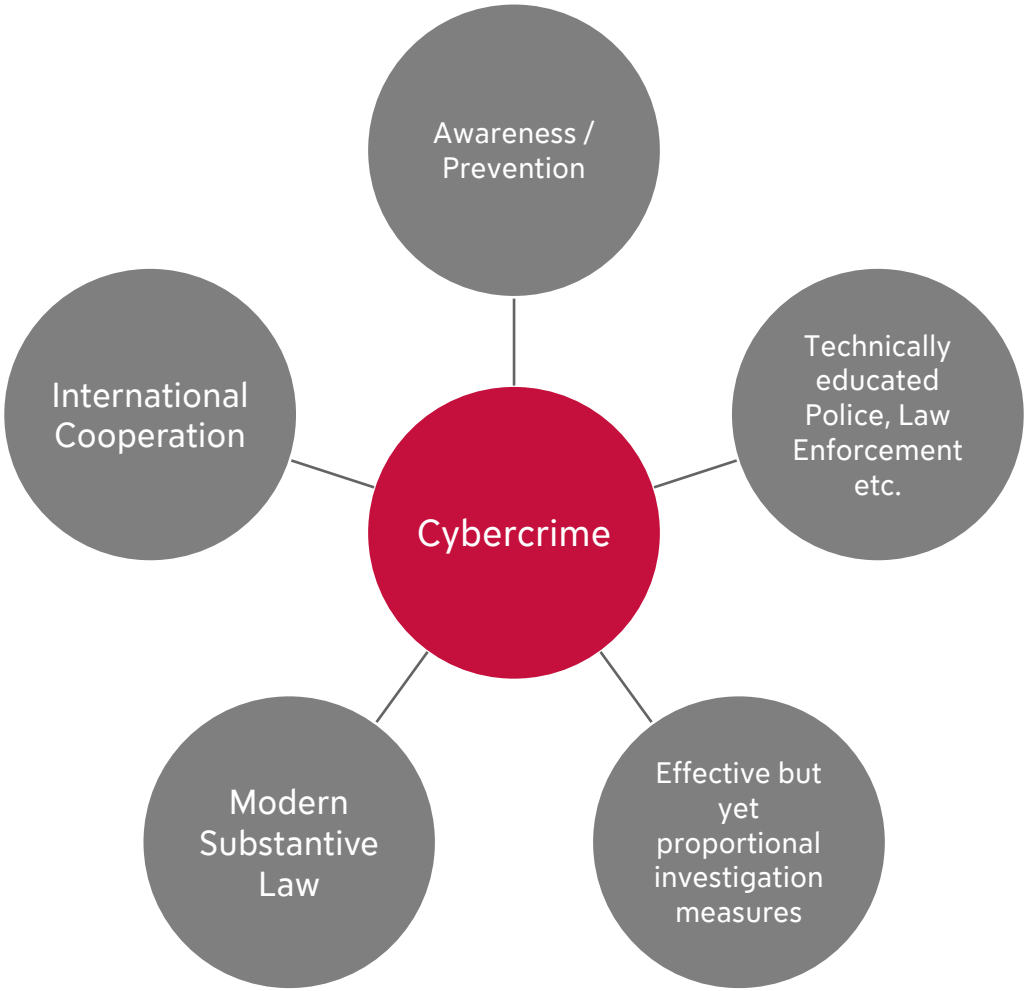
- Preservation of stored computer data ➔ in preparation for mutual assistance
- Aim: Preventing data from vanishing
- Limits
  - Dual Criminality
  - National Sovereignty / National Security (*ordre public)*
  - National procedural rules ➔ Quick ≠ quick

The Convention on Cybercrime – Mutual Assistance

Art. 32: Trans-border access to stored computer data with consent or where publicly available

- A real trans-border measure
- Trans-border access to stored computer data, but only if:
  - Consent ➔ by the user, whose data is stored
  - Publicly Available
- Limits
  - Mostly *not* publicly available
  - Perpetrator will hardly give consent

Conclusion


Awareness / Prevention
International Cooperation
Technically educated Police, Law Enforcement etc.
Cybercrime
Modern Substantive Law
Effective but yet proportional investigation measures

Friedrich-Alexander-Universität
Fachbereich Rechtswissenschaft

Thank you very much.

Florian.Nicolai@fau.de

www.cybercrime.fau.de
www.str2.rw.fau.de