CGS - Discussion Papers
www.cgs-bonn.de

Julia Linzen

CGS-Spezial-Reihe: Analysen zur globalen Politik des Internets

CYBERWAR UND CYBERWARFARE

Bereits Realität oder (dys-)/utopisches Zukunftsszenario?

CGS - Discussion Paper 14

Dezember 2014

Center for Global Studies bonn

universitätbonn

Die Vorstellung von Cyberkriegen, die unser aller Sicherheit zukünftig existenziell gefährden werden, scheint im gegenwärtigen Diskurs um Cybersicherheit das dominierende Denkmuster zu sein. Inwieweit und ob von Cyberwarfare und Cyberwar tatsächlich eine Gefahr ausgeht, welche unterschiedlichen Positionen und Argumentationsweisen in der aktuellen Debatte existieren, soll dabei im vorliegenden Artikel diskutiert werden.

1. Einleitung

Cybersicherheit und der Schutz kritischer Infrastrukturen werden in der globalen Welt des 21. Jahrhunderts – nicht nur von US-Präsident Barack Obama – als eine zentrale gegenwärtige und zukünftige Herausforderung formuliert, die es zu gewährleisten gilt. Die Bedeutsamkeit des Cyberspace wird auch dadurch ersichtlich, dass sich immer mehr Staaten in ihrer sozialen, kulturellen, wirtschaftlichen, wissenschaftlichen, technischen und politischen Entwicklung vom Cyberraum abhängig machen. Leben, Arbeiten und Agieren ohne auf die Vorzüge und Freiheiten der globalen Vernetzung und der digitalen Informationstechnologien zurückgreifen zu können, erscheint vielen Menschen als schwieriges, gar sinnloses Unterfangen.
Gleichsam wird das Cyberspace auch von Kriminellen oder radikalen Akteuren zu ihren Vorteilen genutzt, hat die kriminelle und terroristische Unterwelt doch in der Informations- und Kommunikationstechnologie ein geeignetes Medium für ihre Machenschaften gefunden. Dabei reicht ihr Spektrum von “traditionellen“ kriminellen Aktivitäten wie Betrug, Fälschung und Urheberrechtsverletzungen bis hin zu spezifischen Delikten der Internetkriminalität (Spam, Malware, Spyware). Gleichzeitig bietet das Internet eine Plattform und scheint zugleich ein optimales Werkzeug für Terroristen zu sein, die sich über den Cyberspace organisieren, untereinander kommunizieren, ihre Propaganda verbreiten und schlussendlich so zu einem großen Teil über das Medium radikalisieren.
Diese Nutzung durch nicht-staatliche Akteure, die kriminelle und/oder terroristische Ziele verfolgen, wird von den Staaten als Grund angebracht, die Rechte der Nutzer im Web immer stärker einschränken zu wollen. Gleichzeitig sind staatliche Entitäten darum bemüht, die Hoheitsrechte über das Cyberspace zu erlangen, um sich – laut eigener Aussage – effektiv gegen die o.g. Gefahren schützen zu können. Ihre Bemühungen sind jedoch nicht nur defensiver Natur, vielmehr – nachdem sie das militärische und strategische Potenzial des Cyberspace entdeckt haben – sind auch immer mehr Staaten bestrebt, offensiv ihre Cybermittel auszubauen.
Die Befürchtungen, dass ein Zeitalter bevorsteht, in dem zu einem großen Teil Kriege ausschließlich elektronisch stattfinden werden und in dem es zu einem regelrechten Wettrüsten im Cyberspace kommen wird, sind im gegenwärtigen Diskurs um Cyberwar und Cyberwarfare (zu dt.: Cyberkrieg und Cyberkriegsführung) populäre Gedankenszenarien.
Inwieweit diese Schreckensvorstellungen wirklich realistisch sind oder vielmehr im Bereich der Fiktion und Panikmache zu verorten sind, gilt es allerdings zu überprüfen. Dabei soll nach einer Problematisierung der Definition der beiden genannten Begriffe aufgezeigt werden, dass die Begriffszuschreibung keineswegs unumstritten ist, sondern eines der Hauptprobleme der gegenwärtigen Debatte darstellt. Nach einem Überblick über den aktuellen Forschungsstand zu diesen beiden Themen, sollen kurz die wichtigsten Argumentationsweisen- und stränge vorgestellt werden. Ferner wird diskutiert, welches gegenwärtige und zukünftige Gefahrenpotenzial von Cyberkrieg- und Cyberkriegsführung ausgeht. Inwieweit die Debatte

von Sozialwissenschaft und Öffentlichkeit entscheidend mitgeführt werden kann und sollte, wird abschließend erörtert.

