VERIFIKATION IM CYBERSPACE

Ansätze und technische Grundlagen für die Kontrolle von Cyberwaffen

Stand der Militarisierung des Cyberspace

- UNIDIR "The Cyber Index - International Security Trends and Realities“, 2013
  - 47 Staaten mit militärischen Cyberdoktrinen
  - 10 Staaten mit explizit offensiven Programmen
- USA: Cyber Command eigenständige Militäreinheit
- Russland
  - 2017 Einrichtung einer "Abteilung für Informationssicherheit und Cyberabwehr"
  - Steuerung nicht-staatlicher Gruppen durch Nachrichtendienste (APT 28, Fancy Bear, Sofacy ...)
- Frankreich: Cyber-Doktrin mit Auftrag zu Offensiv-Fähigkeiten
- Neue Akteure z.B.: Nord-Korea, Iran
- Deutschland
  - Bundeswehr: "Kommando Cyber & Informationsraum" (CIR)
  - ZITiS & Agentur für Innovationen in der Cybersicherheit
  - Cyberfähigkeiten für NATO-Einsätze bereitgestellt

Relevante Vorfälle

- Eternalblue, WannaCry & NotPetya
  - Zero-Day-Exploit aus "Giftschrank" der NSA für alle Windows-Versionen ab Windows XP
  - EternalBlue durch "ShadowBroker" gestohlen und 04/2017 veröffentlicht
  - Mai 2017 WannaCry Ransomware: 200.000 Systeme in 150 Ländern
  - Juni 2017 NotPetya, gezielte Attacken gegen politische Einrichtungen und Industrie in der Ukraine, Europa, Russland und USA
- Hacking-Attacken gegen Deutschland:
  - 2015 Parlakom-Hack: Datenspionage im IT-System des Bundestages
  - 2017/2018 Hack des Regierungsnetze: Spionage auswärtiges Amt
  - 2019 Datenleaks: Daten von Abgeordneten veröffentlicht
- etc. ...
  - APT28, Sofacy, Fancy Bear, Cozy Bear
  - 2015 Hack TV5
  - 2016 Democratic National Commitee
  - 2018 OPCW

Internationale Initiativen

- UN
  - 2003 UN Beschluss zu Fokus auf Bedrohungen der internationalen Sicherheit im Cyberspace
  - 2015: Verabschiedung unverbindlicher Normen für staatliches Verhalten im Cyberspace
    - Verantwortlichkeit für "nationalen" Cyberspace
    - Keine Aktivitäten die wissentlich IT-Systeme schädigen können durchführen oder dulden
- OSZE
  - Beschlüsse 2013 und 2016: Cyberspace als gemeinsame, internationale Ressource
  - Schutz und Unversehrtheit kritischer Infrastrukturen
- Zwischenstaatliche und ziviligesellschaftliche Initiativen
  - Paris Call for Trust and Security in Cyberspace - Frankreich, 2018
  - Commonwealth Cyber Declaration - Commonwealth Heads of Government Meeting, 2018
  - "Contract for the web" - Tim Berners-Lee, 2018
- Vorstöße aus der Wirtschaft
  - Mircosoft: "Digitale Genfer Konvention“, 2017
  - Google: "Digital security and due process: A new legal framework for the cloud era", 2017
  - Siemens: "Charter of Trust“, 2018

Praktische Maßnahmen der Rüstungskontrolle

Technische Herausforderungen durch den Cyberspace

- Dual Use von IT-Technologie
- Duplizierbarkeit von Software & Daten
- Virtualität
- Abbildung territorialer Souveränität und Grenzen im Cyberspace
- Das “Payload"-Problem
  - Abgrenzung zwischen Kriminalität, Spionage und Sabotage
  - Eher Frage der Motivation des Akteurs als der angewandten technischen Mittel
- Attribution im Cyberspace
  - Maßgebliche Voraussetzung für Recht auf Selbstverteidung UN Charta Art. 51
  - Möglichkeiten zur Verschleierung
  - Nur nachträglich forensisch rückverfolgbar

ϟ Haftung, Kontrolle, Regulation und Limitierungen problematisch

Was kann man messen im Cyberspace

- Disclaimer:
  - Wir betreten Neuland
  - Mögliche Maßnahmen stets nur zielgerichtet und partiell anzuwenden
- Messbar "von Außen" ohne spezielle Anpassungen
  - Verbrauch und Kapazitäten der Stromversorgung
  - Termische Leistung der Kühlsysteme
  - Netzwerkbandbreiten und maximale Kapazitäten
  - Umfang, Menge und Datenraten der Netzwerk-Verbindungen
  - Personal
  - => viele Parameter durch existierende Systeme meßbar
  - => geeignet für Überwachung des Status Quo von Anlagen

