stellen."[22] So haben Medienpädagogik und verwandte Disziplinen früh anzusetzen bei all den Aufgaben, die schließlich zu wichtigen Fragen auf einer Meta-Ebene führen könnten: Worin liegt das Faszinosum von Big Data, dass wir viele der Dienste so unhinterfragt in Anspruch nehmen und uns nicht um ihre positivistisch-verkürzende Sichtweise kümmern? Warum lassen wir zu, dass durch die Zahlengläubigkeit Prozesse der Digitalisierung nicht nur die Rahmenbedingungen bilden, sondern oft den Kern in vielen Lebensbereichen? Und warum sind Vermessung, Berechnungen, Statistiken oft mehr wert als ästhetische Erziehung und real-sinnliche Erfahrungen?

erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Anmerkungen

1 Mayer-Schönberger V, Cukier, K (2013): Big Data. Die Revolution, die unser Leben verändern wird. München, S. 78

2 Ortlieb CP (2010): Ökonomie ist eigentlich keine Wissenschaft. In FAZ vom 08.05.2010. Online unter: http://www.faz.net/aktuell/gesellschaft/oekonomie-ist-eigentlich-keine-wissenschaft-11418489.html (letzter Zugriff: 08.03.2018)

3 Mayer-Schönberger/Cukier, S. 94

4 Meyer-Ebrecht D (2016): Selbstbestimmt war gestern? Wenn wir das Entscheiden Maschinen überlassen. In: FIfF-Kommunikation 1/16, S. 12-15, S. 14

5 Burkhardt M (2015): Digitale Datenbanken. Eine Medientheorie im Zeitalter von Big Data. Bielefeld 2015, S. 341

6 Lobe A (2016): Wir laufen auf Autopilot. In: FAZ vom 27.02.2016. Online unter: http://www.faz.net/aktuell/feuilleton/kuenstliche-intelligenz-wir-laufen-auf-autopilot-14079287.html (letzter Zugriff: 31.01.18)

7 Borck C (2017): Big Data. Praktiken und Theorien der Datenverarbeitung im historischen Querschnitt. In: NTM – Zeitschrift für Geschichte der Wissenschaften, Technik und Medizin 4/2017, S. 399 – 405, S. 404

8 Dander V (2014): Von der ‚Macht der Daten' zur ‚Gemachtheit von Daten'. Praktische Datenkritik als Gegenstand der Medienpädagogik. In: Mediale Kontrolle unter Beobachtung 3.1/2014. Online unter: http://www.medialekontrolle.de/wp-content/uploads/2014/09/Dander-Valentin-2014-03-01.pdf (letzter Zugriff: 08.03.2018), S. 1-21, S. 2

9 Bächle, TC (2016): Digitales Wissen, Daten, Überwachung zur ... Berlin 2016, S. 13

13 Ebd., 12 (Hervorhebung im Original)

14 Püschel F (2014): Big Data und die Rückkehr des Positivismus. Zum gesellschaftlichen Umgang mit Daten. In: Mediale Kontrolle unter Beobachtung 3.1/2014. Online unter: http://www.medialekontrolle.de/wp-content/uploads/2014/09/Pueschel-Florian-2014-03-01.pdf (letzter Zugriff: 16.01.2018), S. 1-23, S. 12

15 Bächle, S. 72

16 Püschel, S. 18

17 Simanowski, S. 80

18 Gapski H (2015): Big Data und Medienbildung – eine Einleitung. In: Ders. (Hg.): Big Data und die Medienbildung. Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt. Marl, S. 9-18, S. 10ff.

19 Ebd., 13

20 Burckhardt, S. 302

21 Bächle, S. 142

22 Dander, S. 3

Hans-Jörg Kreowski

Der Informationsraum aus militärischer Sicht

Dieser Artikel ist eine schriftliche Ausarbeitung eines Vortrags auf dem Kongress der Informationsstelle Militarisierung 2017 zum Thema Krieg im Informationsraum. Es geht um Cyberkrieg, was die etwas gängigere Bezeichnung für eine bedenkliche Entwicklung ist.