2. Definitionsansätze zu Cyberwar und Cyberwarfare

Obgleich die Begrifflichkeit Cyberwar[1] in Medien und Öffentlichkeit omnipräsent scheint, ist erstaunlich, dass eine konkrete Definition nicht existiert. Fälschlicherweise wird des Öfteren das gesamte Spektrum der Cyberkriminalität von Kreditkartenbetrug bis zur Manipulation von IT-Infrastruktur unter dem Begriff des Cyberkrieges subsumiert.[2] Das Konzept wird dabei oft mit anderen Begrifflichkeiten wie Cyberterrorismus, Cyberkriminalität und Cyberspionage gleichgesetzt und synonym verwendet, wenn gleich sich diese auf der Akteurs-Ebene und in Bezug auf mögliche Strafverfolgungsmaßnahmen erheblich unterscheiden, sind doch die o.g. Cyberbedrohungen durch Strafverfolgungsbehörden zu bekämpfen[3]; für das (potenzielle) Szenario des Cyberkrieges wären hingegen militärische Verteidigungsmaßnahmen von Nöten.[4]
Um den Versuch einer Definition von Cyberwar zu unternehmen, gilt es zunächst darauf hinzuweisen, dass es sich bei dieser Wortschöpfung um ein Kompositum der Wörter „cyber“ und „war“ handelt. Daher könnte im engeren – vor allen Dingen – wörtlichen Sinne – Cyberkrieg als eine Zustandsbeschreibung eines Krieges mit Cybermitteln verstanden werden. Gleichzeitig würde diese Auslegung aber auch eine Verschiebung der Kampfhandlungen auf den Cyberspace als unmittelbares Angriffsziel implizieren. Peter Singer und Allan Friedman argumentieren ähnlich: „The key elements of war in cyberspace all have their parallels and connections to warfare in other domains“[5].
Sofern die Kriterien eines politischen Zieles und Modus, welche den Kriegszustand von kriminellen Akten unterscheidet, erfüllt sind und eindeutig ein Gewaltelement festzustellen ist[6], kann – laut ihrer Vorstellung – von einer kriegerischen Auseinandersetzung gesprochen werden. Damit lehnen sich die beiden u.a. an die Vorstellungen Carl von Clausewitz‘ vom Krieg als Fortsetzung der Politik mit anderen Mitteln an.[7] Überträgt man diese Erkenntnisse auf das Konzept des Cyberkrieges, so lässt sich summierend feststellen, dass Cyberwar als eine kriegerische Auseinandersetzung im und um den Cyberspace verstanden werden kann, die – vorwiegend mit Mitteln aus dem Bereich der Informationstechnologien – eine Fortsetzung von Politik darstellt, um den Feind wehrlos zu machen und/oder zur Erfüllung des Willens des Aggressors zu zwingen.
Obgleich, wie deutlich wurde, eine genaue Begriffsbestimmung und Auslegung deutlich unkomplizierter ist als vielfach dargestellt, bleibt ungeklärt, inwieweit eine Cyberattacke beispielsweise auf Teile der Infrastruktur eines Landes bereits als eine Art digitale

[1] John Arquila und David Ronfeldt prägten 1993 den Begriff in ihrem Buch „Cyberwar is coming!“.
[2] Vgl. u.a. Tassilo Singer, *Cyberwarfare – Damoklesschwert für das Völkerrecht?* (S + F Sicherheit und Frieden, Nr. 1 / 2014, Jahrgang 32), S. 17.
[3] Vgl. Walter J. Unger, *Cyber Defence – eine nationale Herausforderung* (S + F Sicherheit und Frieden, Nr. 1 / 2014, Jahrgang 32), S. 10.
[4] Ebd.
[5] Peter W. Singer / Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014), S. 121.
[6] Vgl. ebd.
[7] Vgl. Carl von Clausewitz, *Vom Kriege*, 1832 (Ullstein Verlag, 1980), S. 27.

