Protokoll zu Workshop 4 der CODE JT 2018

Begrüßung durch Dr. Byok

- Das Thema Cybersicherheit wurde bislang in Deutschland (DE) vernachlässigt
- Neue Kommandos/Behörden (z.B. CIR) sollen neue Impulse geben
- Steigende mediale Präsenz und erhöhtes Interesse am Thema Cybersicherheit
- Problem aus juristischer Sicht: Bei Cyber-Attacken sind Verantwortliche/Verursacher häufig nicht identifizierbar (Attributionsproblematik), Kompetenz (innere/äußere Sicherheit)
- Aus militärischer Sicht erforderlich sind:
    - Resilienzbildung/Härtung von militärischen IT Systemen erforderlich wegen zunehmender Anfälligkeit (forcierte Digitalisierung der Landstreitkräfte) und
    - offensiver Fähigkeiten auszubilden (Zentrum für Cyberoperationen (ZCO))

Vortrag Dr. Herpig: Digitaler Gegenangriff Hackback

- Definition: *Eine aktive Gegenmaßnahme unterhalb der Schwelle des bewaffneten Konflikts, die dazu ausgelegt ist einen Cyberangriff abzuwehren und/ oder aufzuklären* (*Quelle: Herpig, Stiftung neue Verantwortung, 2018)*
- Debatte in DE derzeit im zivilen und nicht im militärischen Kontext
- Aktivitäten im Rahmen des digitalen Gegenangriffs lassen sich wie folgt kategorisieren:
    - Passive Verteidigung: Dient zum Sammeln von Informationen, zur Prävention und zur Erkennung von Cyber-Angriffen
    - Aktive Verteidigung: Nutzung von Datenfallen, ISP Unterstützung und aktiver Informationssammlung (z.B. Beacons) zur Aufklärung und Reaktion auf Cyber-Attacken
    - Übernahme der externen Angreifer-Infrastruktur: Dient zur Reaktion und Aufklärung von Cyber-Angriffen sowie als repressive Maßnahme gegen den Angreifer (*Quelle: Herpig, Stiftung neue Verantwortung, 2018)*
        - Unterstützung durch ISP zum Unterbinden von Bots
        - Umfasst koordinierte Botnet Takedowns
        - Nutzung von Command-und-Control Infrastruktur um Bot-Rechner zu desinfizieren
    - Infiltration interner Struktur: Dient der Aufklärung von Cyber-Attacken; beispielsweise übernehmen Datenfallen zerstörerische Aktionen, wenn auf diese ein Zugriff erfolgt (z.B. Verschlüsselung); Aufklärung in Systemen der Angreifer über beispielsweise Sensoren, Kameras, etc., um die Zurechenbarkeit zu verbessern

- Ein zentrales Problem für Gegenangriffe ist die Attribution, da die Urheber von Cyber-Angriffen nur schwierig zu finden respektive greifbar sind. Aufgrund dessen besteht auch das Risiko, falsche Ziele (z.B. Rechner in Krankenhäusern) zu treffen und so Kollateral-Schäden zu verursachen.
- In den USA gibt es die Diskussion, ob private Firmen Hackbacks straffrei durchführen dürfen (Active Cyber Defense Certainty Act 2.0 (ACDC)). Der *Active Cyber Defense Certainty Act* erlaubt in bestimmten Fällen Privatfirmen, straffrei Hackbacks durchzuführen.