Während Albert Einstein zu einem denkbaren dritten Weltkrieg noch sagt: „I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones", legt sich Mandeep Singh Bhatia fest: *World War III: The Cyber War*[1]. Wenn auch die meisten anderen Fachleute und KommentatorInnen nicht soweit gehen, zeigt die enorme Resonanz des Themas Cyberkrieg in den Printmedien, dass hier eine neue ernsthafte Bedrohung heraufzieht (siehe Abbildung 1 mit diversen Titelbildern zum Cyberkrieg).

Das Thema hat mit *Zero Days: Hinter den Kulissen des Cyberkriegs* von Alex Gibney auch die Filmwelt erreicht. Der Dokumentarfilm wurde auf der Berlinale 2016 gezeigt. Mit Datum 19. August 2016 kann man recht reißerisch lesen[2]:

> *„Die Dokumentation von Alex Gibney fängt als Spurensuche über den Computervirus Stuxnet an. Und während IT-Sicherheitsexperten, Ex-NSA- und CIA-Chefs, ehemalige Mossad-Agenten und auch ein paar Whistleblower über das reden, worüber niemand reden darf, fällt der Satz, dass es sich gerade anfühle wie 1945, nachdem die USA zwei Atombomben über Japan gezündet haben: In dieser verwirrend coolen Spionage-Geschichte, die Sie permanent auf der Stuhlkante hält, geht es um mächtige neue Waffen, über deren Reglementierung man dringend reden muss, wenn die Welt nicht noch mehr im Chaos versinken soll."*

Stuxnet ist aber nur ein Beispiel. Die Liste gravierender Cyberattacken ist lang. So hieß es bei Heise Security am 27. Juni 2017: „Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm", wobei Computersysteme verschlüsselt wurden mit dem Angebot, sie bei Zahlung von Lösegeld wieder zu entschlüsseln. So wurde am 15. Mai 2015 von SPIEGEL ONLINE gemeldet: „Sicherheitsalarm im Parlament: Cyberangriff auf den Bundestag", was bei n-tv die Überschrift „Cyber-Attacke löst Alarm aus: Beispielloser Angriff auf den Bundestag" erhielt. Die Beseitigung des erheblichen Schadens hat über 100 Millionen Euro gekostet. Weitere Beispiele liegen weiter zurück: eine Angriffsserie auf US-amerikanische Computersysteme von

Abbildung 1: Auswahl an Titelbildern zum Thema Cyberkrieg

Rüstungskonzernen, NASA und andere, die unter dem Namen Titan Rain bekannt wurde, die Denial-of-Service-Attacken auf estländische und georgische Regierungswebseiten, die tagelang außer Betrieb waren, die als Olympic Games bezeichnete und bisher vielleicht gravierendste Malwareattacke mit dem bereits angesprochenen Cyberwurm Stuxnet auf die nuklearen Wiederaufbereitungsanlagen des Irans, die dessen Atomwaffenprogramm um Monate zurückgeworfen hat. Die Entwicklung von Stuxnet hat nach Schätzungen von Fachleuten vielleicht bis zu einer Milliarde US-Dollar gekostet, zeigt aber, dass Cyberattacken zur Zerstörung technischer Anlagen führen können. Viele weitere Beispiele ähnlicher Art ließen sich anführen. Sie alle zeigen, dass sich Cyberangriffe mit Viren, Würmern, Trojanern und sonstiger Schadsoftware für Spionage, Propaganda und Informationsmanipulation verwenden lassen, dass man damit Service-Webseiten und Computersysteme insgesamt lahmlegen, infiltrieren und umfunktionieren kann, ja dass es sogar möglich ist, technische Geräte wie Kraftfahrzeuge, Flugzeuge bis hin zu ganzen Industrieanlagen fernzusteuern oder zu zerstören. Besonders bedroht sind kritische Infrastrukturen wie Energie- und Wasserversorgung, Krankenhäuser, Straßen-, Bahn- und Flugverkehr, Verwaltungseinrichtungen und militärische Einrichtungen. Je nach Ausmaß reichen die Konsequenzen von unbequem bis Elend und Tod.