Kriegserklärung zu verstehen ist. Während die US-amerikanische Regierung eine Cyberattacke nur dann als solche auffasst, wenn ihr Ergebnis in „death, injury or significant destruction“ resultiert[8], sehen Länder wie Estland, die 2007 mit einem großflächigen DoS-Angriff auf ihre Cyberinfrastruktur konfrontiert waren, den Tatbestand einer solchen Attacke deutlich früher erfüllt. Bisher ist und bleibt folglich das Kriterium der menschlichen Versehrtheit für die meisten Nationen das entscheidende Bewertungsmoment.

> „Cyber attacks that cause repairable physical damage with no long-term consequences and no injury to humans have not been treated as use of force or armed attacks.“[9]

Die Staatengemeinschaft hat bisher allerdings noch nie die Rechtsauffassung vertreten, dass ein Cyberkrieg stattfindet oder stattgefunden habe.[10]
Abzugrenzen von der problematischen Begrifflichkeit des Cyberkrieges, sind die Möglichkeiten des Cyberwarfare. Entgegen eines weit verbreiteten Irrglaubens, muss der Einsatz von Cybermitteln im Kontext einer Kriegsführung oder eines operativen geheimdienstlichen Prozesses dabei nicht konsekutiv oder zwangsläufig in einen Cyberwar münden. Per Definition darf und muss Cyberkriegsführung weit verstanden werden[11]: So können unter diese Kriegsführung sowohl direkte Angriffe im Sinne von Kampfhandlungen als auch unterstützende, allgemeine Operationen wie Spionage oder die Manipulation von Technik durch Cybermittel subsumiert werden. [12] Mit diesen Möglichkeiten stellt Cyberkriegsführung bereits ein wichtiges und unterstützendes Mittel in geheimdienstlichen und militärischen Operationen dar.[13]
Es lässt sich also resümieren, dass alleine die Distinktion zwischen Cyberwar und Cyberwarfare häufig ausbleibt und so zu einem erheblichen Teil für den kontrovers geführten Diskurs über die Existenz und die Gefahren(potenziale) dieser beiden Begrifflichkeiten verantwortlich ist. Während Cyberkriegsführung in der militärischen und geheimdienstlichen Praxis bereits ein legitimes Mittel zu sein scheint, hat das Szenario eines Cyberkrieges bisher nicht stattgefunden.

3. Dominierende Sichtweisen im gegenwärtigen Diskurs

Ob ein solch rein elektronischer Krieg überhaupt jemals stattfinden wird, darüber existieren in der Forschung unterschiedlichste Meinungen, die im Folgenden skizziert werden sollen. Miriam Cavelty-Dunn steht dabei stellvertretend für eine Forschungsmeinung, die der gegenwärtigen Konzeptualisierung von Cyberkrieg entschieden widerspricht. Sie behauptet,

---

[8] Die *Tallinn Manual on the International Law Applicable to Cyber Warfare*, eine akademische, nicht-bindende Studie zur Frage, ob und inwieweit bestehendes Völkerrecht auf Cyberkonflikte und Cyberkrieg anwendbar sei, kommt zu einem ähnlichen Urteil. Artikel 30: “cyber attack' as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.” Allerdings wird hier ausdrücklich auch auf Schadenszufügung und Zerstörung von Objekten eingegangen.
[9] James P. Farwell / Rafal Rohozinski: *Stuxnet and the Future of Cyberwar* (Survival, Volume 53, Nr. 1, Februar / März 2011), S. 30f.
[10] Vgl. Tallin Manual on the International Law, hier zitiert nach: Singer, *Cyberwarfare – Damoklesschwert für das Völkerrecht?*, S. 17.
[11] Vgl. ebd.
[12] Vgl. ebd.
[13] Vgl. David C. Gompert / Martin Libicki: *Cyber Warfare and Sino-American Crisis Instability* (Survival: Global Politics and Strategy, Volume 56, Nr. 4), S. 11ff.

dass Cyberkriege gegenwärtig nicht existieren und aus mannigfaltigen Gründen auch zukünftig nicht stattfinden werden. Thomas Rid, Professor für Security Studies am King's College in London teilt Cavelty-Dunns Einschätzung eines regelrechten Cyberhypes, denn „cyberwar has never happened in the past, it is not occuring in the present, and it is highly unlikely that it will disturb the future“[14].
Als Gründe für das Ausbleiben von Cyberkriegen benennt Dunn Cavelty die Ineffizienz und die Gefahr eines konventionellen Gegenschlages.[15] Ferner problematisiert sie ebenfalls die Synonyme und definitorischen Ungenauigkeiten, die dazu dienen, eine gewisse Sensationsgier zu stillen beziehungsweise zu befriedigen:

