Recht & Regulierung im Cyber- und Informationsraum

- Workshop IV, CODE Jahrestagung 2018 -

Moderation: Oberst i.G. DR. JAN BYOK LL.M., 11. Juli 2018

Pressespiegel

20 Digitale Revolution — Handelsblatt

Künstliche Intelligenz in der Rüstung

Tödliche Algorithmen

Kampfroboter beeindrucken und verschrecken die Öffentlichkeit. Doch künstliche Intelligenz wird künftige Kriege auch auf subtilere Weise verändern.

Thomas Hanke, Donata Riedel
Paris, Berlin

Terminator III: Frühe Vision intelligenter Waffensysteme.

Künstliche Intelligenz

Von Drohnen und Walen

Wale sind schwer zu ergründende Wesen. Die Meeresriesen tauchen nur kurz an die Wasseroberfläche - daher ist es eine Herausforderung für Forscher, sie zu untersuchen. Intel hat eine Lösung entwickelt, um das zu erleichtern: Drohnen kreisen über den Tieren, um ihre

SPIEGEL ONLINE — NETZWELT

Pläne zum digitalen Gegenschlag

Wenn der Staat zum Hacker wird

Was tut ein Rechtsstaat, wenn ihm sensible Daten gestohlen wurden? Darf er sich in fremde Server hacken, um Informationen aus der Ferne zu löschen? Die Behörden stehen vor einem Dilemma.

Von Jörg Diehl und Fabian Reinbold

Bundeswehr

Soldaten gegen Cyberkrieger

Deutschland behält sich vor, im Ernstfall sogar mit einem militärischen Gegenschlag auf einen staatlich gesteuerten Hackerangriff zu reagieren.

Frankfurter Allgemeine — Inland

BUNDESWEHR SETZT AUF SOFTWARE

Die Krisen von Morgen erkennen

VON BJÖRN MÜLLER - AKTUALISIERT AM 04.07.2018 - 22:34

Die Bundeswehr lässt eine Software entwickeln, um sich besser für zukünftige Krisen wappnen zu können. Dabei dient die amerikanische Armee als Vorbild – doch das Vorhaben hat seine Tücken.

ZEIT ONLINE

Cyber-Kommando der Bundeswehr

Freiwillige und Nerds – was ist das für eine Truppe?

Das neue Cyber-Kommando der Bundeswehr

Militärs mit Computermaus und Laptop

Am 1. April nimmt das neue Bundeswehr-Kommando "Cyber- und Informationsraum" (CIR) in Bonn offiziell den Dienst auf. Damit wird in Deutschland vollzogen, was in anderen Staaten und Realität ist: Cyber-Krieger werden neben Heer, Luft eigenen Waffengattung.

Von Tom Schimmeck

Verliert die Bundeswehr den Cyberkrieg, bevor er begonnen hat?

- Offen -

1. Definition

Der Informationsraum ist der Raum, in dem Informationen generiert, verarbeitet, verbreitet, diskutiert und gespeichert werden. Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann. (S. 36, Weißbuch 2016)

2. (Völker-)rechtliche Dimension

- kein gesondertes Abkommen zur Ächtung von Cyberwirkmitteln durch BReg angestrebt (S. 5 f., BT Drucksache 19/2307)
- Verbot unterschiedslos wirkender Mittel (insbes. Art. 51 Nr. 1 Genf I), wenn nicht verhältnismäßig (Art. 51 Nr. 5 lit. b und Art. 57 Nr. 2 lit. a iii Genf I)
- cyberinhärente Attributionsproblematik (S. 38, Weißbuch 2016)
- Cyberangriff ggf. "bewaffneter Angriff" i.S.d. Art. 51 VN-Charta/Art. 5 NordatlantikV (z.B. Stuxnet als wirkungsgleicher Angriff auf KRITIS)
- 154 Regeln (“black letter rules”) des NATO-Tallinn Manuals 2.0 als Orientierung (ius ad bellum)

3. Politische Dimension (Weißbuch, Koalitionsvertrag)

- ganzheitlicher Ansatz (Nationaler Pakt Cybersicherheit, BSI)
- „Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien“ (ADIC)
- IT-Sicherheitsfonds zum Schutz sicherheitsrelevanter Schlüsseltechnologien
- Europäische Verteidigungsunion (PESCO, Verteidigungsfonds (EVF))

4. Militärische Dimension

- CIR als strategischer Handlungsraum (kriminelle, terroristische, nachrichtendienstliche, militärische Akteure)
- „Advanced Persistent Threats“, DDoS-Angriffe, Ransomware etc. ("Krieg des armen Mannes")
- Resilienzbildung/Härtung wegen zunehmender Anfälligkeit (u.a. Digitalisierung der Landstreitkräfte (Dila),OODA-Loop, UAV)
- Aufwuchs offensiver Fähigkeiten (Zentrum für Cyberoperationen (ZCO)) mit 100 Dienstposten (Aufstellung: 05.04.2018)

Podium

Dr. Sven Herpig

- Leiter Transatlantisches Cyberforum, Stiftung Neue Verantwortung e.V.
- zuvor: IT-Stab Auswärtiges Amt, BSI
- Beratung politischer Institutionen zum Thema Cybersicherheit

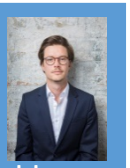
Stefan Sohm

- Referatsleiter BMVg: Völkerrecht und Rechtsgrundlagen der Auslandseinsätze der Bundeswehr
- Vorsitz: Deutsche Gesellschaft für Wehrrecht u. Humanitäres Völkerrecht

Steve Ritter

- gelernter Bankkaufmann und Jurist
- seit 2011 beim BSI tätig und hat dort u.a. das IT-Sicherheitsgesetz und die NIS-Richtlinie juristisch begleitet

Florian Glatz



- Rechtsanwalt, Software Entwickler, Unternehmer im Bereich Blockchain
- Mitgründer des Legal Tech Centers und Präsident des Blockchain Bundesverbands

Dr. Alexander Duisberg

- Partner bei Bird & Bird LLP
- tätig im Bereich Datenschutz, digitale Transformationsprojekte und komplexe technologische Transaktionen