## Ausarbeitung

# Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (*Cyber Warfare*)

[redacted]

**Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (*Cyber Warfare*)**

Verfasser/in: [redacted]

Aktenzeichen: WD 2 - 3000 - 038/15
Abschluss der Arbeit: 24. Februar 2015
Fachbereich: WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe
Telefon: [redacted]

## Inhaltsverzeichnis

## 1. Einführung

Spätestens seit den Diskussionen um den Computerwurm *Stuxnet* sind staatliche und nichtstaatliche „Cyber-Attacken“ in aller Munde; neue Beispiele erobern die Schlagzeilen seitdem in kurzer Folge. So fand eine renommierte russische IT-Firma erst kürzlich Spähprogramme auf Festplatten diverser Computerhersteller in etwa 30 Staaten (darunter Iran, Russland, Pakistan, Afghanistan, China, Mali, Syrien, Jemen und Algerien). Diese Programme hätten erhebliche Ähnlichkeit mit *Stuxnet*; die infizierten Rechner seien teilweise von staatlichen und militaristischen Einrichtungen verwendet worden.[1]

Verbunden mit solchen Meldungen ist regelmäßig die Frage nach Herkunft und (staatlicher) Zurechenbarkeit der Angriffe. Rechtlich stellt sich insbesondere die Frage, inwiefern **Regeln des herkömmlichen humanitären Völkerrechts** auch **auf die digitale Kampfführung im Cyber-Raum übertragbar** sind, wo Anpassungen vorgenommen worden sind oder nach Einschätzung der Fachwelt notwendig wären.[2] Das folgende Gutachten nimmt dabei insbesondere zu Fragen der **Kennzeichnungspflicht von Kombattanten** (dazu 2.), zur **Attribution / Zurechnung von Cyber-Attacken** (dazu 3.) sowie zur **Abgrenzung zwischen Perfidie (Heimtücke) und Kriegslist** (dazu 4.) Stellung.

Zu den rechtlich noch nicht vollständig geklärten Problemen gehören u. a. die Frage, inwiefern sich das humanitär-völkerrechtliche **Unterscheidungsgebot** auf die digitale Kriegsführung übertragen lässt[3], wie mit dem Einsatz **ziviler Akteure** im Cyber-Konflikt umzugehen ist[4] und wann eine Cyber-Attacke die Schwelle eines **bewaffneten Konflikts** überschreitet.[5]

---

1 Siehe hierzu *Menn*, Joseph, *Russian researchers expose breakthrough U.S. spying program*, bei Reuters (US-Edition), 16.02.2015, http://www.reuters.com/article/2015/02/16/us-usa-cyberspying-idUSKBN0LK1QV20150216 (letzter Zugriff: 18.02.2015).

2 Überblicksartig *Lin, Herbert*, *Cyber confict and international humanitarian law*, in: International Review of the Red Cross, Band 94 (2012), S. 515–531; *Stadlmeier, Sigmar/Unger, Walter J.*, Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht, in: *Schmalenbach, Kirsten* (Hrsg.), Aktuelle Herausforderungen des Völkerrechts, Frankfurt/Main: Peter Lang (2012), S. 63–80; *Döge, Jenny, Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime*, Archiv des Völkerrechts, Band 48 (2010), S. 486–501.

3 Siehe zu dieser Frage etwa *Ziolkowski, Katharina*, Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen: zum „virtuellen Raum“ des Internet und dem Schutzstandard der vor 30 Jahren in Kraft getretenen Protokolle“, in: Humanitäres Völkerrecht – Informationsschriften, 2008, S. 202–213, S. 210 ff; *Theeuwen, Wieteke, Cyberspace Operations in International Armed Conflict: The Principles of Distinction and Proportionality in Relation to Military Objects*, in: Humanitäres Völkerrecht – Informationsschriften, 2013, S. 188–194; *Schmitt, Michael N.* (Hrsg.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge/New York: Cambridge University Press (2013), Regeln 31–40 (S. 110 ff.), 43 (S. 144 ff.), 49 (S. 156 ff.); mit Lösungsansätzen *Geiß, Robin/Lahmann, Henning, Cyber warfare: applying the principle of distinction in an interconnected space*, in: Israel Law Review, 2012, Band 45 (3), S. 381–399, S. 390 ff.