> „Niemand bestreitet, dass wir als Gesellschaften außerordentlich vernetzt und abhängig und deshalb, theoretisch „verwundbar“ sind. Aber das Verunstalten von Webseiten ist kein Cyberwar. DDoS-Attacken, auch wenn Banken betroffen sind, sind kein Cyberwar. … Elektronische Kriegsführung ist nicht Cyberwar. Das Verbreiten von halb wahrer oder nicht wahrer Information im Krieg ist kein Cyberwar.“[16]

Die Negierung des Cyberkrieges geht einher mit der Vorstellung von Panik- und Angstmacherei, die von Akteuren wie Sicherheitsfirmen und Regierungen aktiv und bewusst gesteuert und geschürt wird, um Restriktionen von Freiheiten im Netz oder auch wirtschaftliche Interessen durchzusetzen. In diesem Kontext spricht Dunn Cavelty von so genannten “Threat Representatives“, die die aktuellen Debatten um Cybersicherheit – aus partikularen, vorrangig ökonomischen Interessen – dominieren.[17] Daher sehen Forscher wie Cavelty-Dunn nicht im Cyberkrieg an sich Gefahrenpotenzial, sondern vielmehr in dem fehlgeleiteten Diskurs und der Aufmerksamkeit, die das Konzept des Cyberkrieges gegenwärtig auf sich zieht. Gleichwohl kritisiert sie, dass in der Forschung über Cybersicherheit, ebenso wie bei Debatten um Cyberkrieg und Kriegsführung, eine theoretische Aufarbeitung mit den Theorien der Internationalen Beziehungen fast gänzlich fehlt. Lediglich die “Securitization Theory“[18] bietet ihrer Meinung nach erste Anhaltspunkte für neue Untersuchungsrahmen.
Der Negierung des Cyberkrieges folgt aber keineswegs eine Verneinung der Cyberkriegsführung. Die unterstützende Komponente in geheimdienstlichen oder militärischen Operationen wird durchaus anerkannt, gleichwohl wird betont, dass die menschliche Komponente fortwährend von entscheidender Bedeutung ist, wenn es um die Durchführung verschiedenster Einsätze geht. Exemplifiziert wird dies durch die Verwendung des Computerwurmes Stuxnet, der u.a. das iranische Atomprogramm erheblich beeinträchtigte und störte. Die Viren mussten in diesem Beispiele exogen durch einen Memory Stick in das iranische Netzwerk eingespeist werden.
Jedoch existieren auch deutlich andere Perspektiven zu Cyberwar und Cyberwarfare. Der Berliner Computersicherheitsexperte Sandro Gaycken sieht in Cybermitteln wie Hacking

---

[14] Thomas Rid, *Cyberwar and Peace – Hacking Can Reduce Real-World Violence* (Foreign Affairs, Essay. November / Dezember 2013, abrufbar unter: http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace).
[15] Vgl. Miriam Dunn-Cavelty, *So wahrscheinlich wie die Sichtung von E.T.*, (The European, 09.01.2011, abrufbar unter: http://www.theeuropean.de/myriam-dunn-cavelty/5160-cyberwar-und-cyberangst).
[16] ebd..
[17] Vgl. Myriam Dunn Cavelty, *From Cyberbombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse* (International Studies Review, Nr. 15 / 2013), S. 106f.
[18] Vgl. ebd., S. 107.

beispielsweise eine grund- und neuartige Bedeutung als militärisches Wirkmittel, welches es „schwächeren“ Akteuren mit Hilfe von vergleichsweise geringem Ressourceneinsatz ermöglicht, „stärkere“ Gegner kontinuierlich zu schwächen und ihnen punktuell zu schaden.[19] In diesem Kontext wird auch diskutiert, inwieweit der Einsatz von Hacking und Co. reale Gewalt eindämmen könne. Eine Vielzahl von Meinungen steht nicht nur Cyberkriegsführung äußerst positiv gegenüber, sondern stuft auch die Gefahrenpotentiale eines Cyberkrieges für das menschliche Individuum als erträglich und absehbar ein.[20] Diese bejahende Haltung geht mit der Vorstellung einher, dass sich die Austragung von Konflikten insoweit transformiere, als dass das Risiko für menschliche Kollateralschäden durch neuere, präzisere und effektivere Wirkmittel immer weiter reduziert werden könne. [21] Die Idee einer sauberen und “zivilisierten“ Form von Kriegsführung und Krieg wird vom Sicherheitsberater Phil Lieberman als äußerst attraktiv eingeschätzt und bewertet. So führt er aus, dass die Möglichkeit bestehe, „precise, surgical, virtual, and most importantly, bloodless […] warfare where no one dies“ [22] zu betreiben. Würmer wie Stuxnet entwickeln sich in diesen Gedankenszenarien zu einem optimalen Werkzeug, um den Feind durch Sabotage erheblich zu schwächen und zu beeinträchtigen. Physischer oder gar tödlicher Schaden an Menschen soll durch die Wahl dieser Mittel gänzlich vermieden werden.

