Möglichkeiten und Grenzen zur Bestimmung von Cyberwaffen

Thomas Reinhold[1]

Abstract: Seit der Entdeckung der Schadsoftware Stuxnet ist der Cyberspace in den Fokus der internationalen Sicherheitspolitik gerückt. Während Staaten zunehmend die neue Domäne in ihre Sicherheits- und Militärdoktrinen aufnehmen, verdeutlichen Vorkommnisse wie der Sony-Hack oder die Beschädigung eines deutschen Stahlwerks die komplexen Abhängigkeiten von IT-Systemen und deren Verwundbarkeiten. Internationale Bemühungen um die Etablierung verbindlicher Regelungen für das staatliche und militärische Agieren im Cyberspace werden durch ein fehlendes gemeinschaftlich akzeptiertes Verständnis des Themas oder der Definition von Begrifflichkeiten erschwert. Insbesondere das Konzept der "Cyberwaffe" und eine tragfähige und im Kontext international verpflichtender Konventionen belastbare Eingrenzung dieses Begriffs ist dabei für Abrüstungs- und Rüstungskontrollabkommen von zentraler Bedeutung. Eine Gegenüberstellung unterschiedlicher, sowohl generalisierender als auch situationsbezogener Definitionsansätze von Cyberwaffen verdeutlicht dabei die verschiedenen zu integrierenden Betrachtungsebenen. Die im Gegensatz zu konventionellen Waffentechnologien spezifischen Eigenschaften von Software zeigen aber auch die Schwierigkeiten und Grenzen derartiger Ansätze auf.

Keywords: Cyberpeace, Cyberwar, Cyberwaffe, Abrüstung, Rüstungskontrolle

Einleitung

Mit der Entdeckung der Schadsoftware Stuxnet im Juni 2010 [LANGNER2013] ist der Cyberspace in den Fokus der internationalen Sicherheitspolitik gerückt. Die Diskussionen um die Sabotage der iranischen Atomanreicherungsanlage haben dabei ein wichtiges Licht auf diese, in internationalen Debatten lange Zeit vernachlässigte Domäne geworfen, die zunehmend auch in Sicherheits- und Militärdoktrinen Beachtung findet. Eine Studie des Center for Strategic and International Studies [LEWIS2011] stellte bereits 2011 fest, dass 33 Staaten den Cyberspace als weitere Domäne in ihre militärische Planung integriert haben. Die strategische Ausrichtung umfasst dabei neben den defensiven Aspekten und dem Schutz eigener Infrastrukturen zum Teil auch explizit offensive Maßnahmen wie die Entwicklung von Computer Network Operations (CNO) für den Zugriff auf fremde IT-Systeme oder die gezielte Identifikation und Analyse potentieller Ziele im Cyberspace, wie im Falle der „Presidential policy directive PPD-20" des US-Präsidenten vom Oktober 2012 [USA-GOV2012]. Einer aktualisierten

[1] Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, Beim Schlump 83 20144 Hamburg, reinhold@ifsh.de

Studie des UN Institute for Disarmament Research [UNIDIR2013] zufolge hat sich die Zahl der Staaten mit militärischen Cyber-Programmen seither auf 40 Staaten erhöht, wovon zehn Staaten eine offensive Cyber-Strategie verfolgen und an der Entwicklung offensiv wirksamer Cybermittel arbeiten. Auf der anderen Seiten haben Stuxnet und weitere Vorfälle der vergangenen Jahre die komplexen und umfassenden Abhängigkeiten von IT-Infrastrukturen und Computersystemen und die unklaren Gefährdungen insbesondere kritischer Infrastrukturen verdeutlicht. Beispiele dafür sind die Hacking-Attacke gegen das Netzwerk von Sony-Pictures-Entertainment von 2014 [FBI2014], gegen den französischen Fernsehsender TV5 [HEISE2015] oder die im BSI-Lagebericht von 2014 beschriebene Sabotage eines deutschen Stahlwerks [BSI2014].

