**Zeitschrift:** ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

**Herausgeber:** Schweizerische Offiziersgesellschaft

**Band:** 183 (2017)

**Heft:** 4

**Artikel:** Cyberwar und Cyber-Terrorismus : Bedrohungen in Gegenwart und Zukunft

**Autor:** Goerts, Stefan

**DOI:** https://doi.org/10.5169/seals-681595

# Cyberwar und Cyber-Terrorismus: Bedrohungen in Gegenwart und Zukunft

**Cyberwar und Cyber-Terrorismus gehören wie der internationale Terrorismus zu den Herausforderungen der hybriden Kriegführung des 21. Jahrhunderts. Schon heute sind Operationen im Cyber- und Informationsraum zunehmend Bestandteil kriegerischer Auseinandersetzungen.**

Stefan Goertz

Diese Tendenz wird sich zukünftig noch erheblich verstärken. Der Cyber- und Informationsraum[1] hat sich zu einem internationalen und strategischen Handlungsraum entwickelt, der so gut wie grenzenlos und von existentieller Bedeutung für alle ist.[2] Cyberwar und Cyber-Terrorismus sind eine eigene Dimension im Kontext der hybriden Kriegführung, weil sie weder nationale noch institutionell-hierarchische Strukturen kennen, wodurch die Grenzen zwischen Krieg und Frieden, Offensive und Defensive, innerer und äusserer Sicherheit sowie kriminell und politisch motivierten Angriffen verschwinden.

## Cyber-Angriffe als taktische Mittel von Cyberwar und Cyber-Terrorismus

Staat, Wirtschaft und Gesellschaft sind in der vernetzten, digitalisierten Welt des 21. Jahrhunderts verwundbarer für Angriffe im Cyber- und Informationsraum geworden. In den letzten Jahren haben sich staatliche und nicht-staatliche Akteure – im Rahmen der hybriden Kriegführung – diese digitale Verwundbarkeit zu Nutze gemacht. Die Anonymität von Angriffen (Attributionsproblematik) und die Möglichkeiten zur asymmetrischen Schadenswirkung machen Cyber-Angriffe zu einem taktisch äusserst effektiven Mittel, um Ziele unterhalb der Schwelle eines militärischen Angriffs zu erreichen.[3] Deswegen kategorisiert und behandelt die NATO den Cyber- und Informationsraum als einen eigenen Operationsraum.

Cyber-Angriffe sind Straftaten, die eine Einwirkung auf informationstechnische Systeme im oder durch den Cyber-Raum – mit dem Ziel, die IT-Sicherheit zu beeinträchtigen – beabsichtigen.[4] Dabei können Cyber-Angriffe sowohl eine politische, z.B. terroristische, eine nachrichtendienstliche, aber auch eine wirtschaftliche Motivation haben. Cyber-Angriffe umfassen auch Cyber-Spionage und Cyber-Informationsmanipulation.

### Cyber-Sicherheitsstrategie für Deutschland

«Die Folgen von Cyber-Angriffen beschränken sich nicht auf den Cyber-Raum. Erfolgreiche Angriffe können gesellschaftliche, wirtschaftliche, politische und auch persönliche Schäden verursachen. Angriffe auf staatliche Institutionen mit dem Ziel der Ausspähung oder Sabotage können die Funktionsfähigkeit von Verwaltung, Streitkräften und Sicherheitsbehörden erheblich beeinträchtigen und damit Auswirkungen auf die öffentliche Sicherheit und Ordnung haben.»
(Bundesministerium des Innern, 09.11.16, Seite 39)

U.S.-Heeressoldaten bei einer Cyber-Ausbildung im Cyber Center of Excellence der U.S. Army, Fort Gordon in Augusta/Georgia, USA. Bild: Wikicommon

## Definition von Cyberwar und Cyber-Terrorismus

Bei Cyberwar bzw. Cyber-Krieg handelt es sich um die Nutzung des Internets und von Computern zur staatlichen Kriegführung bzw. zur Kriegführung nicht-staatlicher Akteure gegen Staaten, häufig im Sinne von Cyber-Angriffen oder Cyber-Spionage. Als einer der ersten Cyber-Kriege wird der Kosovokonflikt gesehen, in dem die beteiligten Akteure Informations- und Kommunikationstechnologien als taktische Kampfmittel einsetzten. So wurde beispielsweise das jugoslawische Telefonnetz gestört und Konten des serbischen Präsidenten Milosevic gehackt. Im Gegenzug griffen serbische Hacker unter anderem einen NATO-Server an.