Zum Begriff Cyberkrieg

An dieser Stelle möchte ich einen Versuch wagen, den Begriff Cyberkrieg wenigstens ansatzweise zu definieren als Kriegsführung mit Informations- und Kommunikationstechnik (IKT) wie Computer, Netzwerke, Software als Waffen und militärische Systeme aller Art, deren Entwicklung und Betrieb des Einsatzes von Informatikmethoden bedürfen. Dabei ist schon umstritten, ob das IKT-Steuerung von militärischen Systemen wie Raketen, Drohnen, Luftabwehr, Panzer etc. einschließt. Ich würde das bejahen, weil es sich um dieselben oder zumindest sehr ähnliche methodische und technologische Grundlagen aus der Informatik sowie der Informations- und Kommunikationstechnik handelt.

Der Begriff Cyberkrieg ist noch relativ jung. Vieles, was darunter subsumiert wird, wurde früher als Informationskrieg bezeichnet. Ute Bernhardt und Ingo Ruhmann geben im Dossier 74 *Information Warfare und Informationsgesellschaft – Zivile und sicherheitspolitische Kosten des Informationskriegs*, das als Beilage der Zeitschriften *Wissenschaft und Frieden* 1/2014 und *FIfF-Kommunikation* 1/2014 erschien, einen umfassenden Überblick. Sie sehen die Anfänge in der Entschlüsselung der Enigma-Chiffriermaschinen, die vom deutschen Militär im Zweiten Weltkrieg für die Verschlüsselung des Nachrichtenverkehrs eingesetzt wurden. Ein Team von Fachleuten um den berühmten britischen Mathematiker Alan Turing in Blechley Park hat das mit Hilfe von Vorläufern heutiger Computer geschafft, was nicht ohne Einfluss auf den Kriegsverlauf blieb.

Es führte bereits damals zur Gründung der National Security Agency (NSA) in den USA und des Government Communication Headquarters (GCHQ) in Großbritannien, die beide bis heute eine entscheidende Rolle als Cyberkriegführer spielen. Einen ersten Höhepunkt des *Information Warfare* war dann der Aufbau von C3I-Systemen (Control, Command, Communication, Intelligence) im Kalten Krieg in den USA, durch die die Kriegführungsebene auf Informations- und Kommunikationstechnik abgestützt wurde. Seitdem sind vor allem die Fähigkeiten dazugekommen, in generische Systeme durch Hacking gezielt einzudringen, sie zu manipulieren und sie zu zerstören.

Auf der begrifflichen Seite muss beachtet werden, dass alle Varianten wie Cyberkrieg, Informationskrieg, Krieg im Informationsraum oder Krieg im Cyber- und Informationsraum den gemeinten Sachverhalt nur sehr bedingt treffen. So ist *cyber*, das vom Altgriechischen *steuern und navigieren* stammt, zu eng und als Synonym für *Computer- und Internet-gestützt* zu nebulös. So ist *Information* zu statisch, und der *Informationsraum* ist überhaupt gar kein „Raum", sondern ein riesiges Netz aus Computern und computergesteuerten Geräten, Anlagen, Maschinen etc. Tatsächlich geht es um programmierte, von Algorithmen getriebene Kriegsführung. Ich verwende den Begriff Cyberkrieg dennoch auch weiterhin, weil er inzwischen so etabliert ist, dass mit jeder anderen Bezeichnung Verständnisschwierigkeiten entstehen könnten.

