

leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/

3 <https://www.heise.de/newsticker/meldung/Bundeswehr-Weissbuch-Planspiele-fuer-den-Krieg-im-Cyberraum-3270870.html> m. w. N.

4 Die Bundeswehr sucht händigeren  
len und Universitäten rekrutiert sie  
Plakataktion der Bundeswehr: „Der  
Cyberraum verteidigt“, so lautet ein  
deutsche.de 2.4.2016.

5 <http://www.spiegel.de/netzwelt/netzpolitik/ist-ein-cyberkrieg-ein-krieg-a-841096.html>

6 Cordula Droege, Ist Cyberwar ein Krieg? In: Spiegel-online 2.7.2012.

7 Beispiel: der Computerwurm Stuxnet gegen das iranische Atomprogramm (2010) – gemäß Tallinn-Manual wäre dies als kriegerischer

Akt zu werten, also als völkerrechtswidriger Angriffskrieg. Nicht aber, wenn dieser Angriff von den USA gestartet wird: Dann gilt der digitale Übergriff mit steuerndem Sabotage-Schadprogramm nur noch als „Akt der vorbeugenden Selbstverteidigung“ gegen das iranische

Waffen produziert werden können.  
ist nicht eindeutig geklärt, es gibt  
dass der Wurm eine Entwicklung des  
Zusammenarbeit mit Israel ist.) <https://www.spiegel.de/netzwelt/netzpolitik/ist-ein-cyberkrieg-ein-krieg-a-841096.html> m. w. N.

8 Stattdessen werden aber IT-Sicherheitslücken, die für Cyberattacken nutzbar sind, als Angriffsoptionen offen und geheim gehalten, anstatt sie zum Schutz der eigenen Zivilbevölkerung aufzudecken und zu beseitigen. Auf diese Weise werden die Möglichkeiten zur Computerespionage und -kriminalität, zu Cyberterrorismus und -krieg gefördert.

erschienen in der FfF-Kommunikation,  
herausgegeben von FfF e.V. - ISSN 0938-3476  
[www.fiff.de](http://www.fiff.de)



Thomas Gruber

## Onlineoffensive: Die Bundeswehr im Cyber- und Informationsraum

Die Gefährdung der Zivilgesellschaft durch Attacken im Cyberraum war im vergangenen Jahr ein äußerst präsent Thema in der deutschen Presse. Die Angriffsszenarien reichten dabei von einer wirtschaftlichen Bedrohung durch „Hackerangriff[e] auf [...] deutsche Banken“<sup>1</sup> bis hin zu einer existenziellen Gefahr für das Individuum „durch Cyber-Angriffe [...] [auf] Krankenhäuser oder die Energieversorgung“<sup>2</sup>. Oft sind die Herkunft und die Intention der Attacken unbekannt – militärische Einheiten bestimmter Staaten oder Staatenbündnisse könnten geopolitische Interessen verfolgen, nationale Geheimdienste könnten Spionage betreiben oder kriminelle Organisationen könnten privatwirtschaftliche Akteure anvisieren. Diese Unsicherheit eignet sich allerdings gut für den Aufbau und die Festigung von Feindbildern; die Sprache wird dabei suggestiver: „Warnung vor russischen Cyberattacken: Angriffsziel Deutschland“<sup>3</sup> oder „Massiver Hacker-Angriff auf Thyssen-Krupp – waren es Chinesen?“<sup>4</sup>

