Recherche zum Thema Cyberwar
U. Kastens, 24.09.2019

A.:
Florian Flögel: **Cyberwar – Systematisierung und Kategorisierung einer „neuen“ Bedrohung, Kieler Analysen zur Sicherheitspolitik Nr. 35 Januar 2014**
https://www.ispk.uni-kiel.de/de/publikationen/upload-working-paper/KASZ%2035.pdf

1. Einleitung und Definitionen

Cyber: Wird als Präfix für alle Begriffe genutzt, die sich auf automatisierte und informations- verarbeitende Prozesse beziehen.

Cyberspace: Setzt sich aus allen elektronischen Geräten und Medien zusammen, die mit der Erschaffung, Speicherung, Übertragung und Verarbeitung von digitalen Daten zu tun haben.

Informationsbasierte Gesellschaften: Die Industriegesellschaften der entwickelten Staaten verwandeln sich zunehmend in informationsbasierte Gesellschaften (*Third-Wave-Societies)*. Diese technologisch hochentwickelten Gesellschaften sind politisch, wirtschaftlich und gesellschaftlich stark vom Funktionieren ihrer vernetzten Infrastruktur abhängig.

Kritische Infrastruktur: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

Cyberkriminalität: Die *Cybercrime Convention* des Europarats ...
Das Bundeskriminalamt definiert Cyberkriminalität in einem Satz: „Der Begriff *Cybercrime* umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden.“

Cyberterrorismus: Zurzeit lassen sich keine Fälle feststellen, die sich eindeutig als Cyberterrorismus einstufen lassen. Das Konzept wird aber regelmäßig in Literatur und Presse als Bedrohung kommuniziert.

2. Das Phänomen „Cyberkrieg“

2.1 Cyberangriffsformen

Angriffswerkzeug für das Zielcomputersystem,
konventionelle Hackertools, Zugang zu fremden Computer oder Netzwerk verschaffen, Sicherheitslücken nutzen, auf dem Zielgerät Schadsoftware installieren, Fallen stellen,
Computerwurm infiziert möglichst viele Rechner, kopiert sich selbst und verschickt sich weiter.

DoS- oder DDoS-Attacke: Eine *(Distributed) Denial of Service* Attacke macht sich die begrenzten Kapazitäten eines Webseitenbetreibers zunutze. Flut an Aufrufen überlastet die Kapazitäten der Server und führt zu einem temporären Ausfall des Webdienstes; Einsatz von Bot-Netzen (Tausende gekaperte Privat-Computer).

Beispiel für Angriff auf komplexe Industrieanlage: Wurm Stuxnet (2010), angesetzt auf iranische Atomanlage in Natanz; wirksam gegen allgemeiner eingestztes System der Firma Siemens zur Überwachung und Steuerung von Industrieanlagen.

DoS-Angriff auf Estland 2007, gegen estnische Parlament,
den Staatspräsidenten sowie diverse Ministerien, Banken und Medien.

2.2 Cybersabotage

Als Sabotageakt wird nach allgemeinem Verständnis ein gezielter Angriff bezeichnet, der einen maschinellen Prozess durch eine schädigende Einwirkung unterbricht bzw. eine ganze Einrichtung durch Beschädigung (gar Zerstörung) einzelner Komponenten davon abhält ihren Aufgaben im gewünschten Maße nach-zukommen, um ein politisches oder militärisches Ziel zu erreichen.

Erstens verfügt das Militär der ent- wickelten Staaten über einen hohen Grad an integrierter z.T. unverzichtbarer IT und EDV, vor allem im Bereich Kommunikation, Koordination und Hightech-Waffensysteme. Dieses Zusammenspiel wird als *Network Centric Warfare* bezeichnet

Zweitens wäre kritische Infrastruktur ein attraktives Ziel für Sabotage, da eine Destabilisierung der Lage durch direkten Einfluss auf die zivile Bevölkerung im Konfliktfall den Vorteil zugunsten des Angreifers verschieben würde.

Ein dritter Bereich wäre die Sabotage von Schlüsselindustrien, wie beispielsweise die Ölförderung und Verarbeitung.