- Gefahr der politischen Eskalation bei Hackbacks
- Offensive Cyber-Fähigkeiten können die defensive Mission von öffentlichen Behörden schwächen.
- Da Cyber-Angriffe nicht selten aus dem Ausland erfolgen, bewegt man sich bei Gegenangriffen rechtlich gesehen zumeist in einem Bereich, der außerhalb der deutschen Rechtsprechung liegt.
- Situation hinsichtlich der Durchführung von Hackbacks in Deutschland:
    - Es fehlen noch empirische und rechtliche Grundlagen
    - Politische Diskussion über das Zurückstehlen von Daten
    - Problematik der Attribution
    - Fachpersonal ist nicht ausreichend verfügbar (Industrie ist für IT Spezialisten attraktiver) und muss aus aktuellem Bestand genommen werden
    - Invasivere Maßnahmen nur mit Aufklärung, nicht mit Verweis auf mehr IT-Sicherheit zu rechtfertigen
    - Momentan sind Hackbacks der zivilen und nicht der militärischen Domäne zugeordnet (BMI)

In Deutschland besteht die Dringlichkeit nach einer sachlichen, öffentlichen Debatte über die Ausführung von Hackbacks

Vortrag Stefan Sohm: Verfassungs- und völkerrechtliche Aspekte der Verteidigung im Cyber- und Informationsraum

- Cyber-Angriffe können militärischen Hintergrund haben
- Der Einsatz der Bundeswehr im Cyberraum unterliegt den allgemeinen rechtlichen Voraussetzungen für einen Einsatz der Streitkräfte!
    - Verfassungs-und Völkerrecht sind prinzipiell anwendbar
    - Auf absehbare Zeit sind keine neuen völkerrechtlichen Regelungen zur militärischen Nutzung des Cyber-Raums zu erwarten
    - Computer-Netzwerk-Operationen stellen keinen Verstoß gegen völkerrechtliche Vorgaben
- Cyber-Angriffe können u.a. als Informationswaffe betrachtet werden: Kenntnis von vertraulichen Inhalten könnten zur Destabilisierung eingesetzt werden
- Cyber-Angriffe können verhältnismäßiger als kinetisch Angriffe sein
- Einsatzkategorien:
    - Im Rahmen militärischer Einsätze
    - Schutz der eigenen Infrastruktur
    - Als subsidiäre Unterstützung ziviler Behörden
- Zuständigkeit der Bundeswehr ist bei militärischen Einsätzen immer gegeben
- Völkerrechtliche Grundlage: Friedensvölkerrecht vers. Recht des bewaffneten Konflikts
- Cyber-Angriffe können die Schwelle zum bewaffneten Angriff überschreiten und auch menschlichen Schaden nach sich ziehen
- Humanitäres Völkerrecht (Kriegsvölkerrecht, ius in bello) findet Anwendung, wenn ein virtueller Angriff die Schwelle zum das Selbstverteidigungsrecht auslösenden bewaffneten Angriff überschreitet.
    - Das Konfliktvölkerrecht soll ein Mindestmaß an Humanität gewährleisten

  - Grundsätze sind u.a. Exzessverbot, Unterscheidungsgebot
- Zentrale Fragestellung, wie die Schwelle zu definieren ist, ab der ein Cyber-Angriff als bewaffneter Angriff angesehen werden kann (Wirkung in Realität; Schädigung von Menschen an Leib und Leben)
  - Fake News reichen dafür in der Regel nicht aus
  - Um die Schwelle des bewaffneten Angriffs zu überschreiten, muss der Cyber-Angriff mit Blick auf Umfang bzw. Wirkung dem Einsatz konventioneller Waffen und kriegerischen Handlungen gleichkommen.
- Man muss nicht mit Cyber-Angriffen auf Cyber-Attacken antworten
- Schutz eigener Infrastruktur: Hackback ist vielleicht nicht das erste Mittel der Wahl
- **Ein gesondertes „Digitales Recht" respektive Cyber-Sonderrecht ist nicht erforderlich**

Vortrag Steve Ritter: Informationssicherheit – Grund und Grenzen der Regulierung im Cyberraum