### Bundeswehrstrukturen für den Cyberkrieg

Dieses Klima der Verunsicherung und der Bedrohung nutzen auch die Bundesregierung und das Bundesministerium für Verteidigung (BMVg), um die Ausweitung von militärischen Befugnissen im Cyberraum und die dementsprechende Aufrüstung der Bundeswehr zu rechtfertigen. Am 1. April 2017 ist die Struktur der Bundeswehr in diesem Zug um einen eigenen Organisationsbereich zum Cyber- und Informationsraum (CIR) gewachsen.<sup>5</sup> Das Kommando des CIR ist in Bonn Hardthöhe, dem Hauptsitz des BMVg, angesiedelt und befehligt 13.500 vorhandene Dienstposten. Die Aufgabenbereiche bestehen neben der Administration, Organisation und Bereitstellung von IT-Struktur vor allem in den verschiedenen Aspekten der Kriegsführung im Cyber- und Informationsraum. So fallen unter den neuen Organisationsbereich beispielsweise die psychologische Kriegsführung („operative Kommunikation“), die Störung feindlicher und Sicherung eigener Kommunikationsnetze („elektronische Kampfführung“), die Vernetzung und technische Ausstattung der Kriegseinheiten („Führungsunterstützung“) sowie Angriff und Verteidigung im Cyberraum („Cyber-Operationen“). Neben den bereits bestehenden Stellen werden außerdem 300 neue geschaffen, von denen 230 auf die Führung des Organisationsbereiches, 40 auf den Fachbereich *Cybersicherheit* und 20 auf die Verbesserung von Cyber-Operationen entfallen.

Um die Funktionalität des neuen Organisationsbereiches gewährleisten zu können, fehlt der Bundeswehr allerdings vor allem eines: qualifiziertes Personal. Denn während der Verteidi-



gungshaushalt jährlich immer großzügiger ausfällt, muss nach Wegfall der Wehrpflicht erheblich nachgeholfen werden, um das deutsche Militär als attraktiven Arbeitgeber darzustellen. Die Bundeswehr steigt mit riesigen Werbekampagnen, Kompromissbereitschaft und mit starkem Fokus auf ihre Zielgruppen in den Wettbewerb auf dem Arbeitsmarkt ein. Im Falle des Cyber- und Informationsraumes sind diese Bemühungen beispielsweise am Projekt *Digitale Kräfte* erkennbar, das mit 3,6 Millionen Euro Finanzierung<sup>6</sup> einen großen Teil der 12,5 Millionen Euro schweren Werbekampagne *Mach, was wirklich zählt*<sup>7</sup> der Bundeswehr ausmacht. Mithilfe von großflächigen Plakataktionen, Netzwerk-Sessions, auf Karrieremessen und in Jobcentern sollen IT-affine Personen, Gamer:innen und *Nerds*<sup>8</sup> für eine



Bundeswehr-Karriere begeistert werden. Dabei ist das Ziel, die Bundeswehr als moderne Arbeitgeberin mit Möglichkeiten zum Quereinstieg ohne starre Hierarchien darzustellen sowie das angehende Personal durch rührselige nationalistische Aussagen und gute Bezahlung ideologisch und finanziell an sich zu binden. Eine weitere Taktik der Nachwuchsgewinnung, die die Bundeswehr schon in anderen Fachbereichen erfolgreich einsetzt, ist die Anwerbung von Studierenden. An der Bundeswehruniversität München entsteht zu diesem Zweck beispielsweise der Masterstudiengang *Cyber-Sicherheit*, der ab 2018 jährlich 70 Absolvent:innen für eine anschließende Bundeswehrlaufbahn liefern soll.<sup>9</sup> In diesem Rahmen wird die Bundeswehruniversität um ein Forschungszentrum zur Cybersicherheit, 11 neue W3-Professuren und knapp 70 neue Stellen im Mittelbau und dem wissenschaftsstützenden Personal ergänzt. Neben der Neugewinnung von Personal sieht das BMVg außerdem die Gründung einer „Cyber-Reserve“ vor, die aus ausscheidenden Berufs- und Zeitsoldat:innen, Freiwilligen Zivilist:innen oder Seiteneinsteiger:innen aus MINT-Berufen besteht und die Schlagkräftigkeit des CIR erhöhen soll.