In den internationalen politischen Beziehungen haben diese Aspekte zu Verunsicherungen geführt und an historischen Entwicklungen wie dem kalten Krieg, Rüstungswettläufen in der atomaren, biologischen und chemischen Kampfführung oder die Debatten um die Aufrüstung des Weltalls gerührt. Aus Friedens- und Sicherheitspolitischer Sicht wurden damit viele Fragen zum Cyberspace aufgeworfen die bis heute kaum geklärt sind. Obgleich entscheidende internationale Organisationen wie die UN oder die OECD Expertengruppen einberufen und Gremien gegründet haben um sich diesem Problemen zu widmen, werden internationale Debatten oft durch ein fehlendes gemeinschaftlich akzeptiertes Verständnis des Themas oder der Definition von Begrifflichkeiten erschwert. Dazu zählt die Frage nach einer genauen Abgrenzung des Raumes “Cyberspace” und den Aspekten der nationalstaatlichen Souveränität in dieser Domäne ebenso, wie die Definition von Cyberattacken in Verbindung mit der Frage nach der exakten Ausprägung von Cyberangriffen, die als Attacken im Sinne des Völkerrechts verstanden werden können. Exemplarisch dafür steht ein gemeinsamer erster Entwurf der russischen und chinesischen Regierung für eine Cyberkonvention [RU2011]. Darin ist primär die Sprache von “Informationssicherheit” als wesentliches Ziel einer solchen Konvention, die neben der Unverletzlichkeit nationaler IT-Infrastrukturen auch die nationale Souveränität und Kontrolle über die in nationalen IT-Systemen übertragenen und gespeicherten Informationen umfasst. Dieser Ansatz kollidiert dabei mit den Auffassungen von Staaten, die demokratische Werte wie das Recht auf Meinungsfreiheit durch solche Kontrollmöglichkeiten bedroht sehen. Weitere Versuche sich der der gemeinsamen Definitionsfindung zu widmen, wie das Tallinn-Manual [NATO2013] des NATO-Exzellenzzentrums CCDCOE, haben dabei deutlich gemacht, dass etablierte Konzepte des Völkerrechts oder Analogien zu den Diskussionen um klassische militärische Mittel aufgrund spezifischer Eigenschaften des Cyberspace und von Software nur eingeschränkt möglich sind und an ihre Grenzen stoßen.

Normen und Definitionen für den Cyberspace

Die Bemühungen um klare Definitionen stellen daher eines der wichtigsten Grundlagen für die weitere friedliche Ausgestaltung des Cyberspace dar. Sie bilden die Basis für die Entwicklung verbindlicher Normen für staatliches und militärisches Agieren im Cyberspace und die Festschreibung derartiger Regelungen in Form internationaler

Konventionen nach dem Vorbild des Übereinkommen über das Verbot biologischer Waffen [UN1972] oder dem Übereinkommen über das Verbot chemischer Waffen [UN1993]. Derartige Konventionen können in der Vereinbarung von Rüstungsbegrenzenden Maßnahmen (Abrüstung) oder in Übereinkommen über die Kontrolle der Herstellung, des Handels und der Verbreitung von Waffen oder kritischen Technologien und Waffenfähigen Materialien bestehen (Rüstungs- und Exportkontrolle). Insbesondere Abrüstungsabkommen werden in aller Regel gestützt durch die Vereinbarung von Verifikationsregimen, deren Aufgabe unter anderem in der gegenseitigen Überwachung bei der Einhaltung der vereinbarten Regelungen besteht. Solche Verifikationsregime, wie beispielsweise der Atomwaffensperrvertrag (Treaty on the Non-Proliferation of Nuclear Weapons [NPT1968]), beruhen dabei oft auf der Festsetzung von Höchstgrenzen für spezifische Schlüsseltechnologien oder Waffenbestandteile, die durch Inspektionen überwacht werden können. Der Versuch einen solchen Ansatz auf den Cyberspace zu übertragen gestaltet sich besonders aufgrund der schwierigen Definition des Begriffs "Cyberwaffe" und den, im Gegensatz zu konventionellen Waffen spezifischen Eigenschaften von Software als immaterielle, virtuelle und beliebig duplizierbare Produkte problematisch. Als "Cyberwaffe" wird in aller Regel Software jeglicher Art verstanden, die aufgrund ihrer spezifischen Konstruktion darauf angelegt ist, in einem IT-System oder in angeschlossenen Systemen reguläre Abläufe zu stören oder diese über Modifikationen zu zerstören. Diese Betrachtungsweise erfasst jedoch wesentliche Aspekte einer völkerrechtlich hinreichenden Definition einer Waffe, wie den möglichen Zerstörungsumfang oder die Intention eines Angreifers nicht. Zum anderen schließt sie große Bereiche von Software ein, die im zivilen und eindeutig nicht-militärischen Bereich Anwendung finden. Ein engere Umgrenzung des Begriffs ist daher geboten.