Problematischerweise existiert innerhalb der Europäischen Union immer noch keine einheitliche Definition des Begriffes Cyber-

Terrorismus. Cyber-Terrorismus kann als «der Gebrauch von Cyber-Kapazitäten, um ermächtigende, störende oder zerstörende militante Operationen durchzuführen und Angst mittels Gewalt oder Gewaltandrohung zu instrumentalisieren, um einen politischen Wandel zu verfolgen» definiert werden.[5] In den letzten Monaten hat sich nicht nur die Quantität von Cyber-Angriffen, sondern vor allem die Qualität ganz evident gewandelt. So stellt die Entwicklung von einfachen Viren hin zu komplexen, schwer erkennbaren Attacken (Advanced Persistant Threats, APT) einen Qualitätssprung dar. Durchschnittlich werden über 200 Tage benötigt, um einen APT zu erkennen.

Als taktisches Mittel von Cyber-Terrorismus können sich Cyber-Angriffe z.B. gegen IT-gesteuerte kritische Infrastrukturen – wie die Elektrizitätsversorgung (z.B. Kernkraftwerke), die Trinkwasserversorgung, den Bahnverkehr, Verkehrsleitsysteme und die Flugsicherung (mit dem Ziel, Kollisionen herbeizuführen) – richten. Diese Anschlagsziele sind nach terroristischer Logik daher effektiv, weil hohe Opferzahlen und Schäden sehr wahrscheinlich sind. Zusätzlich ist es taktisch denkbar, dass solche Angriffe mit «konventionellen» terroristischen Anschlägen gekoppelt werden.[6]

## Aktuelle Beispiele von Cyber-Angriffen

Cyber-Angriffe auf Staaten und ihre Behörden, ihre kritischen Infrastrukturen, Wirtschaft und Wissenschaft sind schon lange Realität. Weltweit bekannte Beispiele sind z.B. die Operation «Shady Rat» (etwa «zwielichtige Ratte» oder «verborgener Fernzugriff»), in der von ca. 2006 bis 2011 weltweit mindestens 72 Unternehmen, Organisationen und Regierungen systematisch ausgespäht wurden, darunter Behörden der USA, Kanadas und der Vereinten Nationen, wobei sich in 49 Fällen die Angriffe gegen amerikanische Ziele der Elektronik- und Rüstungsindustrie wendeten. Die – wahrscheinlich chinesischen – Cyber-Angreifer bewegten sich zwischen einem und 28 Monaten in den gehackten Systemen.[7] Am 23.12.2015 kam es in der Ukraine zum weltweit ersten durch einen Cyber-Angriff verursachten Blackout auf die Stromversorgung der West-Ukraine. Von den mehrstündigen Blackouts waren insgesamt drei Stromversorger und ca. 225 000 Haushalte betroffen. Für den Cyber-Angriff wurde Russland verantwortlich gemacht.[8] Weitere bekannt gewordene Cyber-Angriffe sind der «STUXNET-Angriff» auf ein iranisches Atomprogramm im Jahr 2010, der «OPM-Breach» 2014 in den USA mit einem Datenabfluss von ca. 18 Millionen personenbezogener Daten von US-Staatsbediensteten und der Cyber-Angriff auf den Deutschen Bundestag 2015, bei dem über vier Tage lang das Parlakom-Netzwerk komplett abgeschaltet werden musste.[9] Beim Cyber-Angriff auf das Atomkraftwerk in Grundremmingen soll das Bundesamt für Informationstechnik verhindert haben, dass der Angriff die Steuerung des Atomkraftwerkes erreichte.[10] Beim Ende 2014 vermutlich von russischen Hackern durchgeführten Angriff auf Computer des Schweizer Rüstungskonzerns RUAG sollen Daten über geheime Projekte des Schweizer Verteidigungsdepartements – darunter Informationen zur AAD 10 – gestohlen worden sein.[11]