Neben der Negierung, aber auch der grundsätzlich bejahenden Position zu Cyberwar und Cyberwarfare, existiert aber noch eine deutliche pessimistischere Darstellung, die sich besonders in der US-amerikanischen Debatte festgesetzt zu haben scheint. Führende Militär- und Politikbeobachter prognostizieren dort einen „electronic Pearl Harbor“[23], vor dem es sich unbedingt zu schützen gilt. Cyberwar ist für sie kein zukünftiges Szenario, sondern hat vielmehr bereits angefangen: Stuxnet und die DoS-Angriffe in Estland 2007 werden in diesem Kontext als Vorboten und Beweise eines unter der Oberfläche bereits stattfindenden Cyberkrieges angesehen. Stuxnet hat dabei – laut diesen Meinungen – vor allen Dingen Potenziale aufgezeigt, wie in der Zukunft durch hochfortgeschrittene Würmer oder Malware, auch längerfristige Beeinträchtigungen erzielt werden können. Schreckensszenarien von Angriffen auf kritische Infrastrukturen, die in der Folge ganze Länder funktionsunfähig machen könnten, werden dabei als ultimatives Schreckensszenario immer und immer wieder regelrecht heraufbeschworen. Joseph Nye, ehemaliger stellvertretender US-Verteidigungsminister, äußert sich in diesem Zusammenhang beispielsweise wie folgt:

> „Der Cyberkrieg, auch wenn er erst in den Kinderschuhen zu stecken scheint, ist die dramatischste aller tendenziellen Bedrohungen. Große Staaten mit hoch entwickelten technischen und menschlichen Ressourcen könnten im Prinzip durch Cyber-Angriffe auf militärische und zivile Ziele enorme Störungen und physische Zerstörungen anrichten.“[24]

Ein regelrechtes Cyberaufrüsten scheint daher nur logische Konsequenz zu sein.

---

[19] Vgl. Sandro Gaycken, *Cyberwar: Das Internet als Kriegsschauplatz* (Open Source Verlag 2010), S. 104f.
[20] Vgl. Ronald J. Deibert, *Black Code- Surveillance, Privacy and the Dark Side of the Internet (Signal 2013),* S. 97f.
[21] Vgl Rid, *Cyberwar and Peace – Hacking Can Reduce Real-World Violence*.
[22] Deibert, *Black Code- Surveillance, Privacy and the Dark Side of the Internet,* S. 108.
[23] Diese Metapher ist in der US-amerikanischen Debatte ein beliebtes Stilmittel, um die Gefahren des (vermeintlich) unkontrollierbaren Cyberspace und seiner Cybermittel vor Augen zu führen. Geprägt hat diesen Begriff der ehemalige Anti-Terror Berater des Weißen Hauses Richard A. Clark.
[24] Zitiert nach: Unger, *Cyber Defence – eine nationale Herausforderung*, S. 10.

4. Versuch einer Abwägung

Wie diese unterschiedlichsten Meinungen und Sichtweisen zu den beiden Themen demonstriert haben, ist die Debatte um Cyberwar und Cyberwarfare äußerst lebhaft und von Gegensätzlichkeit geprägt. Allerdings – und dies erscheint im gegenwärtigen Diskurs nicht genügend berücksichtigt zu werden – muss sehr genau zwischen dem tatsächlichen Gefahrenpotential und den Schreckensszenarien von Öffentlichkeit und führenden Militärbeobachtern differenziert werden. Cybergefahren sollten und müssen immer in ihrem unmittelbaren Kontext betrachtet und analysiert werden und daher ist es unerlässlich, die unterschiedlichen Akteure, die an einer solchen Debatte partizipieren, und ihre Interessen zu untersuchen. Dabei gilt es, nicht außer Acht zu lassen, dass seitens Rüstungsfirmen, aber auch Computersicherheitsspezialisten ein großes Interesse besteht, den „Cyberwar-Hype" aufrechtzuerhalten.