Weltweites Cyberwettrüsten

Dass das als Cyberkrieg bezeichnete Phänomen ernst genommen werden muss und eine eklatante neue Bedrohung darstellt, ergibt sich aus der Tatsache der weltweiten gigantischen Aufrüstung in diesem Bereich. Mehr als 100 Staaten haben Cyberkriegseinheiten gebildet, die zudem überwiegend offensiv ausgerichtet sind. Die USA betreibt mit der NSA und dem United States Cyber Command (USCYBERCOM) die größte Einheit. China hat die *Blaue Armee*, eine Hackereinheit, die offiziell rein defensiv ausgerichtet ist. Russland wird verdächtigt, wiederholt offensiv Cyberangriffe zu betreiben oder zu unterstützen, was allerdings wohl nicht wirklich bewiesen ist. Der Iran brüstet sich damit, die weltweit zweitgrößte Einheit zu haben. Israel hat die *Cyber Defense Taskforce*, Großbritannien die *Government Communication Headquarters* (GCHQ) und so weiter und so weiter.

Auch Deutschland steht da nicht zurück, auch wenn die Regierung erst spät auf die weltweite Entwicklung systematisch reagiert hat. Seit 2011 arbeitet der Nationale Cyber-Sicherheitsrat, der beim Beauftragten der Bundesregierung für Informationstechnik angegliedert ist. Im selben Jahr nahm das Nationale Cyberabwehrzentrum seine Arbeit auf, in dem die Cyberaktivitäten von Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesamt für Verfassungsschutz und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe koordiniert werden. Assoziierte Mitglieder sind das Bundeskriminalamt, der Bundesnachrichtendienst, die Bundespolizei, die Bundeswehr mit dem Militärischen Abschirmdienst sowie das Zollkriminalamt. Außerdem haben das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2012 die *Allianz für Cybersicherheit* geschmiedet. Die Strukturen dieser Einrichtungen sind allerdings eher intransparent und ihre Kontrolle ziemlich unklar. Die Bundeswehr steht nicht abseits. Seit 2016 baut sie einen Organisationsbereich *Cyber- und Informationsraum* (CIR) mit rund 13.500 Dienstposten auf. Das Kommando CIR, die Führungsebene des Bereichs, wurde am 5. April 2017 offiziell durch die Verteidigungsministerin in Dienst gestellt. Es bildet ein Dach über Abteilungen, die vorher über viele Bereiche der Bundeswehr verteilt waren; insbesondere sind ihm das Kommando Strategische Aufklärung, das Kommando Informationstechnik der Bundeswehr, ehemals Führungsunterstützungskommando der Bundeswehr, und das Zentrum für Geoinformationswesen der Bundeswehr unterstellt. Aufgaben wie die Erstellung von Lageplänen, Weiterentwicklung, Ausbildung, nationale und internationale Zusammenarbeit im Cyber- und Informationsraum sowie die Informationssicherheit in der Bundeswehr liegen damit in einer Hand. Soweit, so unspektakulär. Aber der Organisationsbereich CIR bringt auch einige äußerst bedenkliche Entwicklungen mit sich. So hat die Bundeswehr neben Heer, Marine und Luftwaffe eine weitere Teilstreitkraft gebildet, was auch weltweit betrachtet eine neue Qualität darstellt. Defensive und offensive Cyberkriegsfähigkeiten sollen massiv ausgebaut werden. Dazu führt die Bundeswehr eine millionenschwere Werbekampagne zur Personalgewinnung durch und hat an der Universität der Bundeswehr München einen Masterstudiengang IT-Sicherheit eröffnet, dessen personelle Ausstattung jede zivile Hochschuleinrichtung vor Neid erblassen lässt.

... aus militärischer Sicht

Cyberkrieg gilt als militärisch attraktiv, weil bei einem Angriff keine eigenen SoldatInnen direkt gefährdet sind, weil die Rückverfolgung schwierig und teilweise unmöglich ist, so dass der Angegriffene gar nicht weiß, wer angreift, weil der Angriff auf meist zivile Ziele den Gegner empfindlich schwächen kann, weil Cyberwaffen vergleichsweise billig zu haben sind. Die mangelhafte Rückverfolgung und Zuordnung von Cyberangriffen begünstigt Attacken auch unterhalb der Kriegsschwelle als „Nadelstiche" oder Versuchsballon. Die Vorteile gelten allerdings nur für die Angreifer, für die Angegriffenen verkehrt sich das in das Gegenteil. Aber auch die Vorteile sind eher scheinbar und in vielfältiger Hinsicht eigentlich Nachteile. Weil zum Beispiel Cyberwaffen relativ leicht zu beschaffen oder zu entwickeln sind, können viele Staaten und auch größere Terrorgruppen sich das leisten, so dass die eigene Gefährdung wächst. Zudem ist das Angreifen mit Cyberwaffen wesentlich einfacher als das Verteidigen, weil dafür die Instrumente bekannt sind und man nur ein paar gute Computer und ein Team von Hackern braucht, die wissen, wie man die unzähligen Schwachstellen und Sicherheitslücken für die Installation von Schadsoftware nutzen kann. Cyberabwehr dagegen ist bei massiven und komplexen Angriffen technisch viel schwieriger und nur unzureichend beherrscht.