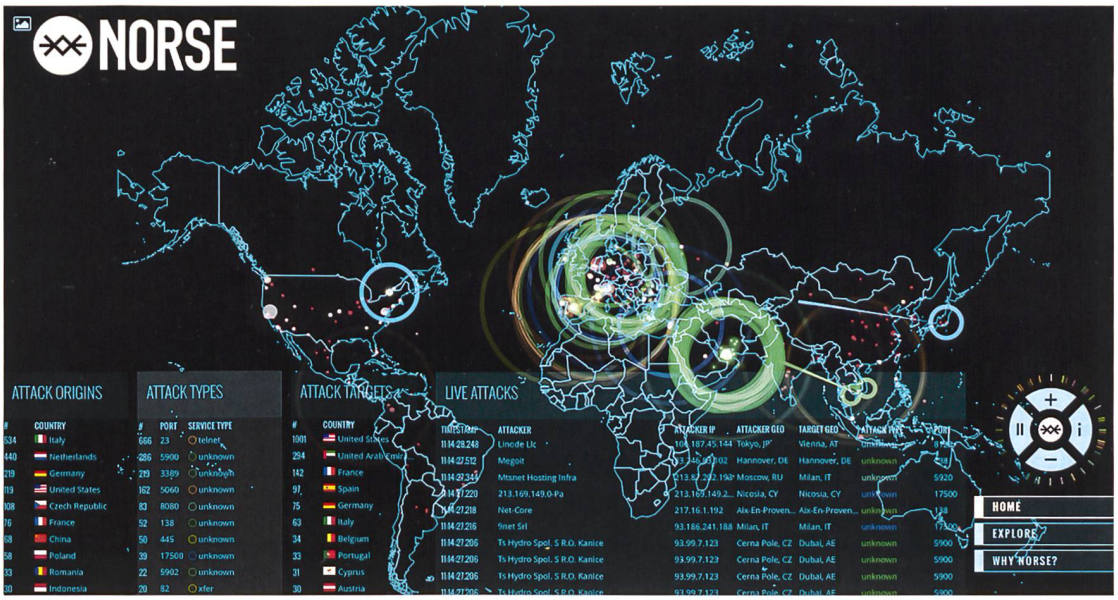
### Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) (SN002)

Der Bundesrat hat am 27. Juni 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» gutgeheissen. Mit der Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, welchen sie täglich ausgesetzt sind.

Als wesentlich für die Reduktion von Cyber-Risiken bezeichnet die Strategie das Handeln in Eigenverantwortung und die nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden sowie die Kooperation mit dem Ausland. Diesen Handlungsbedarf deckt die Strategie mit 16 Massnahmen ab, die bis 2017 umzusetzen sind.

**«Cyberwar und Cyber-Terrorismus sind eine eigene Dimension im Kontext der hybriden Kriegführung.»**

Die technischen Mittel von Cyber-Angriffen sind sehr kostengünstig, effektiv und erzielen durch DDoS-Attacken, APTs, backdoors, hacktivists und Cyber-Armeen eine asymmetrische Wirkung, um Ziele unterhalb der Schwelle eines militärischen Angriffs durchzusetzen. So sind Cyber-Angriffe fester Bestandteil konventioneller Operationen von Streitkräften und/oder Nachrichtendiensten geworden, was in der




