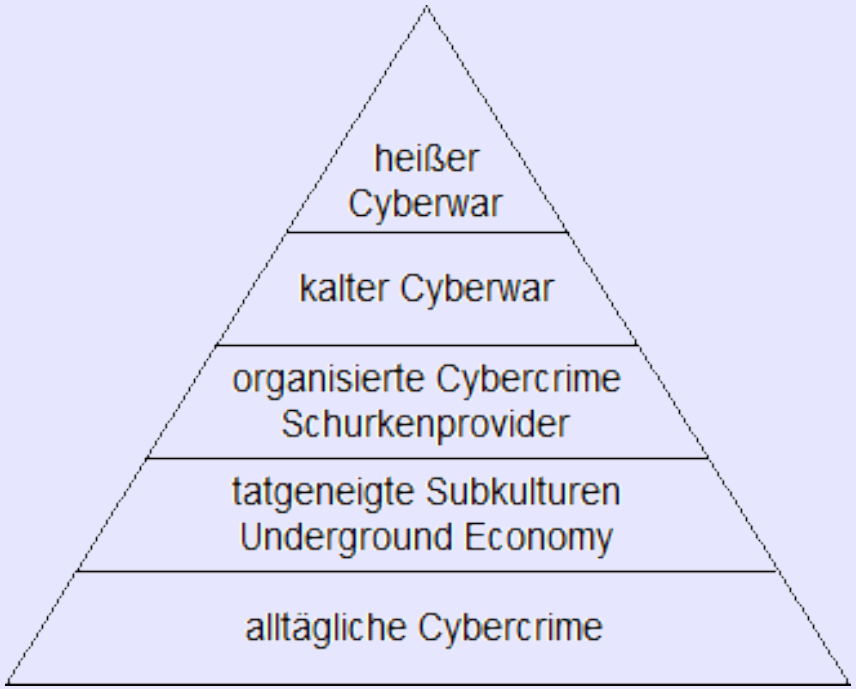
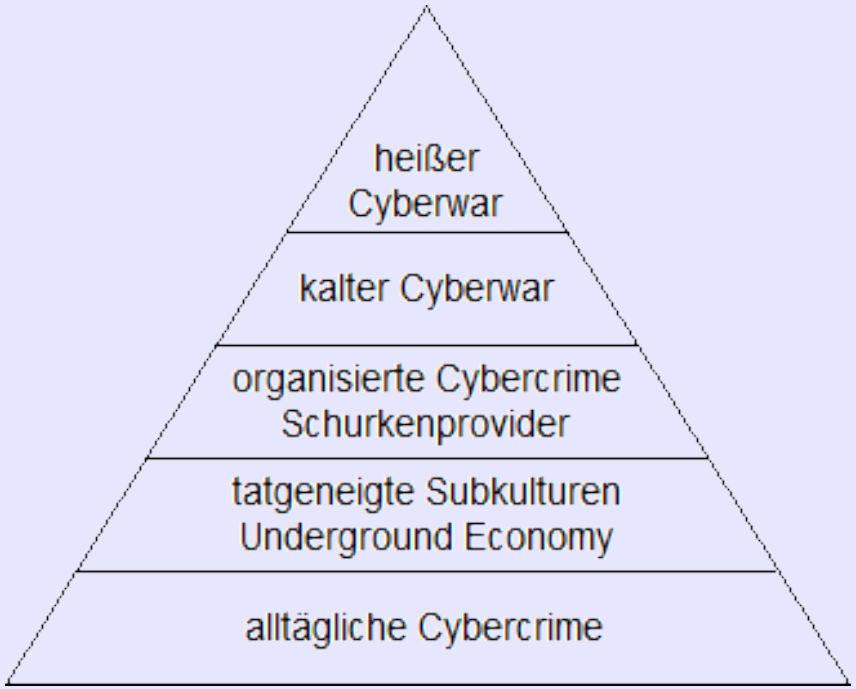
allgemeine Internetkriminalität



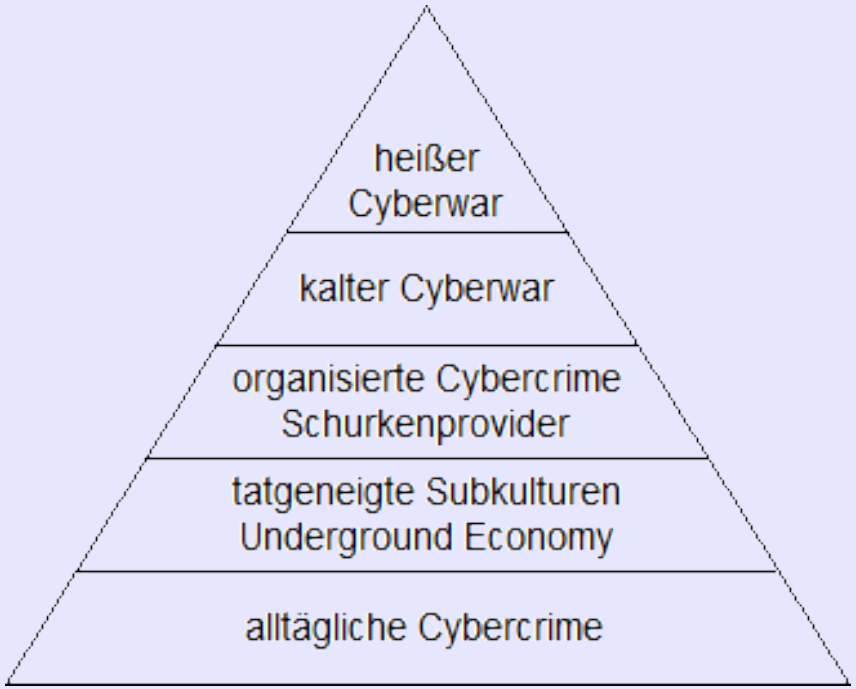
- Datendiebstahl *(Konten, Banking)*
  - Identitätsdiebstahl
  - Phishing
  - Finanzagenten
- „eBay“-Betrug
  - falsche Produktbeschreibungen
  - Vorauszahlungsbetrug
- Warenbetrug
  - falsche Identitäten
  - Fake-Adressen
  - Warenagenten
  - Packstationen
- Carding, Skimming
- Geldwäsche
  - „graue“ Zahlungssysteme
  - Kreditkarte auf Guthabenbasis