- Warum will man etwas regulieren? → Befugnis-Schaffung
- Computergrundrecht:
  - Geschaffen durch Entscheidung des BVerfG im Jahre 2008. Das Telekommunikationsgesetz bezog sich nur auf Strecke zwischen Kommunikationspartner
  - Grundrecht auf Vertraulichkeit und Integrität
  - Gewährleistungsaspekt
- Digitalisierung bringt Gefahren und Risiken mit sich:
  - Streaming Boxen öffnen häufig ungesicherte Webserver
  - IOT (Internet of Things) Devices sind aus Kostengründen häufig schlecht abgesichert und bieten Angreifern Lücken (Bsp.: Kühlschrank schickt Spam Emails)
  - Persirai Botnet: Nutzung von IP Kameras für DDoS Angriffe
- Möglichkeiten der Regulierung:
  - Gesetzliche Haftungsregulierung
    - Problem: Frage ob alle Patches vom Nutzer eingespielt worden sind
  - Option der Verkäuferhaftung
  - Strafrecht: Verbote als Mittel
  - Technische Vorgaben für Produkte
  - Zulassungsbeschränkung für Produkte
- Grenzen der Regulierung:
  - Bestimmung des Marktorts von Anbietern und Diensten
  - Was passiert, wenn der Hersteller im Ausland ist
  - Wer haftet bei Open Source Produkten
  - Während Angreifer international operieren findet die Regulierung lokal statt
  - Netzsperren sind problematisch
- Gewährleistung durch Befugnis Erweiterung:
  - Zwangsbereinigung, Gegenangriff, Netztrennung
  - Problem der Attribution ist gegeben
  - Befugnis Ausübung kann Eingriff in Grundrecht darstellen

Zusammenfassend ist auch im Themenkomplex der Regulierung im Cyberraum noch eine ausdifferenzierte Debatte erforderlich

Vortrag RA Florian Glatz: Blockchain: Chancen, Risiken, Recht

- Bitnation Deutschland: Deutschland ist der zweitgrößte Betreiber von Fullnodes im Bitcoin Netzwerk; 20 % aller Fullnodes stammen aus Deutschland.
- Initial Coin Offerings (ICO) stellen eine neue Möglichkeit der Kapitalakquise dar und sind in Teilen vergleichbar mit einer initialen Ausgabe von Wertpapieren.
- Was ist eine Blockchain? → Entspricht einer unveränderlichen chronologischen Datenbank, die gewisse Informationen aufzeichnet und von Akteuren in einem Netzwerk geteilt wird. Die Datenbank ist dabei auf mehrere Rechner verteilt (dezentral) wobei spezielle Algorithmen verfügbar sind die gewährleisten, dass alle dezentralen Datenbanken konsistent sind (Konsensmechanismen).
- Man unterscheidet zwischen permissionless und permissioned sowie zwischen öffentlichen und privaten Blockchains.
- Mit Blockchains lässt sich Eigentum digital abbilden: Asset-baked Token stellen digitale Repräsentationen einer Sache oder eines Rechts dar (z.B. Aktien oder andere Wirtschaftsgüter)
- Wirtschaftsbeziehungen lassen sich auf Blockchains abbilden
- Blockchains nutzen eine Reihe von Technologien:
    - Als Netzwerkprotokoll werden Standardprotokolle des Internets (TCP/IP) genutzt
    - Darauf aufbauend nutzen Blockchains in Ihrer Logik Peer to Peer (P2P) Protokolle zur Erzeugung eines dezentralen Kommunikationsnetzwerks, in dem Datenpakete zwischen den Teilnehmern ohne die Präsenz eines zentralen Kontenpunkts übertragen werden können
    - Durch die Nutzung von Konsensmechanismen wird gewährleistet, dass alle Teilnehmer der dezentralen Datenbank über einen identischen Datenbestand verfügen
- Smart Contracts basieren auf der Blockchain Technologie und werden dazu genutzt, die Logik von realen Verträgen technisch/programmatisch abzubilden. Sie bestehen aus einer Menge von formalen Regeln (Vertragsbedingungen), die im Programmcode abgebildet sind. Eingehende Daten werden kontinuierlich auf Einhaltung dieser Regeln überprüft. Entsprechend dem Ergebnis können automatisiert vorher vertraglich festgelegte Aktionen angestoßen werden. Beispielsweise würde sich so ein einfaches Währungssystem durch 20 Code Zeilen abbilden lassen.
- Smart Regulierung: Öffentliche Verwaltungsaufgaben können mit Hilfe der Blockchain Technologie digital abgebildet werden.
- **Derzeit ist noch ein Mangel an rechtlichen Rahmenbedingungen und Regulierungen in Deutschland vorhanden. Wünschenswert sind:**
    - Anerkennung Blockchain-basierter Zeitstempel als Strengbeweis in der ZPO