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

Dennoch wird Cyberrüstung von Politik und Militär für nötig erachtet mit der Begründung, dass alle im Cyberbereich rüsten, so dass man selbst nicht abseits stehen kann. Die Konsequenz ist eine gigantische weltweite Cyberrüstungsspirale. An der drehen insbesondere die USA mit ungeheuren Geld- und Personalmitteln. In ihrer *Strategy for Operating in Cyberspace* wird das damit motiviert, dass die USA im Bereich Defensive schwach ist bei gleichzeitiger hoher Abhängigkeit von funktionierender Informationstechnik und hoher Verletzlichkeit durch Vernetzung, Zentralisierung, Standardisierung, Mobilität. Man findet dort eine weitgefasste Definition eines Cyber-Angriffs: Denial-of-Service-Attacken, Sabotage von militärischen und zivilen Systemen (insbesondere von kritischen Infrastrukturen), Manipulation von Informationen, Wirtschaftsspionage und Diebstahl geistigen Eigentums. Hacktivismus, Cybercrime und Cyberwarfare werden undifferenziert als Bedrohungen der nationalen Sicherheit angesehen. Die Eintrittsschwelle für Gegenangriffe wird in diesem Strategiepapier sehr niedrig angesetzt, wobei ausdrücklich konventionelle Gegenschläge vorgesehen sind. Auch wenn dieser Vorbehalt bisher wohl nicht zur Anwendung gekommen ist, klingt er doch ziemlich besorgniserregend. Was auch Deutschland und die anderen NATO-Partner der USA in diesem Zusammenhang betrifft, ist die Frage, ob die USA im Falle eines Cyberangriffs den Bündnisfall ausrufen und so die ganze NATO in einen (Cyber-)Krieg hineinziehen können.

An einer anderen Stelle beschäftigt sich die NATO bereits mit einem wichtigen Aspekt der Cyberkriegsführung. Zwischen 2009 und 2012 wurde von einer internationalen Gruppe mit rund 20 Fachleuten am *NATO Cooperative Cyber Defence Centre of Excellence* in Tallinn eine rechtlich nicht bindende Studie erarbeitet, wie sich das Kriegsvölkerrecht für den Kriegsfall (vor allem die Genfer Konventionen) auf Cyber-Konflikte und Cyberkrieg anwenden lässt. 2013 erschien Teil 1 des *Tallinn-Manuals* bei Cambridge University Press. Der Fokus des ersten Teils liegt auf den massivsten Cyber-Operationen, die während bewaffneter Konflikte durchgeführt werden oder das Verbot von Gewalteinsatz in internationalen Beziehungen verletzen. 95 Regeln zur Interpretation einzelner Bestimmungen des Kriegsvölkerrechts hinsichtlich Cyberkrieg sind aufgestellt worden. Inzwischen ist auch 2017 Teil 2 erschienen, in dem niederschwelligere Cyberangriffe behandelt werden.