### Deutsche Strategien im Cyberkrieg und Darstellung in der Öffentlichkeit

Mit dem Organisationsbereich Cyber- und Informationsraum der Bundeswehr entsteht also ein neuer militärischer Akteur, der auf den deutschen Arbeitsmarkt drängt. Wie sieht aber die operative Strategie des CIR aus? Welche Einsatzgebiete gibt es? Die Aufgaben der deutschen Streitkräfte im Cyber- und Informationsraum werden in der öffentlichen Darstellung meist auf defensive Aktionen beschränkt – es gelte, der Verteidigung von „Staat, Wirtschaft und Gesellschaft“ zu dienen. Zur Entwicklung wirksamer Verteidigungskonzepte müssten zwar auch Cyberattacken erforscht und verstanden werden, diese würden aber keinem Angriffszweck dienen. Sollte zur Landesverteidigung doch einmal eine offensive Nutzung der Cyber-Konzepte vonnöten sein, so seien diese laut Katrin Suder, der zuständigen Staatssekretärin des BMVg, wie jeder andere militärische Angriff der Bundeswehr auch durch ein Mandat des Bundestages zu legitimieren.<sup>10</sup> Diese Versuche, damit auch im Cyber- und Informationsraum über eine deutsche Politik der militärischen Zurückhaltung zu sprechen, wirken aufgrund der militärischen Strategiepapiere und des tatsächlichen Vorgehens von Bundeswehr und BMVg nahezu lächerlich. Während öffentlich ausufernd über das destruktive Potential von Cyberangriffen berichtet wird, die noch dazu nur schwer nachzuverfolgen sind, sind ebendiese Eigenschaften natürlich auch äußerst interessant für das deutsche Militär. Und so wird im Weißbuch der Bun-

deswehr 2016 zum Thema Cyber- und Informationsraum von „offensive[n] Hochwertfähigkeiten, die es zu beüben und weiterzuentwickeln gilt“<sup>11</sup> gesprochen. Wie diese „Hochwertfähigkeiten“ verwendet werden, zeigt beispielsweise die seit kurzem bekannte Attacke der Gruppe *Computer Netzwerk Operationen*, die im CIR zukünftig im *Zentrum Cyber-Operationen* zu finden ist<sup>12</sup>: Bereits im Jahr 2015 attackierten deutsche Soldat:innen das afghanische Mobilfunknetz, um an Informationen zu einer Geiselnahme zu gelangen. Da dieser Einsatz weder ein Bundestagsmandat hatte, noch öffentlich gemacht wurde, ist zu vermuten, dass bei weitem nicht alle offensiven Cyberaktionen durch die vorgesehenen Kontrollinstanzen gehen.

Außer im Rahmen eines Militäreinsatzes soll die Bundeswehr auch verstärkt in die zivile Kommunikation eindringen. Im Abschlussbericht zum Aufbaustab des CIR ist diesbezüglich von einer verstärkten Zusammenarbeit des BMVg mit dem Bundesministerium des Inneren (BMI) die Rede, in deren Rahmen „gemeinsam ein neues Verständnis über die intensivere Kooperation und auch Beitragsfähigkeit der Bundeswehr [...] auch in Friedenszeiten“<sup>13</sup> entwickelt werden soll. Nach den militärischen Publikationen ist außerdem der Begriff der Landesverteidigung ein äußerst biegsamer: So seien nicht nur militärische Attacken ein Grund für ein Eingreifen der Bundeswehr, sondern auch Wirtschaftsspionage oder Rekrutierungsbemühungen terroristischer Gruppierungen in sozialen Netzwerken. Gleichzeitig, so wird allerdings betont, sollen die sonst für solche Aufgaben zuständigen Polizeien und Geheimdienste nicht in ihren Kompetenzen beschnitten werden, sondern eine „Überlappung“ mit den Arbeitsbereichen der Bundeswehr stattfinden. Der Trend der polizeilich-militärischen Zusammenarbeit im Cyberraum wird auch durch die Ansiedlung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITIS) auf dem Campus der Bundeswehruniversität in München verdeutlicht.<sup>14</sup> Die ZITIS ist eine Einrichtung, die das BMI mit Methoden der „digitalen Forensik, der Telekommunikationsüberwachung, der Kryptoanalyse (De-kryptierung), der Massendatenauswertung/Big-Data sowie [...] technischen Fragen von Kriminalitätsbekämpfung, Gefahrenabwehr und Spionageabwehr“<sup>15</sup> unterstützen soll. Die Spionagebehörde und die militärische Hochschule sollen laut dem BMI eng kooperieren und perspektivisch sogar zusammenwachsen.