## 2. Kennzeichnungspflicht für technische Einrichtungen bei der digitalen Kriegsführung

### 2.1. Völkerrechtliche Grundsätze zur Kennzeichnung von Kriegsparteien

Das humanitäre Völkerrecht kennt den Grundsatz, dass Kombattantinnen und Kombattanten in internationalen bewaffneten Konflikten ein von **weitem erkennbares (bleibendes) Zeichen** tragen müssen. Diese Pflicht beruht auf völkerrechtlichen Verträgen[6], ist aber auch als Völkergewohnheitsrecht anerkannt.[7] Eine völkerrechtliche **Kennzeichnungspflicht** gibt es darüber hinaus nur sehr begrenzt. Hauptbeispiele sind Kriegsschiffe und Luftfahrzeuge, deren Kennzeichnung die **nationale und** (ggf.) **militärische Zugehörigkeit** erkennen lassen muss.[8] Eine besondere völkerrechtliche Kennzeichnungspflicht für **militärische Wirkmittel** – wie Munition, einzelne Raketen oder Bomben – besteht dagegen nicht.[9] Viele Wirkmittel, wie etwa Drohnen oder Schusswaffen, sind in der Praxis allenfalls nach Modellen unterscheidbar und eher auf den Hersteller oder Exporteur zurückzuführen als einer Kampfpartei zuzuordnen.

4 Siehe dazu *Lülf, Charlotte*, *International Humanitarian Law in Times of Contemporary Warfare – The New Challenge of Cyber Attacks and Civilian Participation,* in: Humanitäres Völkerrecht – Informationsschriften, 2013, S. 74–82; *Tallinn Manual*, Fn. 3., Regel 35 (S. 118 ff.); ausführlich zur Frage legaler Beteiligung von Zivilpersonen *Watts, Sean, Combatant Status and Computer Network Attack*, Virginia Journal of International Law, Band 50 (2010), S. 392-447 (411 ff., 430 ff.); ferner *Padmanabhan, Vijay M., Cyber Warriors and the Jus in Bello,* International Law Studies, U.S. Naval War College, Band 89 (2013), S. 288–308.

5 Siehe zu dieser Frage etwa *Linaki, Evangelia*, *Cyber Warfare and International Humanitarian Law: a Matter of Applicability*, in: Humanitäres Völkerrecht – Informationsschriften, 2014, S. 171 ff.; *Ziolkowski*, Computernetzwerkoperationen, Fn. 3, S. 206–209; *Tallinn Manual*, Fn. 3, Regeln 30 (S. 106 ff.), 20 (S. 75 ff.), 22 (S. 79 ff.), 23 (S. 84 ff.); ausführlich *Keber, Tobias O./Roguski, Przemysław Nick*, Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis, in: Archiv des Völkerrechts, Band 49 (2011), S. 399–434, S. 406–418, zur Staatenpraxis S. 418–431.

6 **Regel 1 Nr. 2** im Anhang des **(IV.) Haager Abkommens** vom 18.10.1907, betreffend die Gesetze und Gebräuche des Landkrieges, Ordnung der Gesetze und Gebräuche des Landkriegs; deutsche Übersetzung erhältlich unter http://www.admin.ch/opc/de/classified-compilation/19070034/198511010000/0.515.112.pdf (letzter Zugriff: 19.02.2015). **Artikel 4 A Nr. 2 Buchstabe b des (III.) Genfer Abkommens** über die Behandlung der Kriegsgefangenen, deutsche Übersetzung verfügbar unter http://www.admin.ch/opc/de/classified-compilation/19490187/201407180000/0.518.42.pdf (letzter Zugriff: 19.02.2015).

7 *Tallinn Manual*, Fn. 3, Regel 26 (S. 97, 99); *Henckaerts, Jean-Marie/Doswald-Beck, Louise* (Hrsg.), *Customary International Humanitarian Law*, Volume I: Rules, Cambridge: Cambridge University Press (2005), korrigierte Auflage 2009, Regel 106 (S. 384 ff.).