Der US- amerikanische Terrorismusexperte und ehem. Sonderberater für Cybersecurity unter Präsident George W. Bush, Richard Alan Clarke, bezieht dazu in seinem 2010 erschienen Werk *World Wide War* (Originaltitel: *Cyber War: The Next Threat to National Security*) deutlich Stellung. In Clarkes Ausführungen ist der Cyber-war Realität. Es geht um die Vorherrschaft im Cyberspace. Daher begrüßt er die offensive Haltung der USA, bemängelt allerdings die Maßnahmen zum Schutz gegenüber feindlichen Cyberagriffen.

2.3 Cyberspionage

Die Überwachung jeglicher Telekommunikation, *Signal Intelligence* (SIGINT), ist zur wichtigsten Aufgabe von Geheimdiensten geworden. Cyberspionage nimmt in Staaten, wie die USA, Russland und China, einen großen Teil der finanziellen Ressourcen und Cyberkapazitäten ein.

Technisch betrachtet, bedienen sich Cyberspione ähnlichen Werkzeugen, die auch bei der Cybersabotage benutzt werden (Trojaner, Backdoors, Rootkits etc.).

Die Angreifer verschafften sich [2003] Zugang zu Netzwerken von US-Einrichtungen wie dem *State Department*, dem *Department of Homeland Security*, dem Pentagon und dem Rüstungsunternehmen *Lockheed Martin*.

Ein weiterer wichtiger Teilbereich ist die Industriespionage durch das Ausspähen der IT von Unternehmen.
Bei *Operation Aurora* waren neben IT- Unternehmen wie *Adobe*, *Google*, *Yahoo* und *Symantec*, auch Rüstungskonzerne und die Finanzbranche betroffen, z.B. *Northrop Grumman* und *Morgan Stanley*.58 *Shady RAT* war zwischen den Jahren 2006 und 2008 aktiv und spähte über 70 internationale Unterneh- men, Regierungen und NGOs weltweit aus.

2.4 Cybersubversion

Im politischen Kontext ist die Untergrabung der bestehenden politischen Ordnung oder der Machtinhaber unter Zuhilfenahme subversiver Mittel gemeint. Diese subversiven Mittel schwanken in ihrer Intensität zwischen Terrorismus, Propaganda, Befehlsverweigerung und sozialem Ungehorsam.

Es soll im Folgenden ausschließlich um Subversion im direkten Zusammenhang mit dem Internet gehen, dabei sind Bewegungen wie *Occupy Wall Street*, *Anonymous* oder der „arabische Frühling“ gemeint.

2.5 Das Attributionsproblem

Den Urheber einer Cyberattacke zu identifizieren, ist aus technischen, justiziellen und politischen Gründen nahezu unmöglich. Physische Spuren wie Fingerabdrücke werden i.d.R. nicht hinterlassen. Daher gehen IT-Forensiker den Datenspuren nach, z.B. durch Ermittlung der IP-Adresse oder dem Inhalt einer Schadsoftware

Diese Anonymität durch die Non-Attribution ist für Staaten Fluch und Segen zugleich – auch für die Staaten die offensive Cyberstrategien verfolgen. Es ermöglicht ihnen verdeckte Operationen mit weniger menschlichem Einsatz (*boots on the ground*) durchzuführen, andererseits fallen essentielle strategische Prinzipien wie die Abschreckung weg.

2.6 Rechtliche und konzeptionelle Rahmenbedingungen

Es existiert weder eine Art von *Internet Governance* noch verbindliche völkerrechtli- che Regelungen für virtuelle zwischenstaatliche Auseinandersetzungen.

[U]nter Krieg [wird] eine mit Waffengewalt geführte Auseinandersetzung zwischen zwei Gruppen verstanden, von denen wenigstens eine als reguläre Armee oder bewaffnete Streitkraft auftreten muß.

