

Kapitel 4.18 Informationstechnologie

● **Informationstechnologie (IT)**

- „Elektronische“ Beweismittel = Sachbeweis

● **„Cyber-Attacken“**

- Computerkriminalität
- Militärspionage
- Wirtschaftsspionage
- Cyberkrieg

Einfallmöglichkeiten

- Verwendung von allgemeiner Software
- Verwendung von W-Lan-Zugang
- „Geliehene“ Sticks
- Laptops von Wartungstechnikern

● **Straftaten**

- Computerbetrug (§ 263 a StGB)
- Computersabotage (§ 303 b StGB)
- Fälschung von Geld und Wertzeichen mithilfe der Elektronik (§ 149 StGB)
- Jegliche Art von strafbaren Handlungen, bei deren Ausführung elektronischen Geräten benutzt werden.

● **Geräte**

Computer, Netzwerke, Internet, Mobilfunk (Handy), Elektronische Notizbücher, Heim-Elektronik wie Festnetztelefone oder Video-/DVD-Rekorder sowie Chip-Karten und Magnet-Karten.

4.18.1 IT-Beweissicherung

- **Beschlagnahme** von IT durch Sachunkundige
 - **nichts** verändern
 - **nichts** ein- oder ausschalten
 - **nicht** nachschauen
 - **nicht** nach etwas Brauchbarem suchen
 - **Geräte dem Fachmann übergeben !!!**

- **Ermittlungsgruppen**
Bundeskriminalamt, Landeskriminalämter,
Bundespolizei, Zoll, Steuerfahndung, Bundeswehr
und Bundesamt für Sicherheit in der
Informationstechnik (BSI) hat 2011 ein „Cyber-
Abwehrzentrum“ eingerichtet (DHB KR, Kapitel 2,
Seite 14)

4.18.2 Datenauswertung

- Durch Fachleute