Definitionsversuche zu Cyberwaffen

Die Autoren der OECD-Studie "Reducing Systemic Cybersecurity Risk" [SOMMER2010] widmen sich der Frage nach der Definition von Cyberwaffen unter dem Blickwinkel der Eigenschaften klassischer Waffen: "*There is an important distinction between something that causes unpleasant or even deadly effects and a weapon. A weapon is "directed force" – its release can be controlled, there is a reasonable forecast of the effects it will have, and it will not damage the user, his friends or innocent third parties"*. Um insbesondere die bei Cyberwaffen problematische zeitnahe Zuordnung eines Angriffs - das sogenannte Attributionsproblem - aufzugreifen schlagen die Autoren bei der Bewertung von Schadsoftware weitere Bewertungsaspekte vor und empfehlen eine Analyse anhand der folgenden Kriterien:

- *Is this something whose targeting and impact can be controlled (is there a risk of friendly fire?)*
- *What success rate can be expected in terms of targets?*
- *Is there any collateral damage?*
- *What resources and skills are required?*

- *How much inside knowledge and/or inside access of target is required? How easy is this to achieve?*
- *Can the weapon be detected before or during deployment?*
- *Can a perpetrator be detected during or after deployment?*
- *What are the actual effects and how long do they last?*
- *How long can an attack be carried out before it is thwarted by counter-technology?*
- *How long can an attack be carried out before perpetrators are identified?*

Die Autoren definieren damit ein wirksames und auf Software übertragbares Raster anhand dessen sich Schadsoftware auf Basis der spezifischen technischen Umsetzung voneinander abgrenzen lässt. Allerdings nehmen die Autoren bei ihrer Aufstellung der Bewertungsmaßstäbe keine Gewichtungen der einzelnen Kriterien vor und vermeiden eine klare Aussage über die Unterscheidung zwischen krimineller Schadsoftware und Cyberwaffen. Die Kriterien sollen in erster Linie als Hilfsmittel dienen um konkrete Vorfälle zu bewerten. Daher eignen sie sich insbesondere um die Fülle an verfügbarer Schadsoftware bei der Diskussion um Cyberwaffen einzugrenzen: "*On this basis it will be seen that the most common forms of virus (..) fail as credible cyberweapons, because they are relatively difficult to control. However a targeted DDoS is a likely cyberweapon.*"

Ein weiterer Versuch der Begriffsfindung besteht in der Betrachtung des tatsächlich bewirkten Schadens einer Schadsoftware. Dieser kann aufgrund der starken Vernetzung sowie der komplexen und verzögerten Wechselwirkungen von IT-Systemen unter Umständen beträchtlich von der intendierten Wirkung abweichen, wie unzählige Vorfälle der vergangenen Jahre gezeigt haben. So wurde die Schadsoftware Stuxnet beispielsweise auf sehr viel mehr Rechner weltweit entdeckt als nur auf den IT-Systemen der Anreicherungsanlage in Natanz, die Stuxnet sabotieren sollte. Den Ansatz Schadsoftware über die tatsächlich ausgelöste Wirkung zu kategorisieren verfolgen die Autoren der Studie "On the Spectrum of Cyberspace Operations" [BROWN2012]. Sie bewerten den beabsichtigten und unbeabsichtigten Schaden gemeinsam innerhalb eines Spektrums, das von dem reinen Eindringen und nicht-invasiven Agierens in fremden Computersystemen ("*enabling operations*") über die zeitweise Unterbrechung von Diensten ("*cyber disruption*") bis hin zur tatsächlichen Schädigung von Dingen oder Personen reicht ("*cyber attacks*"). Aus Sicht der Autoren entsprechen dabei erst Varianten von Schadsoftware, deren Auswirkung in letztere Kategorie fallen, dem Konzept einer Waffe beziehungsweise eines bewaffneten Angriff im Sinne des Völkerrechts nach der UN Charta Art. 51 [UN1945]. Auch dieser explizit situationsbezogene Ansatz eignet sich damit eher für die Bewertung konkreter Vorfälle, insbesondere für die Abwägung nach angemessenen Reaktionen eines angegriffenen Staates, wie für die im Recht auf Selbstverteidigung vorgesehene Maßgabe der Proportionalität von Maßnahmen. Obgleich für eine Definition im Rahmen internationalen Konventionen eher die Betrachtung der strukturell intendierten Wirkung einer Schadsoftware nötig ist, so bietet sich die Kontinuums-Klassifikation doch an um große Teil der "üblichen" Hacking-Attacken wie dem Einbruch in IT-Systeme und dem