(D)DoS Attacken können in ihrer Wirkungsweise mit „virtuellen Sitzblockaden“ verglichen werden.
Durch die indirekte physische Wirkung erfüllt *Stuxnet* tendenziell die notwendige Bedingung der Gewaltausübung, kann also durchaus als waffenähnlich eingestuft werden,

Dennoch kann auch *Stuxnet* nicht als kriegerischer Akt ge- wertet werden, da durch die Non-Attribution keine Kombattanten auszumachen sind,
...

5 Konklusion

An den vorgestellten Kategorien wird deutlich, dass es sich beim Phänomen Cyberwar um kein Novum handelt, auch die Bezeichnung als „fünfte Domäne des Krieges“ ist irreführend und nicht zutreffend. Cyber-Sabotage, Spionage und Subversion eröffnet keine neuartigen *Theatres of War*, denn im Kern greifen Geheimdienste und Militär nur die erweiterten technologischen Möglichkeiten der sich ständig weiterentwickelnden Telekommunikationsmittel und Technologien auf.

Die Analyse der verschiedenen Cyberangriffsformen zeigt, dass die meisten Cyberangriffe entweder gar kein oder nur indirektes Gewaltpotential aufweisen, somit nur sehr bedingt als Cyberwaffen bezeichnet werden sollten.

Der Cyberwar im engeren Sinne bleibt im Jahr 2014 folglich eindeutig ein Hype, der allerdings Großmächten wie den USA und China dazu dient machtpolitische Räume und Offensivfähigkeiten auszubauen.

B.:
Thomas Rid: Mythos Cyberwar. Über digitale Spionage, Sabotage und andere Gefahren. Edition Körber, 2018, ISBN: 978-3-89684-260-2

Aus der Buchbeschreibung:
„Der Politikwissenschaftler Thomas Rid ist sich sicher: Der Cyberkrieg findet nicht statt. Die bisher dokumentierten Cyberattacken lassen sich nicht als Krieg bezeichnen, denn es fehlt die zielgerichtete Gewalt gegen Menschen, die brutale Zerstörung, die untrennbar mit dem Gedanken des Krieges verbunden ist.

Thomas Rid macht auch klar, dass aus dem Cyberspace durchaus reale Gefahren wie Spionage, Sabotage und Subversion drohen. Detailliert und kenntnisreich erzählt er von Spionageangriffen, von Sabotageakten und von Versuchen, mithilfe der Informationstechnologie Regierungen zu destabilisieren und Umstürze einzuleiten. Kriegerische Handlungen sind dies jedoch für Rid nicht, und dabei geht es um weit mehr als um eine rhetorische Abrüstung: Wir müssen begreifen, wer vom Mythos Cyberwar profitiert. Und wir müssen definieren, welchen Gefahren wir wirklich ausgesetzt sind, um den Sicherheitsanforderungen gut vorbereitet begegnen zu können.“

Trotz des provokanten Titels passt das zu der Konklusion von Flögel, s.o.

Die FAZ diskutiert Rids Buch:
Der neue Krieg: Die fünfte Dimension, Christian Hartmann, 22.01.2019
https://www.faz.net/aktuell/politik/politische-buecher/cyberkrieg-wenn-computer-zum-krieg-fuehren-einladen-15988424.html#void

C.:
Cyber- und Informationsraum der Bundeswehr
https://cir.bundeswehr.de/portal/a/cir/start/kdocir/ueberuns
gesehen in der Version vom 5.8.2019

Das Kommando Cyber- und Informationsraum wurde am 5. April 2017 offiziell durch die Verteidigungsministerin, Ursula von der Leyen in Dienst gestellt.

Rund 260 Angehörigen in der Startaufstellung des Kommando Cyber- und Informationsraum stellten anfänglich die truppendienstliche Führung sicher.

April 2018 wuchs das Kommando Cyber- und Informationsraum um weitere rund 140 Dienstposten.