> „The rise of cybersecurity as an issue has gone hand in hand with a boom in the number of companies trying to make money from it."[25]

Während der Absatz traditioneller Rüstungsgüter einen signifikanten Einbruch erlebt, sind militärische Mittel des modernen High-Tech-Krieges wie UAVs oder eben auch Cybermittel wie Würmer und Viren stärker nachgefragt denn je. Viele Staaten scheinen sich der Verlockung des vermeintlich „sauberen" Krieges offensichtlich nicht entziehen zu können, zumal dieser im Vergleich zu konventionellen militärischen Aktionen vergleichsweise preiswert ist. Rein logisch betrachtet sind Cyberlösungen (wie z.B. ein Programm wie Stuxnet) – wenngleich sie auch in ihrer Entwicklung einen hohen Ressourcenverbrauch haben – um ein Vielfaches günstiger als die Kosten eines Luftschlages oder der Einsatz von Bodentruppen.[26]
Staaten sind ferner bestrebt, den Kampf um Cybersicherheit nicht zu verschlafen. "Most of the world's armed forces have established, or are in the process of establishing cyber-commandos or cyberwarfare units"[27]. Dabei werden – zum Großteil – aber keineswegs defensive Strukturen und Maßnahmen verstärkt, um kritische Infrastrukturen zum Beispiel effektiver schützen zu können, vielmehr wird in offensive Maßnahmen wie die Entwicklung neuer Stuxnets erheblich investiert.[28] Nach Angaben des früheren NSA-Mitarbeiter Edward Snowden arbeite seine ehemalige Behörde bereits an einem Cyberkrieg-Programm namens "MonsterMind", welche ohne menschliches Zutun auf Angriffe auf Cyberstrukturen reagieren könne.[29] Wie eng Sicherheitsbehörden und Cyberkommandos verzahnt sind wird auch dadurch ersichtlich, dass die NSA und das USA Cyberkommando nicht nur geographisch beide in Fort Meade lokalisiert sind; der Direktor der NSA ist zugleich auch oberster Kommandant des United States Cyber Command (USCYBERCOM). Die Volkrepublik China hingegen steht im Verdacht, seine Cybercommandos in kleinen paramilitärischen Einheiten

[25] Singer / Friedman, *Cybersecurity and Cyberwar : What Everyone Needs to Know*, S. 163.
[26] Vgl. James P. Farewell, Rafal Rohozinski, *Stuxnet and the Future of Cyber War* (Survival, Volume 53, Nr. 1, Februar / März 2011), S. 35.
[27] Ronald Deibert, Rafal Rohozinski, *Liberation vs. Control: The Future of Cyberspace (*Journal of Democracy, Volume 21, Nr. 4 / 2010), S. 49.
[28] Singer / Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, S. 146.
[29] Vgl. Tagesschau, *Neue Enthüllungen durch Edward Snowden „NSA arbeitet an Cyberwar-Programm* (Tagesschau, 14.09.2014, abrufbar unter: http://www.tagesschau.de/ausland/snowden-129.html).

zu organisieren.[30] Über diese Einheiten – so der US-amerikanische Vorwurf – soll großflächige Wirtschaftsspionage durch und über das Cyberspace betrieben werden, der amerikanischen Konzernen erheblichen Schaden zufügen soll. Diese Perzeption, ständig einem Cyberangriff oder Wirtschaftsspionage ausgesetzt zu sein, führt – wie eben beschrieben – vor allen Dingen zum Ausbau offensiver Maßnahmen, die Gefahr eines Cyber-Wettrüstens ist folglich nicht von der Hand zu weisen.

