



MILITÄRISCHE CYBERWAFFEN UND DEREN PROLIFERATION

Herausforderungen und Lösungsansätze



- 2010 - Stuxnet: Realität von "Cyberwaffen"
- 2013 - Studie UNIDIR
 - ~10 Staaten mit offensiven Cyber-Planungen
- 2016 - NATO: Cyber ist Bestandteil der kollektiven Verteidigung
- 2017 - Bundeswehr: Kommando Cyber und Informationsraum (KdoCIR)

- Begrenzung des militärischen Bedrohungspotentials ?



- Cybercrime vs. Cyberwar
 - Kriminalität > Regelungen der internationalen Strafverfolgung
 - Staatliche Cyberattacken > Völkerrecht
- "Cyberwaffe" im Sinne des Völkerrechts
 1. Analogie zu klassischen Waffen: **zielgerichtet, kontrollierbar, vorhersagbarer Schaden**
 2. Bewertung des tatsächlichen Schadens: **Spionage, Störung, Sabotage**
 3. Intention des Angreifers: **Strategische Zielauswahl, beabsichtiger Zweck & Schaden**

- Vorfälle von „Cyber-Angriffsformen nach der Definition des BSI (..) auf Behörden und öffentliche Stellen in dem Jahr 2016“

Gezieltes Hacking von Webservern	2
Drive-by-Exploits zur breitflächigen Infiltration	1.572.655
Gezielte Malware-Infiltration über E-Mail / Social Engineering	ca. 3/Woche
Distributed Denial of Service-Angriffe (DDoS)	17
Ungezielte Verteilung von Schadsoftware mittels SPAM oder Drive-by-Exploits	3.815.611
Mehrstufige Angriffe	0
	5.388.441

Informationsfreiheitsanfrage: <https://fragdenstaat.de/anfrage/cyber-angriffsformen-nach-bsi-2016/>



- Problem der Gefährungsbewertung
 - Lagebild zur nationalen IT-Sicherheit
 - Melde-Systeme für Vorfälle und Warn-Mechanismen
- Abhängigkeit von IT und den "Global Playern" in diesem Segment
- Bewertung des Zerstörungspotentials

- Anwendbarkeit etablierter Regeln des Völkerrechts ?



- Technische Spezifika im Vergleich zu A/B/C-Waffentechnologien
 - Dual Use
 - Duplizierbarkeit und Virtualität
 - Attributions-Diffusion
- Sicherheitslücken als das "Grundmaterial" der Cyberwaffen
 - Handel und Marktwert von Sicherheitslücken
 - Gefährdung von IT durch Geheimhaltung
 - Neue Akteure durch "billige" Cyberwaffen



- **Gestaltbarkeit und Verantwortung**
 - Cyberspace ist eine "man made domain"
 - Renaissance der Technikfolgeabschätzung
- **Rüstungskontrolle und Begrenzung im Cyberspace**
 - Verbindliche Definitionen: "intrusion software" im Wassenaar-Abkommen als Vorlage ?
 - Regelungen zum staatlichen Umgang mit Schadsoftware (Vulnerability equity process)
 - Internationale Regelungen zum Cyberwaffen-Handel
- **Forschung zu technischer Kontrolle, Verifikation & Monitoring**