  - Digitale Signaturen wie in der Blockchain Technologie verwendet als anerkannter Authentizitäts- und Identitätsnachweis
  - Gesetzliche Spezifikation eines Blockchain-Protokolls das Anforderungen an (qualifizierten) Vertrauensdienst genügt

Vortrag Dr. Alexander Duisberg: Risikomanagement und Haftung für Sicherheitspannen nach DSGVO und ITSiG

- Der Schritt vom Bundesdatenschutzgesetz zur DSGVO entspricht im Wesentlichen einem inkrementellen Schritt.
- Die in der DSGVO festgelegten und im Vergleich zum Bundesdatenschutzgesetz erheblich strengeren Sanktionen sollen die Einhaltung der im Rahmen der DSGVO festgelegten Richtlinien gewährleisten.
- Firmen werden dazu gezwungen, umfangreiche Prozesse zur Einhaltung der DSGVO Compliance zu etablieren.
- Vorstands- und GF-Haftung (§ 91 Abs. 2 AktG)
  - "Vorstand hat .. insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."
  - Frühwarnsysteme und Cyber-Resilienz unmittelbar verknüpft!
  - Nachweis des Überwachungssystems
- IT SiG (2015) betrifft KRITIS Betreiber sowie deren Zulieferer
- Wann müssen Sicherheitspannen kommuniziert werden:
  - Innerhalb von 72h (auch an Wochenenden)
  - Damit Firmen diese Frist auch einhalten können, müssen diese vorher entsprechende Prozesse definieren und etablieren (Aufgabe des Top-Managements)
  - Haftung bei Versäumnissen (2% Bußgeldrahmen)
  - Meldung an Aufsichtsbehörde
  - Meldung an Betroffene (bei hohem Risiko)
- Mitteilung von IT-Störungen: Unterscheidung von gewöhnlichen und außergewöhnlichen IT Störungen. Bei außergewöhnlichen IT-Störungen und wenn ein Ausfall oder eine Beeinträchtigung eingetreten ist, muss eine Meldung erfolgen.
- **IT Sicherheit ist nicht zuletzt durch die neue DSGVO ein Management Thema. Die im Rahmen der DSGVO festgelegten Sanktionen sind deutlich griffiger im Vergleich zum Bundesdatenschutzgesetz.**

Konklusion

- In Deutschland besteht die Dringlichkeit nach einer sachlichen, öffentlichen Debatte über die Ausführung von Hackbacks. In den USA ist der Diskurs weiter vorangeschritten.
- Ein gesondertes „Digitales Recht“ respektive Cyber-Sonderrecht ist sowohl national als auch international nicht erforderlich.
- Der Themenkomplex „Regulierung im Cyberraum“ erfordert eine noch ausdifferenzierte Debatte.

- Durch Blockchains können in Zukunft zahlreiche Verwaltungsaufgaben digitalisiert werden. Rechtlichen Rahmenbedingungen und Regulierungen hinsichtlich der Nutzung von Blockchains müssen in Deutschland jedoch erst noch geschaffen werden.
- IT Sicherheit ist nicht zuletzt durch strengere Sanktionen bei Verstoß gegen die DSGVO zur Aufgabe des Top-Managements geworden. Die strengeren Sanktionen machen die DSGVO im Vergleich zu ihren nationalen Vorgängern griffig.