Der Einsatz und die Verwendung von Stuxnet, dessen Implementierung primär auf die Störung des iranischen Atomprogrammes ausgerichtet war, stellt sicherlich ein Novum, eine Zäsur dar, führten doch zwei Staaten – wenn auch nie öffentlich bestätigt – eine Cyberattacke auf Teile der kritischen Infrastruktur eines anderen Staates aus.[31] Zudem – und dies ist ebenso erstaunlich – wurde bei der Entwicklung von Stuxnet auf Codes und Techniken zurückgegriffen, die aus dem Bereich des kriminellen Cyberspace stammen.[32] Die eigentliche Gefahr, die von Stuxnet tatsächlich ausging, muss allerdings deutlich relativiert werden. James Farewell und Rafal Rohozinski beschreiben Stuxnet als einen „Frankenstein patchwork of existing tradecraft“[33], der bei weitem nicht so hochentwickelt und fortschrittlich war, wie dies in der Berichterstattung suggeriert wurde. Dass ein physische Anbringen von Memory Sticks von Nöten war, um Teile des iranischen Atomprogrammes zu infizieren, demonstriert weiterhin, dass der “Faktor Mensch“ auch im Zeitalter des Cyberspaces und der Cyberattacken nicht obsolet geworden ist, sondern ihm immer noch eine entscheidende Rolle zu kommt.

Der Einsatz von Cybermittel muss – und das ist offensichtlich – immer sehr genau abgewogen werden, ist doch die Gefahr eines Bumerang-Effektes nicht auszuschließen: “Any aggressor in cyberspace faces the acute threat of blowback: having techniques replicated and repeated against the aggressor.” [34] Wenn Computerwürmer wie Stuxnet einmal entwickelt und verwendet worden sind, ist es nur eine Frage der Zeit bis auch andere Akteure auf diese Techniken und Entwicklungen zurückgreifen können. So veröffentlichte ein ägyptischer Blogger nur wenige Wochen nach der Entdeckung des Wurmes eine 1:1 Bauanleitung von Stuxnet im Internet.[35] Staaten müssen daher sehr genau kalkulieren, ob der Einsatz von Cybermitteln in einem spezifischen Kontext wirklich sinnvoll ist, oder ob man – in letzter Konsequenz – dem eigenen Gegner so strategische Trümpfe in die Hand spielt, die dieser wiederum gezielt gegen den Angreifer selbst einsetzen könnte.

Bei Cyberattacken ist außerdem die Möglichkeit von Fehlwahrnehmungen- und Einschätzungen eklatant höher als das dies bei Angriffen mit konventionellen Waffensystemen der Fall ist. Die Effekte, die eine großflächige Cyberattacke auf Angreifer und Verteidiger haben kann, sind äußerst schwer einzuschätzen[36]: Cybermittel und dessen Auswirkungen und Folgen sind daher in gewisser Weise unberechenbar und nicht zu

---

[30] Vgl. Petra Kolonko, *Die Cyberkrieger von Schanghai* (FAZ, 20.05.2014, abrufbar unter: http://www.faz.net/aktuell/politik/ausland/asien/amerika-gegen-china-die-cyberkrieger-von-schanghai-12948852.html).

[31] Vgl. Rid, *Cyberwar and Peace – Hacking Can Reduce Real-World Violence*.

[32] Farwell / Rohozinski, *Stuxnet and the Future of Cyberwar*, S. 26.

[33] Ebd., S. 25.

[34] Brandon Valeriano / Ryan Maness, *The Fog of Cyberwar – Why the Threat Doesn't Live Up to the Hype (Foreign Affairs, Snapshots, November 2012, abrufbar unter: http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar).*

[35] Vgl. Singer / Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, S. 158.

[36] Vgl. Gompert / Libicki: *Cyber Warfare and Sino-American Crisis Instability*, S. 13.

kalkulieren. So ist es möglich, dass ein Cyberangriff von der angegriffenen Seite gar nicht erst festgestellt wird. Jedoch besteht genauso gut die Möglichkeit und Gefahr, dass der Versuch der Cyberspionage – je nach Ausführung und Technik – als militärisch intendierter Erstschlag interpretiert werden kann.[37]
Zu dieser Problematik der Unberechenbarkeit bleibt eine weitere Frage ebenso unbeantwortet. Denn die verantwortlichen Personen für eine Cyberoperation oder einen Cyberattacke ausfindig zu machen, kann getrost als diffizile Aufgabe bezeichnet werden. Wie bei dem DoS-Angriffe auf Estland 2007 kann über die angreifende Partei und Motivation häufig nur spekuliert werden.