Ohne auf die Details einzugehen, sei daran erinnert, dass die Genfer Konventionen von Kriegsparteien verlangen, Opfer, Wehrlose und Unbeteiligte zu schützen, wobei insbesondere Angriffe auf Zivilpersonen verboten sind. Außerdem sollen zivile Einrichtungen und Kulturgüter verschont werden. Schon allein daraus ergibt sich, dass die außerordentliche Bedrohung von zivilen Infrastrukturen durch die Cyberkriegsrüstung völkerrechtlich inakzeptabel ist. Darüber hinaus sei auch angemerkt, dass die Charta der Vereinten Nationen, der fast alle Staaten der Welt zugestimmt haben, Krieg verbietet. In der Präambel heißt es dazu: „... determined to save succeeding generations from the scourge of war ...“, und im Artikel 2 des ersten Kapitels steht: „... All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered ...“. Im Grundsatz ist also Cyberkrieg wie Krieg verboten.

Cyberpeace

Aus all diesen Fakten, Problemen, Vorkommnissen und allseitigen Bedrohungen wäre die einzig richtige Konsequenz Cyberabrüstung und ein Verbot von Cyberwaffen, zumindest den offensiven. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) führt seit einigen Jahren eine Cyberpeace-Kampagne durch, deren Ziel ein Gegenkonzept zum Cyberkrieg ist.

Angestrebt ist die Ächtung jeglicher Form von Cyberwaffen (zumindest von offensiven). Eine wesentliche Voraussetzung auf dem Weg dahin wäre ein demokratisch gestaltetes, demokratisch kontrolliertes und entmilitarisiertes Internet, das dem Frieden dient und nicht der Ausspähung sowie der Unterstützung militärischer Aktivitäten. Völlig utopisch ist das Ziel nicht, denn es gibt auf der Ebene de Vereinten Nationen ExpertInnen-Gespräche mit dem Ziel eines Cyberwaffen-Verbots oder wenigstens einer Regulierung. Aber auch auf nationaler Ebene lässt sich etwas tun. So könnte sich die Bundeswehr anders als momentan auf reine Cyberabwehr beschränken. So könnte gesetzlich geregelt werden, dass alle im zivilen und militärischen Bereich entdeckten Sicherheitslücken und Schwachstellen in IT-Systemen aufgedeckt und beseitigt werden müssen, statt sie für den eigenen offensiven Gebrauch zu erwerben, zu nutzen und geheim zu halten.

cyberpeace
eine Kampagne des FIfF

Mehr zum Thema Cyberpeace findet man auf der Webseite *https://cyberpeace.fiff.de*. Neben dem bereits genannten Dossier 74 der Zeitschrift Wissenschaft und Frieden möchte ich auf die Publikationen im Abschnitt *Referenzen* als weiterführende Literatur verweisen.

Referenzen

Hügel S, Kreowski HJ und Meyer-Ebrecht D (2017): Cyberwar and Cyberpeace. In: Handbook of Cyber-Democracy, Cyber-Development and Cyber-Defense, Springer, 25 Seiten.

Johnigk S, Kreowski HJ und Nothdurft K (2014): Cyberwar – Schimäre oder reale Bedrohung?, FIfF-Kommunikation 4/2014, Seiten 74-77.

Kreowski HJ and Meyer–Ebrecht D (2017): „Revolution in Military Affairs“. In: The Future Information Society, World Scientific Series in Information Studies, Band 8, Seiten 439-448.

Meyer-Ebrecht D (Hg.) (2015): Kriegführung im Cyberspace, Dossier 79 in Wissenschaft und Frieden 3/2015 und FIfF-Kommunikation 3/2015.

Ganz besonders möchte ich schließlich das 5-minütige Video von Alexander Lehmann: Cyberpeace statt Cyberwar, aus dem Jahre 2017 empfehlen, das mit Unterstützung des FIfF entstanden ist und sowohl sehr anschaulich in das Thema Cyberkrieg einführt als auch die Grundidee von Cyberpeace vermittelt (https://vimeo.com/216584485, https://www.youtube.com/watch?v=St955HBD-7k).

Anmerkungen

1 *Titel eines Artikels im International Journal of Cyber Warefare and Terrorism 1,3 (2011), 11 Seiten*

2 *https://www.stern.de/kultur/film/trailerpremiere-zero-days---der-krieg-tobt-im-computer-7015382.html*