gewerbsmäßige Internetkriminalität



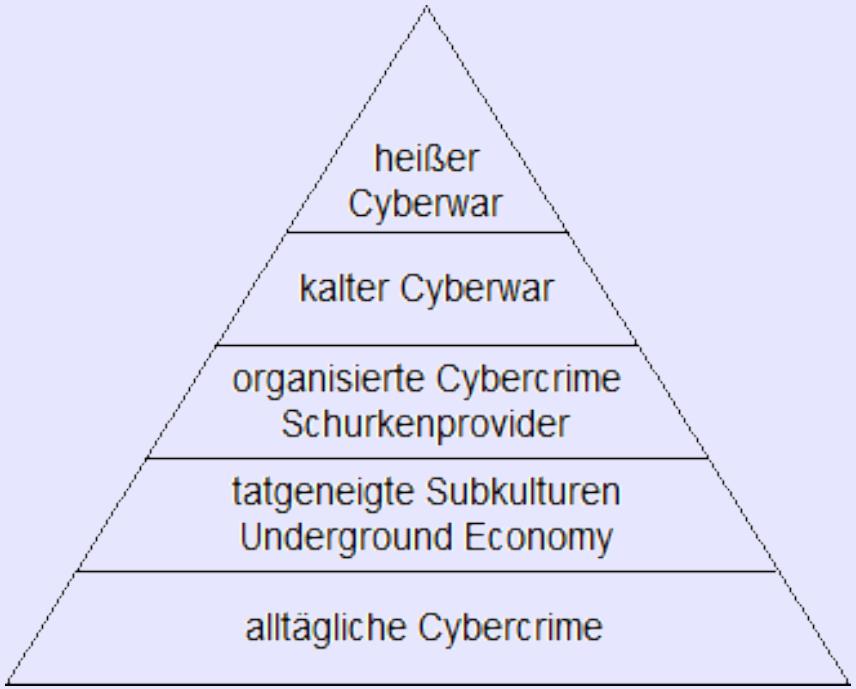
- **Board-Administratoren**
- **Malware-Entwickler**
  (Operating Groups)
- **Exploit-, Rootkit-Händler**
- **Projektleiter *(Koordinatoren)***
- **Webshop-, Inkassodienste**
- **„Wechselstuben“**
- **Hacktivisten**

organisierte Internetkriminalität



- **Board-Betreiber**
- **Botnetz-Betreiber**
- **Schurkenprovider**

kalter Cyberwar

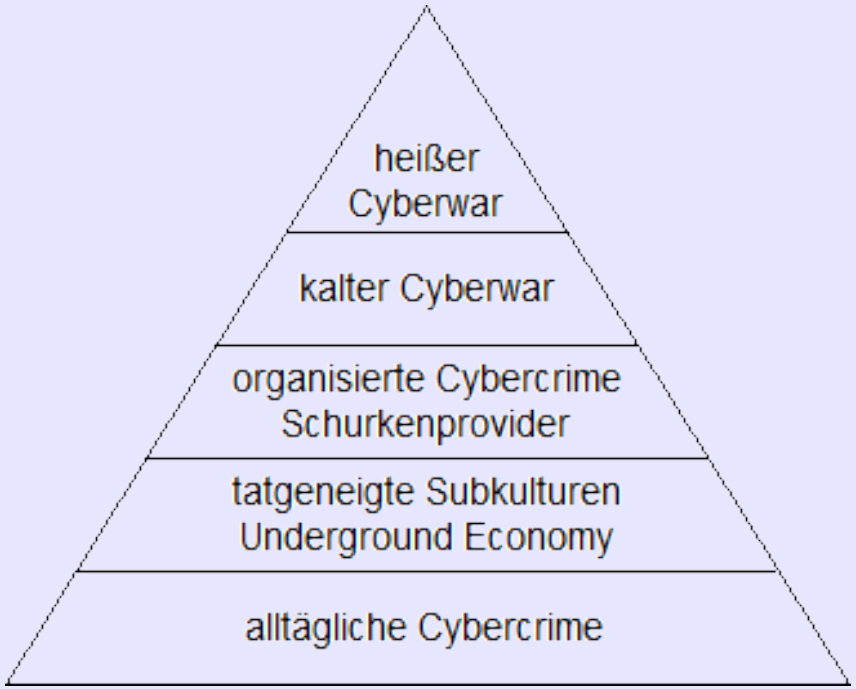


taktische Phase des Kräftemessens
Was kann ich bewirken?
Wie sind die Gegner aufgestellt?
Wie reagieren sie?

weitere „Mitspieler“

- **organisierte Kriminalität**
- **Nachrichtendienste**
- **Militär**
- **Paramilitär**
- **Terroristen**
- **Hacktivisten**
- **Wirtschaftsunternehmen**
- **Söldner**

heißer Cyberwar



Cyberwar ist der strategische Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt.

Erst in der Heißen Phase des Cyberwar dürften neben den bekannten Methoden der Cybercrime ganz verstärkt terroristische und militärische Einsätze zu erwarten sein.