> „Difficulty in identifying a cyber attacker presents multiple headaches for responding. […] It is not clear what degree of certainty in identification is required to justify a response. Launching a response against an innocent party would qualify as an act of aggression, not self defence."[38]

Aus diesem Grund ist es heikel für einen betroffenen Staat eine angemessene Antwort auf einen Cyberangriff zu finden, denn Hacker sind clever genug, ihre Spuren ausreichend zu verwischen oder Daten entsprechend zu manipulieren. Inwieweit diese Fragen durch geltendes Völkerrecht bereits abgedeckt sind, darf weiterhin hinterfragt werden. Denn wer soll für einen solchen Angriff zur Verantwortung gezogen werden: Der Auftraggeber der Attacke oder die Vollstrecker bzw. Entwickler dieser Technologien?

5. Abschließende Bemerkungen

Trotz des Gefahrenpotenzials, welches zweifelsohne von dem Einsatz von Cybermitteln ausgehen kann, ist es äußerst unwahrscheinlich, dass Staaten zukünftig auf die Möglichkeiten der Cyberkriegsführung verzichten und all ihre Bemühungen und Investitionen um den Ausbau von Cybereinheiten verringern werden. Dies mag umso erstaunlicher anmuten, als dass das Potenzial für staatlich nicht autorisierte Cyberattacken nicht ignoriert werden kann.[39]
Gleichwohl ist das dystopische Schreckensszenario eines globalen Cyberkrieges noch keine Realität, wenngleich Stuxnet, Flame und die DoS-Angriffe auf Estland indiziert haben, welche Möglichkeiten Cybermittel besitzen können. Auch wenn die gegenwärtige Gefahr dieser Würmer, Viren und Attacken nur limitiert zu sein scheint, demonstrieren sie sehr genau, dass mit der Unberechenbarkeit und dem Einfallsreichtum des menschlichen Individuums diese Barrieren und Limitationen bald auch schon fallen könnten. Mit diesem Wissen sollte es vor allen Dingen Aufgabe von Staaten und Regierungen sein, den unangenehmen Begleiterscheinungen dieser Cybermittel Einhalt zu bieten, indem Möglichkeiten des Cyberwarfares, aber auch eine realistische Einschätzung zum Thema Cyberwar, ausgewogen diskutiert werden. Für eine solche Aufarbeitung fehlt Politikern aber schlichtweg die technische Expertise, um die Situation sachlich und fachlich diskutieren und beurteilen zu können.
Wir befinden uns auf der Schwelle zu einem umfangreichen Transformationsprozess der Kriegsführung, einer nie dagewesenen Digitalisierung der Kriegsführung, die Fragen nach der

[37] Vgl. ebd.
[38]. Farwell / Rohozinski, *Stuxnet and the Future of Cyberwar*, S. 34f.
[39] Vgl. Gompert/Libicki, *Cyber Warfare and Sino-American Crisis Instability*, S. 14.

Konzeption und Rechtmäßigkeit dieser neuen Methoden aufwirft. Diese Fragestellungen umfassen dabei unterschiedlichste Dimensionen: Wie sind Cyberattacken völkerrechtlich zu fassen und zu legitimieren? Unterminieren Cyberwaffen nicht in gewisser Weise unsere konventionelle Vorstellung von Krieg, Kriegsführung, Gewalt und Angriff? Auf all diese Fragen gibt es keine befriedigenden Antworten, gleichsam wird die Entwicklung von allen möglichen Cyberwaffen vorangetrieben.
Daher liegt es auch in unser aller Verantwortung, uns mit den Themen von Cybersecurity und Cyberwarfare kritisch auseinanderzusetzen, auch um das potenzielle Szenario von zukünftigen Cyberwars entgegenzuwirken und zu verhindern. In unserer Funktion als Sozialwissenschaftler müssen wir daher sehr genau die unterschiedlichen Cyberwar und Cyberwarfare-Narrative auf ihren Wahrheitsgehalt differenziert prüfen und untersuchen, als Stimme der Vernunft in diesen Zeiten fungieren. Dies ist insbesondere aufgrund der herrschenden Klandestinität und Intransparenz, was die realen und zukünftigen Möglichkeiten und Gefahren von Cybermitteln betrifft, ein schwieriger, aber nicht unmöglicher Vorgang. Gleichwohl dürfen wir nicht in eine Art Cyberpanik und Paranoia verfallen, die eine weitere Beschneidung von Freiheiten im Netz zur Folge haben wird.

Weiterführende und vertiefende Literatur

Thomas Rid, *Cyberwar Will Not Take Place*, Oxford University Press, 2013.

Peter W. Singer / Allan Friedmann, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.

Edward F. Halpin, *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave, 2006.