Diebstahl von Daten für die Begriffsfindung auszuschließen und in den Bereich der nationalen und internationalen Strafverfolgung zu verweisen.

Eine dritte Studie "Cyber-weapons: legal and strategic aspects" [MELE2013] betrachtet die Definition einer Cyberwaffe unter rein konzeptionellen Aspekten: "*a weapon can be also an abstract concept thereby not necessarily a material one, as international and domestic legislation have considered it up to now*". Damit berücksichtigt der Autor den Umstand, dass sich Schadsoftware, die für kriminelle Zwecke benutzt wird, von einem technischen Standpunkt aus betrachtet kaum von Schadsoftware unterscheiden muss, deren Ziel die Zerstörung eines IT-Systems ist. Beide Varianten benötigen Mechanismen um in ihr Zielsystem einzudringen, sich vor Abwehrmechanismen zu schützen und ihren eigentlichen Schadmechanismus auszuführen. Ob dieser im Entwenden von Daten oder dem vollständigen Löschen eines IT-Systems besteht liegt dabei primär in der Intention des Angreifers und weniger in technischen Spezifika der Schadsoftware. Der Autor schlägt für die Eingrenzung einer Schadsoftware als Cyberwaffe daher die Berücksichtigung juristischer und strategischer Dimensionen vor. Diese umfassen den Anwendungskontext und den Zweck eines Schadsoftware-Einsatzes, sowie den beabsichtigten Schaden und die konkrete absichtsvolle Auswahl eines strategisch relevanten Ziels: "*[a cyberweapon is] a part of equipment, a device or any set of computer instructions used in a conflict among actors, both National and non-National, with the purpose of causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject (..) with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage.*" Ein solcher Ansatz, der vor allem die Bewertung eines Vorfalls, des vermuteten Angreifers und dessen Intentionen anstelle des tatsächlichen Geschehens und reeller Schäden in den Fokus rückt, entspricht damit in hohem Maße dem allgemeinen Umgang mit Cybervorfällen durch staatliche Institutionen. Dies wird exemplarisch deutlich am Beispiel der Hacking-Attacke gegen das Netzwerks des in den USA ansässigen Unternehmens Sony-Picture-Entertainment [FBI2014]. Trotz zweifelhafter offizieller Beweise für die Herkunft der Angreifer - mutmaßlich militärische Einheiten aus Nord-Korea - und geringer nachgewiesener Schäden - Diebstahl von Daten - wurde der Vorfall durch die US-Regierung als Bedrohung ihrer inneren Sicherheit gewertet und ausgewählte nordkoreanische Unternehmen und Personen umgehend mit wirtschaftlichen Sanktion belegt [USTREASURY2015].

Eines der hervorgehobenen Bewertungskriterien des konzeptionellen Ansatzes betrifft die gezielte Entwicklung von Cyberwaffen für konkret ausgewählte strategisch relevante Ziele. Mit Blick auf den Aufwand eines solchen Vorhabens kommt der Autor hinsichtlich der weltweiten Verfügbarkeit von Cyberwaffen zu folgender Schlußfolgerung: "*Summarizing these observations, it is possible to understand how the creation and the employment of cyber-weapons require superior intelligence information, time, workforce and testing resources for their creation (..) and ensuring the possibility to hit targets often unreachable by other types of attacks (..) The high costs, the risk*

variables for their creation and efficiency, as well as the "limited" and anyway temporary results, lead to believe that currently research and development activities in the field of cyber-weapons are strategically unprofitable, unless an escalation takes place (..) in the power these software have to increase the damaging level and/or to make their effects last as long as possible".