**Hackerangriffe live.**
Bild: Screenshot «map.norsecorp.com»

Georgien-Krise 2008 und anhand der hybriden Kriegführung Russlands in der Ukraine beobachtet werden kann. Dieses Beispiel der Strategie Russlands in der Ukraine verdeutlicht die Wiedergeburt klassischer Machtpolitik, in der militärische Mittel zum Erreichen nationalstaatlicher Interessen angewendet werden und dadurch das Risiko gewaltsamer zwischenstaatlicher Konflikte, auch in Europa und angrenzenden Staaten, steigt. So schaltete die mutmasslich in russischem Auftrag handelnde Hacker-Gruppe CyberBerkut anlässlich des Besuches des ukrainischen Regierungschefs in Berlin am 7.1.2015 die Internetseiten von Bundeskanzleramt und Bundestag aus und begründete dies damit, dass «die Ukraine mit deutschem Geld das Töten fortsetzen wolle».[12] Hier wenden sowohl staatliche als auch nichtstaatliche Akteure Methoden hybrider Kriegführung zur subversiven Unterminierung eines anderen Staates an.[13]

## Analyse

Durch Cyber-Angriffe und Informationsoperationen (Propaganda), Wirtschafts- und Rüstungsspionage können alle Bereiche des gesellschaftlichen Lebens der besonders anfälligen, offenen, pluralistischen Demokratien zum Ziel hybrider Strategien von Cyberwar und Cyber-Terrorismus werden.

Noch hybrider wird die Bedrohung, wenn reguläre, staatliche Akteure für verdeckte Operationen und Subversion nichtstaatliche Akteure – beispielsweise aus dem Bereich der Organisierten Kriminalität – beauftragen.

Die Wahrung der Cyber-Sicherheit und der Cyber-Verteidigung ist eine behördenübergreifende, gesamtstaatliche Aufgabe, wozu auch der gemeinsame Schutz der kritischen Infrastrukturen gehört. In keinem anderen Phänomenbereich sind die innere und äussere Sicherheit so verflochten und daher nur gesamtstaatlich zu gewährleisten. Cyberwar und Cyber-Terrorismus verwischen – ein Merkmal hybrider Kriegführung – die Grenzen zwischen Krieg und Frieden, was eine besondere Herausforderung an die Feststellung des Bündnisfalls nach Artikel 5 des NATO-Vertrags stellt.[14]

Darüber hinaus müssen die Streitkräfte westlicher, demokratischer Staaten ihre Fähigkeiten in den Bereichen Cyber, Informationstechnologie, militärisches Nachrichtenwesen, Geoinformationswesen und Kommunikation vernetzen, um auf die hybriden Bedrohungen Cyberwar und Cyber-Terrorismus zu reagieren. ■

1 Das deutsche Verteidigungsministerium definiert den Cyber- und Informationsraum wie folgt: «Im Zentrum der Dimension Cyber- und Informationsraum steht die Information. Diese wird im Informationsumfeld durch Menschen wahrgenommen und interpretiert. Der Cyber-Raum ist in das Informationsumfeld eingebettet und ermöglicht die (teil-) automatisierte Verarbeitung und Verbreitung von Informationen. Er umfasst über territoriale und strukturelle Grenzen hinweg alle über das Internet und sonstige Netze auf Datenebene vernetzte oder über Datenschnittstellen erreichbare Informationssysteme. Das elektromagnetische Spektrum ist ein wesentliches Trägermedium von Kommunikation im Cyber-Raum und Informationsumfeld.» Vgl. Bundesministerium Aufbaustab Cyber- und Informationsraum, April 2016, S. 46.
2 Vgl. Die Bundesregierung: Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr, 13.7.2016, S. 37.
3 Vgl. Bundesministerium der Verteidigung: Abschlussbericht Aufbaustab Cyber- und Informationsraum, April 2016, S. 1.
4 Vgl. die Definition des deutschen Verteidigungsministeriums: «Ein Cyber-Angriff im Verständnis des Geschäftsbereiches BMVg ist jede bewusste Handlung mit informationstechnischen Mitteln im, aus und auf den Cyber-Raum, die geeignet ist, die eigene Einsatz- und Operationsführung zu stören und zu beeinflussen oder die Verfügbarkeit, Integrität oder Vertraulichkeit eigener Informationen, IT sowie Waffen- und Wirksysteme zu gefährden.» Bundesministerium der Verteidigung 2015: Entwurf Umsetzungsstrategie Cyber-Verteidigung, S. 34.
5 Brickey, J.: Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace, 2012.
6 http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Terrorismus/cybersterrorismus_node.html; abgerufen am 29.11.2016.
7 http://www.ibtimes.co.uk/mcafee-operation-shady-rat-cyber-attack-hack-hackers-un-us-uk-192442; abgerufen am 30.11.2016.
8 Vgl. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf; abgerufen am 29.11.2016.
9 http://www.spiegel.de/netzwelt/web/bundestag-it-system-wird-nach-angriff-mehrere-tage-abgeschaltet-a-1041806.html; abgerufen am 28.11.2016.
10 Vgl. Behörden Spiegel Juli 2016, S. 37.
11 http://www.nzz.ch/nzzas/cyber-attacke-gegen-ruestungskonzern-ruag-russische-hacker-enttarnen-geheime-schweizer-elitetruppe-ld.18562; abgerufen am 30.11.2016.
12 http://www.n-tv.de/politik/Hacker-legen-Merkels-Webseite-lahm-article14271196.html; abgerufen am 10.12.2016.
13 Vgl. Die Bundesregierung 2016, S. 39.
14 Vgl. ebd, S. 62.