### Bewertung und Bedeutung

Die Darstellung von Seiten des Staates und der Bundeswehr behandelt Cyberattacken auf staatliche Institutionen oder privatwirtschaftliche Unternehmen wie militärische Angriffe auf das eigene Land. So bekommen Probleme der IT-Sicherheit

**Thomas Gruber**

**Thomas Gruber** ist Mathematiker und promoviert an der Universität Bremen zum Thema *Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung*. Er ist Stipendiat der Rosa-Luxemburg-Stiftung und Mitglied der *Informationsstelle Militarisierung* (IMI) in Tübingen.

oder allenfalls kriminelle Aktionen wie Wirtschaftsspionage und Eigentumsdelikte im Cyberraum schnell eine militärische Bedeutung.<sup>16</sup> Die Zivilgesellschaft wird dabei als zu schützende Objekt vereinnahmt, um auf dieser Grundlage das bestehende Wirtschafts- und Herrschaftssystem im Cyberraum zu verteidigen. Zu diesem Zweck werden der Bundeswehr erhebliche finanzielle und personelle Kapazitäten sowie weitreichende Befugnisse im Cyber- und Informationsraum zur Verfügung gestellt. Da die Bundeswehr dabei in einem vorwiegend zivil genutzten Raum agiert, wird empfindlich in die digitale Privatsphäre einzelner Personen oder Personengruppen eingegriffen. So gerät die Zivilgesellschaft auch im virtuellen Raum zunehmend ins Kreuzfeuer staatlicher und militärischer Akteur:innen.

Die aktuellen Versuche, mit denen sich die Bundeswehr neben Polizeien und Geheimdiensten Verfügungsgewalt im Cyber- und Informationsraum verschaffen will, können als zusätzliches Alarmsignal für zivilgesellschaftliche Akteur:innen verstanden werden. Ob Privatpersonen, aktivistische Gruppen oder politische Vereinigungen – es gilt sowohl, eigene kritische Daten zu schützen, als auch den virtuellen Raum gegen staatlichen und militärischen Angriff zu verteidigen und wieder zivil zu vereinbaren.

## Referenzen

- 1 *Hackerangriff auf dreizehn deutsche Banken*, faz.net, 5.1.2017
- 2 *Die Bundeswehr sucht IT-Spezialisten für den Krieg im Cyberspace*, sueddeutsche.de, 5.1.2017
- 3 *Warnung vor russischen Cyberattacken: Angriffsziel Deutschland*, tagesschau.de, 5.1.2017
- 4 *Massiver Hacker-Angriff auf Thyssen-Krupp – waren es Chinesen?*, derwesten.de, 5.1.2017
- 5 *Kommando Cyber- und Informationsraum: Bundeswehr verteidigt die Freiheit – jetzt auch im Netz*, heise.de, 3.4.2017; *Abschlussbericht Aufbaustab Cyber- und Informationsraum*, pdf, 5.1.2017
- 6 *Folien CIR*, pdf, 5.1.2017
- 7 *„Mach, was wirklich zählt“: So viel kostet die Bundeswehr-Werbung*, fr-online.de, 5.1.2017
- 8 *Abschlussbericht CIR*, S. 32
- 9 *Größtes Forschungszentrum für Cyber entsteht*, unibw.de, 5.1.2017
- 10 *Mandatierung, Attribution und offensive Fähigkeiten? Anhörung zur Bundeswehr im „Cyberraum“*, netzpolitik.org, 5.1.2017
- 11 *Weißbuch der Bundeswehr 2016*, pdf, S.93, 5.1.2017
- 12 *Entführte Deutsche: Bundeswehr-Hacker knackten afghanisches Mobilfunknetz*, spiegel.de, 5.1.2017
- 13 *Abschlussbericht CIR*, S. 37
- 14 *Zivil-militärische Zusammenarbeit: ZITIS – Spionagebehörde des BMI zieht auf den Bundeswehr-Campus*, imi-online.de, 3.4.2017
- 15 *Startschuss für ZITIS*, BMI, 3.4.2017
- 16 Kai Denker: *Die Erfindung des Cyberwars*, in: *WeltTrends* 113, S. 17–21