Die Gegenüberstellung der unterschiedlichen Herangehensweisen verdeutlicht die unterschiedlichen Betrachtungsebenen als Klassifikationsmöglichkeiten von Cyberwaffen, von der Bewertung der technischen Eigenschaften einer Software, über den tatsächlichen Schaden bis zum konzeptionellen und strategisch geplanten Zweck der Software. Zusammengefasst ergeben diese Sichtweisen die folgenden Fragen:

- Wie ist die Software exakt technisch gestaltet
- Wofür ist die Software strategisch gedacht
- Wogegen wurde die Software eingesetzt
- Was ist der tatsächlich verursachte Schaden am Ziel und darüber hinaus

Die drei vorgestellten Ansätze verdeutlichen, dass Cyberwaffen trotz spezifischer Eigenschaften, die sie von bisherigen Waffen unterscheiden und auf die im folgenden noch näher eingegangen wird, mit Hilfe etablierter Konzepte für die Kategorisierung klassischer Waffen betrachtet werden können. Damit können diese eine wichtige Grundlage für die Entwicklung von Cyberkonventionen und Abkommen bilden. Dies gilt insbesondere dann, wenn weniger die konkrete technische Ausprägung als vielmehr der beabsichtigte Schaden und der strategische Anwendungszweck im Mittelpunkt stehen. Darüber hinaus zeigen die Ansätze, welche Formen von Schadsoftware vermutlich nicht als Waffe im Sinne des Völkerrechts gelten können, selbst wenn sie im Einzelfall Schäden anrichten. Sie dienen damit der wichtigen Unterscheidung zwischen kriminellem Handeln, dem mit Mitteln der Strafverfolgung begegnet werden kann, und staatlich militärischen Aktivitäten, die nur auf der Ebene von verbindlichen bilateralen oder internationalen Vereinbarungen geregelt werden können.

Das Wassenaar-Abkommen als erster Schritt einer Cyberwaffen-Konvention

Ein erster Ansatz Cyberwaffen im Rahmen einer internationalen Vereinbahrung zu erfassen und deren Verbreitung zu regulieren wurde durch eine Ergänzung des "Wassenaar-Abkommens für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Güter und Technologien" [WASSENAAR1995] unternommen. Dieses, seit 1996 bestehende Abkommen dient der Aufgabe innerhalb der Gruppe von Mitgliedsstaaten Transparenz über den Export mit kritischen und waffenfähigen Ressourcen und Schlüsseltechnologien zu schaffen. Die Wassenaar-Vereinbarungen enthalten jedoch keine Übereinkünfte zu Rüstungsbegrenzenden Maßnahmen und tragen damit zwar den Charakter der Exportkontrolle, nicht jedoch der Abrüstung. Ende 2013 wurde die Liste der zu kontrollierenden Technologie um

"*intrusion software*" erweitert [WASSENAAR2013], mit folgender Definition:

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network capable device, and performing any of the following:

a) *The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or*
b) *The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.*

Mit Blick auf die drei vorgestellten Klassifikationsansätze fällt auf, dass in der Wassenaar-Definition weder eine nähere Einschränkung auf einen strukturell intendierten Schaden der Software noch deren strategischer Einsatzzweck vorgenommen wird. Ausschließlich die technologisch bereitgestellten Fähigkeiten zum Stören oder Zerstören sowie zur Extraktion von Daten aus IT-Systemen gelten als hinreichende Abgrenzung. Diese Definition ist sehr weit gefasst und überläßt den Mitgliedsstaaten, in deren Verantwortung es liegt Exportbestimmung individuell in nationalem Recht zu verankern, einen breiten Interpretations- und Handlungsspielraum. Für eine internationale Konvention, die über den Kreis der gegenwärtig 41 Mitgliedsstaaten des Wassenaar-Abkommens hinaus, geht wird sich eine solch allgemeine Definition nicht durchsetzen lassen, da sie keine einheitliche Bewertungsgrundlage schafft und so die Vergleichbarkeit von nationalen Verfahrensstandards erschwert.