Major d.R.
Stefan Goertz
Dr. rer. pol., Dipl. Politologe
Hochschule des Bundes
Bundespolizei
23562 Lübeck

## Aus dem Bundeshaus

*Es geht um Entscheide von Bundesrat (BR) und Ständerat (SR) vor und in der Frühjahrssession 2017 sowie um parlamentarische Vorstösse und Antworten.*

*Der BR verabschiedete die «Armeebotschaft 2017» (17.027) mit 900 Mio. Franken für Rüstung (Nutzungsverlängerung F/A-18, Nachholbedarf Munition u.a.), 750 Mio. für Armeematerial (Ausrüstung, Erneuerung, Ausbildungsmunition u.a.) und 461 Mio. für Immobilien. Der SR beschloss Kenntnisnahme von «Die Sicherheitspolitik der Schweiz – Bericht des Bundesrates» vom 24. August 2016 (16.061) sowie «Verlängerung der Schweizer Beteiligung an der multinationalen Kosovo Force (KFOR)» vom 1.1.2018 bis zum 31.12.2010 (16.079; «Swisscoy») mit sinkenden Personalbeständen und Jahreskosten.*

*In der Interpellation «Schutz des Schweizer Luftraums durch die eigene Luftwaffe» (16.3936) wird gefährdete Sicherheit festgestellt, wenn ein Land sich nicht mit eigenen Kräften vor Eindringlingen schützen kann. Der BR wird gefragt, ob die Schweiz ihren Luftraum mit den vorhandenen Kampfflugzeugen selbst verteidigen könne. Welche Risiken bestehen bei einem Ersatz erst ab 2025? Der BR antwortet, dass der Luftraum in einer Krisenlage «für einige wenige Wochen» geschützt werden könnte. Die aktuelle und absehbare Bedrohungslage erfordere «keine beschleunigte oder vorgezogene Kampfflugzeugbeschaffung». In der Interpellation «Die Armee hat sich auf den denkbaren Fall vorzubereiten» (16.3998) wird der BR aufgrund eines Szenarios «Zusammenbruch jeglichen Schutzes der EU-Aussengrenze» gefragt, ob und wie die Armee entsprechende Einsätze mit ihren personellen und materiellen Mitteln bewältigen könne. Der BR erläutert die subsidiären militärischen Unterstützungsmöglichkeiten der zivilen Behörden in einer ausserordentlichen Lage und verweist auf seinen «Bericht [...] in Erfüllung des Postulats Malama 10.3045 vom 3. März 2010 – Innere Sicherheit. Klärung der Kompetenzen» vom 2. März 2012.*

*Oberst a D Heinrich L. Wirz*
*Militärpublizist/Bundeshaus-Journalist*
*3047 Bremgarten BE*