IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

# MILITÄRISCHE CYBERWAFFEN UND DEREN PROLIFERATION

## Herausforderungen und Lösungsansätze

# Militärische Akteure im Cyberspace

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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 ?

# Was sind Cyberwaffen (und was sind keine)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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

# Fallzahlen Cyber-Vorfälle 2016

- 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/

# Bedrohung und Herausforderungen aus friedenspolitischer Sicht

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Problem der Gefährungsbewertung
  - Lagebild zur nationalen IT-Sicherheit
  - Melde-Systeme für Vorfälle und Warn-Mechanismen
  - Technische Qualitätssicherung von Software
  - IT-Sicherheitsanalysen im Angesicht omnipotenter Angreifer
- Abhängigkeit von IT und den "Global Playern" in diesem Segment
- Bewertung des Zerstörungspotentials

# Proliferation von Cyberwaffen und deren "Grundmaterial"

- 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

# EternalBlue - Blaupause des Worst-Case

- Ursprung von EternalBlue
  - Zero-Day-Exploit im "Giftschrank" der NSA für alle Windows-Versionen ab Windows XP
  - EternalBlue durch "ShadowBroker" gestohlen und 04/2017 veröffentlicht
  - Warnung an Microsoft: Sicherheitsaktualisierung für Windows 7 aufwärts

- Vorfall #1: WannaCry
  - Mai 2017, scheinbare Ransomware
  - 200.000 Systeme in 150 Ländern
  - Zero-Day-Exploit in Windows-Netzwerken
  - Exploit aus Leaks von NSA-Beständen (EternalBlue)
  - "Killswitch" eingebaut

# EternalBlue - Blaupause des Worst-Case /2

- Ursprung von EternalBlue
  - Zero-Day-Exploit im "Giftschrank" der NSA für alle Windows-Versionen ab Windows XP
  - EternalBlue durch "ShadowBroker" gestohlen und 04/2017 veröffentlicht
  - Warnung an Microsoft: Sicherheitsaktualisierung für Windows 7 aufwärts

- Vorfall #2: NotPetya
  - Juni 2017, scheinbare Ransomware gegen politische Einrichtungen und Industrie in der Ukraine, Europa, Russland und USA
  - Explizit zerstörerischer Payload
  - Eingebettet in spezielle Buchhaltungs-Software
  - Enormer wirtschaftlicher Schaden durch IT-Ausfälle