8 Handbuch des Bundesministeriums für Verteidigung, Humanitäres Völkerrecht in bewaffneten Konflikten, ZDv15/2, Mai 2013, abrufbar über http://www.bmvg.de/ (letzter Zugriff: 18.02.2015), Rn. 349. Für **Kriegsschiffe** vgl. Artikel 29 des Seerechtsabkommens der Vereinten Nationen vom 10.12.1982, Übersetzung erhältlich unter http://www.admin.ch/opc/de/classified-compilation/20040579/201311280000/0.747.305.15.pdf (letzter Zugriff: 23.02.2015), für zivile **Luftfahrzeuge** u.a. das Chicagoer Abkommen über die internationale Zivilluftfahrt vom 07.12.1944, Artikel 20 und Annex 7, Übersetzung erhältlich unter http://www.admin.ch/opc/de/classified-compilation/19440105/201408120000/0.748.0.pdf (letzter Zugriff: 23.02.2015).

9 Bereits **Landkriegsfahrzeuge** sind von der Kennzeichnungspflicht ausgenommen, siehe Handbuch des Bundesministeriums für Verteidigung, ZDv15/2, Fn. 8, Rn. 349.

## 2.2. Anwendbarkeit des Völkerrechts auf Cyber-Angriffe

Es besteht weitgehend Einigkeit darüber, dass das **humanitäre Völkerrecht auf Cyber-Angriffe** im (internationalen wie nicht-internationalen) **bewaffneten Konflikt** (*Cyber Warfare*) grundsätzlich Anwendung findet.[10]

Dies entspricht auch der völkerrechtlichen Praxis bei **neuen militärischen Wirkmitteln**. So hatte der **Internationale Gerichtshof** bereits in seinem Rechtsgutachten zu **Nuklearwaffen** klargestellt, dass die Grundsätze des Kriegsrechts auch auf alle zukünftigen Kriegsformen und Waffen Anwendung finden:

> "*However, it cannot be concluded […] that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to* ***all forms of warfare and to all kinds of weapons****, those of the past, those of the present and* ***those of the future***."[11]

Hierbei konnte sich der Gerichtshof auf **Artikel 36** des **1. Zusatzprotokolls** zu den **Genfer Konventionen** stützen, wonach jeder Vertragsstaat verpflichtet ist,

> „bei der Prüfung, Entwicklung, Beschaffung oder Einführung neuer Waffen oder neuer Mittel oder Methoden der Kriegführung festzustellen, ob ihre Verwendung stets oder unter bestimmten Umständen durch dieses Protokoll oder durch eine andere auf die Hohe Vertragspartei anwendbare Regel des Völkerrechts verboten wäre."[12]

---

10 Siehe hierzu auch das *Tallinn Manual*, Fn. 3, Regel 20 (S. 75). Das Handbuch ist nicht verbindlich und wird auch von der deutschen Bundesregierung nicht als verpflichtend angesehen, siehe das Handbuch des Bundesministeriums für Verteidigung, ZDv15/2, Fn. 8, Rn. 486, 131. Es bietet jedoch eine aufschlussreiche Übersicht über die Anwendbarkeit des traditionellen Völkerrechts auf elektronische Kriegsführung, die der Rechtsauffassung einiger Staaten – unter anderem der USA – durchaus nahekommt. Siehe hierzu ausführlich *Schmitt, Michael N., International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, Harvard International Law Journal, Band 54 (2012), S. 13–37, http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (letzter Zugriff: 18.02.2015), S. 15, ausführliche Gegenüberstellung auf S. 15–37. Zur Begriffsbestimmung siehe *Droege, Cordula*, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*, International Review of the Red Cross, Band 94 (2012), S. 533–578 (538).

11 Internationaler Gerichtshof, *Nuclear Weapons* (*Legality of the Threat or Use of Nuclear Weapons*), http://www.icj-cij.org/docket/files/95/7495.pdf (letzter Zugriff: 19.02.2015), Rn. 86.

12 Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte, Stand vom 18.07.2014, zitiert nach der deutschen Übersetzung http://www.admin.ch/opc/de/classified-compilation/19770112/201407180000/0.518.521.pdf (letzter Zugriff: 19.02.2015).