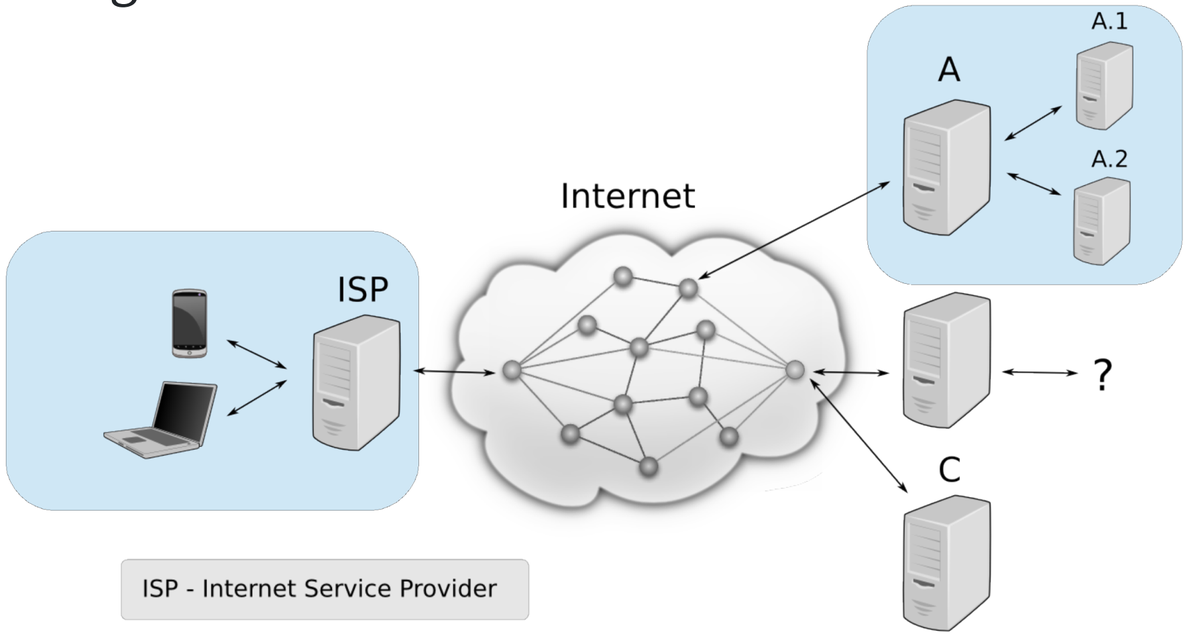
Was kann man messen im Cyberspace /2

- Disclaimer:
  - Wir betreten Neuland
  - Mögliche Maßnahmen stets nur zielgerichtet und partiell anzuwenden
- Messbar "von Innen"
  - Metadaten der Netzwerkverbindung (wer überträgt was wohin und wie oft)
  - Nutzung von Anonymisierungsdiensten
  - Digitale Artefakte, Exploits und Sicherheitslücken ("Reverse-IDS")
  - => Überwachung der Anwendung von Systemen
  - => Starker Eingriff in die Kontrolle der Anwendung von IT
  - => Akzeptanz und politische Bereitschaft fraglich

Technische Ansatzmöglichkeiten

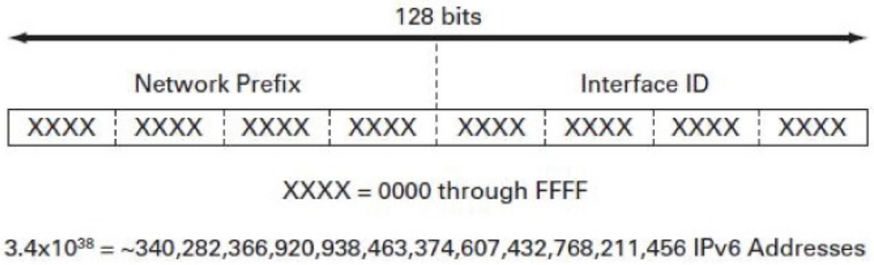
- Cyberspace als einzigartige **“man made domain"**
- Übertragung bestehender IT-Verfahren auf Bereich der Rüstungskontrolle

- Speicherung / Austausch / Sichtung von Verbindungsdaten
  - Unilaterale Selbstverpflichtung zur Transparenz
  - Überwachung der defensiven Orientierung von Cyberprogrammen
  - Rückverfolgung ungewöhnlicher Aktivitäten
  - Maßnahmen der Datenfluß- und der Inhaltsanalyse



Technische Ansatzmöglichkeiten /2

- Lokalisierung, Grenzen und Verantwortlichkeiten
  - Staatliche Souveränität
  - Verlässlichkeit für andere Staaten
- Authentizität und Proliferation
  - Blockchain für fälschungssichere Logging-Daten
  - Digital Rights Management für Proliferations-Kontrolle
- Identifizierbarkeit sensibler Systeme
  - Eindeutige Markierung der Datenströme und deren Ursprung
  - Kennzeichen zur Reduktion irrtümlicher Annahmen



330522

Lessons learned ?

- Erfahrungen mit anderen Technologien
- Analogien zum Cyberspace
- Probleme und Chancen

Vielen Dank

Thomas Reinhold
reinhold@ifsh.de
cyber-peace.org