Erschwerende Spezifika von Schadsoftware

Neben den erläuterten Schwierigkeiten bei der Abgrenzung von Cyberwaffen existieren weitere Rahmenbedingungen die im Vergleich zu konventionellen waffenfähigen Technologien für Schadsoftware einzigartig sind und bei der Definition von Cyberwaffen berücksichtigt werden müssen. Dies betrifft zum einen die fehlende Materialität und die beliebige Dublizierbarkeit von Software, die jegliche effektive Kontrolle von Schadsoftware anhand der Begrenzung des Umfangs von Waffen-Arsenalen oder deren geographischer Lokalisierung verhindert. Diese Maßnahmen sind für klassische Nichtverbreitungs-Verträge sowie für die Nachverfolgbarkeit des Handels mit kritischen Technologien maßgeblich und wichtige Grundlage für Abrüstungs- und Friedensinitiativen. Entsprechende Vereinbarungen wie demilitarisierte Zonen oder die Beschränkung auf Maximalmengen bestimmter Cyberwaffen scheiden daher aus. Ein weiteres Problem bei der Klassifikation einer konkreten Software besteht in der Abgrenzung ihres Zwecks zwischen ausschließlich defensiven und potentiell offensiven Fähigkeiten. Während defensiv orientierte Maßnahmen völkerrechtlich eher unstrittig sind, ist die Abgrenzung defensiv-offensiv für Software schwer vorzunehmen. IT-Systeme effektiv auf Schwächen zu testen umfasst beispielsweise die Entwicklung und den Einsatz von Software für sogenannte Penetrations-Tests, bei denen Angriffe auf eigene Systeme gezielt durchgeführt werden um Schwachstellen zu entdecken, zu beheben und geeignete Schutzmaßnahmen zu etablieren. Derartige Penetrations-Test

können jedoch beispielsweise nicht nur gegen eigene IT-Systeme eingesetzt werden und fallen damit - je nach Interpretation des regulierenden Staates - unter Umständen bereits in die Kategorie der "*intrusion software*" der Wassenaar-Exportkontrollbeschränkungen. Die Regelungen des in Deutschland für die Kontrolle der Wassenaar-Bestimmungen zuständigen Bundesamtes für Wirtschaft und Ausfuhrkontrolle [BAFA2014] folgen einer solchen Interpretation und sehen gegenwärtig die Pflicht für Exportgenehmigungen für einige spezifische Exportländer vor. Das Wassenaar-Abkommen verdeutlicht indes ein weiteres Abgrenzungsproblem bei Schadsoftware. Es wurde insbesondere für die Kontrolle von kritischen Technologien und Gütern geschaffen, die sowohl zivilen als auch militärischen Zwecken dienen können, um aufgrund dieses sogenannten Dual-Use-Charakters im Einzelfall über Exportbeschränkungen entscheiden zu können. Eine solche Entscheidung ist für Software ist jedoch nur schwer vorzunehmen, da wie dargelegt maßgeblich die Intention des Anwenders über die Wirkung des Einsatzes einer Software entscheidet und nicht primär deren technisches Potential. Ein weiteres Problem besteht in der Kontrolle der Verbreitung von Sicherheitslücken in IT-Systemen, die meist den Grundstein einer Schadsoftware bilden und mit Hilfe dessen eine Software Sicherheitsmechanismen umgehen und sich Zutritt zu geschützten IT-Systemen verschaffen kann. Derartige Sicherheitslücken für populäre Software haben teilweise einen hohen ökonomischen Wert und es ist oft lukrativer mit entdeckten Schwächen zu handeln als diese an den Hersteller der Software für eine Fehlerbehebung zu melden. Darüber hinaus bedeutet die Entdeckung schwerwiegender Sicherheitslücken in populärer Software oft einen Image-Schaden für den Herstellers weshalb auch seitens der Unternehmen Schwächen in ihren Produkten möglicherweise eher verschwiegen als veröffentlicht und mit Aktualisierungen behoben werden. Aus diesem Grund ist der Markt des "waffenfähigen Materials" für Cyberwaffen schwer zu überschauen oder zu kontrollieren. Eine belastbare und international als zuverlässig anerkannte Definition von Cyberwaffen muss daher eine verbindliche Kontrolle der Verbreitung von Sicherheitslücken, wie es mit dem Wassenaar-Abkommen in einem ersten Schritt unternommen wurde umfassen.