Aaron Lye

## Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet

*Der Computerwurm W32.Stuxnet, kurz Stuxnet, bekam weltweit von Analyst:innen, Forscher:innen, Hacker:innen, Medien und Politiker:innen in den Jahren 2010/2011, aber auch in den Folgejahren, große Aufmerksamkeit. Dieses lag daran, dass Stuxnet eine große und komplexe Bedrohung war und technisch einiges zu bieten hatte. Die Techniken und Möglichkeiten digitaler Kriegsführung sollen an diesem Beispiel verdeutlicht werden.*

### Technische Beschaffenheit von Stuxnet

Stuxnet ist ein Computerwurm, der sich in 32-Bit-Windowsnetzwerken verbreitet mit dem Ziel, eine spezielle Art von Anlagensteuerungssystemen der Firma Siemens – im Speziellen *SCADA Industrial Control Systems* – anzugreifen. Durch die Infektion des Steuerungsrechners war es dann möglich, auch auf *Programmable Logic Controllers* (PLC) zuzugreifen und diese umzuprogrammieren. Bei Stuxnet handelt es sich also um eine gezielte Attacke, die hochspezifisch für die Kompromittierung eines vorher genau spezifizierten Systems entwickelt wurde. Dies geht aus verschiedenen unabhängigen Analysen des Wurms hervor. Wesentliche Teile der technischen Analyse, bei der der Wurm *reverse-engineered* wurde, wurden gemeinsam von unterschiedlichen Unternehmen, wie Symantec und Microsoft, zusammen mit Einzelpersonen entwickelt, sind gut verstanden und der interessierten Öffentlichkeit zugänglich. Die Art und Beschaffenheit von Stuxnet, die Anzahl der Exploits und auch die Angriffe auf PLCs sind sehr ungewöhnlich. Ein PLC wird im Deutschen

auch speicherprogrammierbare Steuerung (SPS) genannt und ist ein Digitalrechner zur Steuerung oder Regelung von Pumpen, Ventilen, Motoren oder im Allgemeinen von Maschinen oder Anlagen. Die Hardware ist üblich und wird weltweit in Millionen von Systemen verwendet. Die Einsatzgebiete erstrecken sich von Produktionsanlagen mit relativ simplen Steuerungen bis hin zur Steuerung von Robotern und Zentrifugen mit komplexen Abläufen, Kraftwerken (Kern, Kohle, Wasser, Wind), Mineralabbau, petrochemischer Industrie, Wasserwiederaufbereitung und Wassertransport, Zügen etc. Anzumerken ist, dass dieselbe Hardware sowohl in zivilen als auch in militärischen Anlagen benutzt wird.

Der Wurm lässt sich in zwei Teilen betrachten, die jeder für sich interessant sind. Der erste Teil ist die Infektion und Verbreitung des Wurms auf Betriebssystemebene; der zweite Teil ist die Infektion des PLC. Beide Teile sollen im Folgenden kurz erläutert werden. Details zu den Exploits sind beispielsweise in Symantecs Analyse<sup>1</sup> zu finden.