Dies bedeutet gleichzeitig, dass die Wahl neuartiger Wirkmittel nach dem Völkerrecht grundsätzlich erlaubt ist, soweit sie als **kompatibel** mit dem bestehenden Recht angesehen werden.[13] Ein Verbot bestimmter Waffen bedarf dagegen in der Regel einer völkerrechtlichen Vereinbarung.[14]

Einigkeit besteht auch darüber, dass das humanitäre Völkerrecht **außerhalb** bewaffneter Konflikte **nicht anwendbar** ist.[15] Eine der Hauptschwierigkeiten besteht bei einer Cyber-Attacke aber gerade darin, festzustellen, ob ein solcher **bewaffneter Konflikt** vorliegt.[16] Bislang wird nur bei wenigen Cyber-Attacken diskutiert, ob die erforderliche Schwelle für einen bewaffneten Konflikt (und die Anwendung des humanitären Völkerrechts) überhaupt erreicht wurde.[17] Insgesamt gehen große Teile der Literatur davon aus, dass dies bislang noch nie der Fall war.[18]

### 2.3. Übertragbarkeit der völkerrechtlichen Grundsätze zur Kennzeichnung auf den Cyber-Raum

Wie auch die Bundesregierung in ihrer Antwort auf eine Kleine Anfrage im Februar 2015 ausführt, müssten demnach **Kombattantinnen und Kombattanten selbst** in einem **bewaffneten Konflikt** eine Kennzeichnung tragen.[19] Dies gilt insbesondere für diejenigen Armeeangehörigen, die die entsprechenden Angriffs- und Verteidigungsmaßnahmen im Cyber-Raum durchführen.

---

13 Siehe dazu auch **Regel 22** im Anhang des **IV. Haager Abkommens** von 1907 (Fn. 6), der vorsieht, dass die Wahl der Mittel nicht unbeschränkt ist. Auch diese Vorschrift gilt als **Völkergewohnheitsrecht**: Internationaler Gerichtshof, *Legality of the Threat or Use of Nuclear Weapons*, Rechtsgutachten, http://www.icj-cij.org/docket/files/95/7495.pdf (letzter Zugriff: 19.02.2015), Rn. 75; genauer: Internationaler Gerichtshof, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Rechtsgutachten vom 09.07.2004, http://www.icj-cij.org/docket/files/131/1671.pdf (letzter Zugriff: 20.02.2015), Rn. 89: "*The Court considers that the provisions of the Hague Regulations have become part of customary law …*"; Internationaler Gerichtshof, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Urteil vom 19.12.2005, http://www.icj-cij.org/docket/files/116/10455.pdf (letzter Zugriff: 20.02.2015), Rn. 217. Siehe für **Cyber-Attacken** auch *Tallinn Manual*, Fn. 3, Regel 48 (S. 153 ff.).

14 *Stadlmeier/Unger*, Cyber War und Cyber Terrorismus, Fn. 2, S. 70 f.

15 *Droege, Get off my cloud*, Fn. 10, S. 538.

16 Siehe dazu bereits oben, Einleitung, Fußnote 5 mit weiteren Nachweisen, und unten 3.

17 *Linaki, Cyber Warfare*, Fn. 5, stellt nach kurzer Beleuchtung (S. 173 ff.) der Cyber-Operationen der letzten Jahre mit staatlicher Beteiligung fest, dass allenfalls im Fall *Stuxnet* von einem durch Cyber-Attacken ausgelösten bewaffneten Konflikt die Rede sein könnte – wenn denn die Auffassung vertreten wird, dass der Computerwurm tatsächlich einem Staat **zugerechnet** werden kann. Allerdings habe sich in keinem der in Betracht kommenden Fälle der Urheber der Operation dazu bekannt (S. 175).

18 *Krieger, Heike*, Krieg gegen anonymous: völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, in: Archiv des Völkerrechts, Band 50 (2012), S. 1–20, S. 2.

19 Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 18/3799) mit Antwort des Bundesministeriums der Verteidigung im Namen der Bundesregierung vom 6. Februar 2015 (Drucksache 18/3963), Frage 23.

Insoweit Mitglieder der nationalen Streitkräfte betroffen sind, sind **völkerrechtliche Grundsätze** nach der überwiegenden Auffassung[20] wie nach Ansicht der Bundesregierung also **uneingeschränkt anwendbar**.