Fazit

Die vorgestellten Klassifikationskonzepte verdeutlichen, dass auch das Konzept von immateriellen Waffen im virtuellen Cyberspace mit Hilfe etablierter Vorgehensweisen der Bewertung von militärischen Technologien erfassbar sind. Die für effektive und konkrete Abkommen notwendigen Regelungen und Definitionsfeinheiten werden aber gegenwärtig zum einen noch durch unterschiedliche Herangehensweisen und zum anderen durch die für Software einzigartigen Eigenschaften behindert. Ein tragfähige und im Kontext international verpflichtender Konventionen belastbare und sinnvolle Eingrenzung des Begriffs Cyberwaffe muss daher zum einen diese verschiedenen Betrachtungswinkel integrieren. Zum anderen verdeutlichen der ausgeprägte Dual-Use-Charakter und die ambivalente Abgrenzung von defensiven und offensiven Fähigkeiten einer Software, dass es für Cyberwaffen mehr als für bisherige klassische Waffen-Technologien auf die Einzelfallprüfung ankommen wird. Die erweiterten Regelungen

des Wassenaar-Abkommens können hier einen ersten sinnvollen Versuch darstellen über den sich Staaten zu weiteren und weitreichenderen Schritten auf dem Weg einer Kontrolle und Eingrenzung der militärischen Nutzung des Cyberspace austauschen und verpflichten könnten.

Literaturverzeichnis

[BAFA2014] Bundesamt für Wirtschaft und Ausfuhrkontrolle, "Ausfuhrliste B, National erfasste Güter", 2014

[BROWN2012] Brown, G. D. & Tullos, O. W., "On the Spectrum of Cyberspace Operations", Small Wars Journal, 2012

[BSI2014] Bundesamt für Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2014", Bonn, 2014

[FBI2014] Federal Bureau of Investigation, "Update on Sony Investigation", Washington, 2014

[HEISE2015] Heise.de, "Islamisten hacken TV5", http://heise.de/-2597578, 2015

[LANGNER2013] Langner, R. „To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve", Hamburg, 2013

[LEWIS2011] Lewis, J. A. & Timlin, K., Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization, Center for Strategic and International Studies, 2011

[MELE2013] Mele, S., "Cyber-weapons: legal and strategic aspects", Italian Institute of Strategic Studies "Niccolò Machiavelli", 2013

[NATO2013] NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), „The Tallinn Manual on the International Law Applicable to Cyber Warfare", Tallinn, 2013

[NPT1968] Treaty on the Non-Proliferation of Nuclear Weapons, 1968

[RU2011] Ministry of Foreign Affairs of Russia "Convention on international information security", 2011

[SOMMER2010] Sommer, P. und Brown, I., „OECD Study - Reducing Systemic Cybersecurity Risk OECD/IFP Project on Future Global Shocks", 2010

[UN1945] Vereinte Nationen, „Charta der Vereinten Nationen und Statut des Internationalen Gerichtshofs", 1945

[UN1972] Vereinte Nationen, "Übereinkommen über das Verbot der Entwicklung, Herstellung und Lagerung bakteriologischer (biologischer) Waffen und von Toxinwaffen sowie über die Vernichtung solcher Waffen", 1972

[UN1993] Vereinte Nationen, "Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen", 1993

[UNIDIR2013] UNIDIR, United Nations Institute for Disarmament Research, „The Cyber Index - International Security Trends and Realities", Genf, 2013

[USA-GOV2012] US-Regierung, Barack Obama, „Presidential policy directive / PPD-20", Washington, 2012

[USTREASURY2015] US Department of treasury, “Treasury Imposes Sanctions Against the Government of The Democratic People’s Republic Of Korea”, 2015

[WASSENAAR1995] “The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies”, Wassenaar, 1995

[WASSENAAR2013] “The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies - List of dual-use goods and technologies and munitions list”, 2013