Dem Kommando Cyber- und Informationsraum (KdoCIR) sind das Kommando Strategische Aufklärung, das Kommando Informationstechnik der Bundeswehr und das Zentrum für Geoinformationswesen der Bundeswehr direkt unterstellt.
Rund 14.500 Dienstposten gehören zum Organisationsbereich Cyber- und Informationsraum. Ähnlich wie Heer, Luftwaffe und Marine für die Dimensionen Land, Luft und See zuständig sind, sind diese ganzheitlich für die Dimension Cyber- und Informationsraum verantwortlich. Zum einen stellen die Angehörigen den Einsatz, Schutz und Betrieb des IT-Systems der Bundeswehr, sowohl im Inland als auch im Einsatz sicher. Zum anderen stärken sie Fähigkeiten zur Aufklärung und Wirkung im Cyber- und Informationsraum und entwickeln diese weiter.

Generalleutnant Ludwig Leinhos ist der erste Inspekteur Cyber- und Informationsraum.

D.:
BigBrotherAward 2017
https://bigbrotherawards.de/2017

Bundeswehr und Bundesministerin für Verteidigung erhalten den BigBrotherAward 2017 in der Kategorie Behörden für die massive digitale Aufrüstung der Bundeswehr mit dem neuen „Kommando Cyber- und Informationsraum“ (KdoCIR). Diese digitale Kampftruppe mit (geplant) fast 14.000 Dienstkräften wird die Bundeswehr fit machen für den Cyberkrieg - auch für militärische Cyberangriffe auf IT-Systeme und kritische Infrastrukturen anderer Staaten. Mit dieser Militarisierung des Internets beteiligt sich die Bundesrepublik am globalen Cyber-Wettrüsten – ohne Parlamentsbeteiligung, ohne demokratische Kontrolle und ohne rechtliche Grundlage.

E.:
Deutschland will zurückhacken, Kai Biermann, Zeit Online, 12.07.2019
https://www.zeit.de/digital/internet/2019-07/hackback-cyberwar-datensicherheit-digitaler-angriff-bundesregierung

Innenministerium die Abteilung CI. Die Abkürzung steht für Cyber- und Informationssicherheit.
Bundeswehr, Nachrichtendienste und Polizei sollen künftig auch im Netz zurückschlagen dürfen. Entsprechende Dienststellen werden längst aufgebaut.

Deutsche Behörden sollen in fremde Rechner im In- und Ausland eindringen dürfen, sollen sie ausspähen, sie manipulieren, sie abschalten und darauf befindliche Daten löschen.

Mit der **Zentralen Stelle für Informationstechnik im Sicherheitsbereich** (Zitis) wurde beim Innenministerium eine Behörde aufgebaut, die die entsprechenden Werkzeuge für Hackbacks erforschen und Verschlüsselung brechen soll.

Der **Cyber- und Informationsraum** (CIR) ist ein eigener Organisationsbereich der Bundeswehr, der schon einsatzfähig ist. Er könnte neben Heer, Marine und Luftwaffe eine eigene Teilstreitkraft werden.

Es fehlen nur noch die gesetzlichen Grundlagen, damit sie alle auch zurückschlagen dürfen. An denen arbeitet Könens Abteilung im Innenministerium seit mindestens einem Jahr. Die meisten entsprechenden Paragrafen stehen bislang im Entwurf für ein sogenanntes Zweites IT-Sicherheitsgesetz
Geleakter Entwurf (03.04.2019):
https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll

F.:
cyberpeace
Eine Kampagne des
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
https://cyberpeace.fiff.de/Kampagne/Home
seit 2016

Flyer:
https://cyberpeace.fiff.de/Uploads/Uploads/Cyberpeace-Flyer_Online.pdf

YouTube Video zum Cyberwar:
https://www.youtube.com/watch?v=St955HBD-7k&feature=youtu.be

Mit seinem am 1. Oktober [2017] gestarteten Appell gegen Cyberwaffen will das FIfF die Bundesregierung und die Abgeordneten des Deutschen Bundestages auffordern, zum Schutz der Zivilgesellschaft zu handeln und sich dafür einzusetzen,

- **dass Deutschland auf eine offensive Cyberstrategie verzichtet,**
- **dass sich Deutschland verpflichtet, keine Cyberwaffen zu entwickeln und zu verwenden,**
- **dass internationale Abkommen zu einem weltweiten Bann von Cyberwaffen angestrebt werden.**