Allerdings bestehen in der Literatur auch Zweifel am Sinn dieser Vorschrift im Zusammenhang mit digitalen Kampfhandlungen. Einige Autoren wollen deshalb bereits die reine **Zugehörigkeit zu einem Staat** ausreichen lassen.[21] Andere zweifeln mangels Sichtkontakts den **Sinn des Unterscheidungszeichens** bei Cyber-Attacken an und stellen Überlegungen zur Festlegung **militärischer IP-Adressen** an.[22] Wieder andere wollen eine **Ausnahme für die Besatzungen von Kriegsschiffen und Militärflugzeugen** und andere Militärobjekte machen, die ohnehin selbst der Kennzeichnungspflicht unterliegen.[23]

### 2.4. Kennzeichnung technischer Einrichtungen im Rahmen von Cyber-Angriffen

Im Rahmen von Cyber-Angriffen kommt es gerade bei der Bestimmung ihrer **Urheberschaft** zu einer Vielzahl von Herausforderungen. Diese bringt *Jenny Döge* auf den Punkt:

> „*Cyber warfare blurs the traditional distinctions between ordinary crimes and acts of war, and between accidents and attacks. Cyber attacks are ambiguous because they can be less tangible than conventional military actions. This is due to the fact it is easy to camouflage an attack and its source. IP addresses can be faked and signals can be routed through civilian or neutral networks. As previously mentioned, around 96 % of attacks on a network are not detected.*“[24]

Vor diesem Hintergrund stellt sich insbesondere die Frage, ob sich die völkerrechtliche Kennzeichnungspflicht bei **Cyber-Angriffen** auch auf **technische Einrichtungen** bezieht.[25] Die Bundesregierung vertritt in ihrer Antwort auf die o. g. Kleine Anfrage die gegenteilige Auffassung, dass für **technische Einrichtungen** – anders als bei Kombattantinnen und Kombattanten – kein Unterscheidungserfordernis bestehe.[26]

---

20 So auch *Tallinn Manual*, Fn. 3, Regel 26 (S. 99, Rn. 10 ff.).

21 *Watts, Sean, Combatant Status and Computer Network Attack*, Fn. 4, S. 434 ff., 447.

22 *Stadlmeier/Unger*, Cyber War und Cyber Terrorismus, Fn. 2, S. 76 f.

23 Z. B. einige Mitglieder der Expertengruppe des Tallinn-Manuals, siehe Regel 26 (S. 99, Rn. 12).

24 *Döge, Jenny, Cyber Warfare*, Fn. 2, S. 498 (Nachweise ausgeblendet). Zu verschiedenen **Arten und Wirkungsformen von Cyber-Angriffen** siehe die Einführung bei *Ziolkowski*, Computernetzwerkoperationen, Fn. 3, S. 203 f., sowie die Auszüge unter 3.1.

25 Etwa über militärische IP-Adressen, siehe dazu oben, Fn. 22.

26 Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 18/3799) mit Antwort des Bundesministeriums der Verteidigung im Namen der Bundesregierung vom 6. Februar 2015 (Drucksache 18/3963), Frage 25.

Dies deckt sich mit dem derzeitigen Völkerrecht, da es sich bei Cyber-Angriffen lediglich um eine Form **militärischer Wirkmittel**, ggf. auch um **Methoden** der Kampfführung, handelt.[27] **Technische Einrichtungen** im Rahmen der digitalen Kriegsführung unterscheiden sich nicht wesentlich von **anderen Wirkmitteln**, die der Kennzeichnungspflicht nicht unterliegen. So sind **Cyber-Angriffe** trotz aller Besonderheiten grundsätzlich mit **traditionellen Kampfhandlungen** vergleichbar.[28]

Die technische Einrichtung selbst dürfte demnach keinen höheren völkerrechtlichen Anforderungen unterliegen als eine Schusswaffe, ebenso wenig der Computerwurm oder der Trojaner als Äquivalent der Munition.[29] Dies gilt unabhängig von der Frage, ob theoretisch eine technische Möglichkeit besteht, die Herkunft eines Computerwurms oder eines Trojaners (z. B. in seinem Quellcode) zu kennzeichnen.

Dennoch wird anerkannt, dass die **technische Komplexität** erhöhte Schwierigkeiten hervorruft, die **Urheberschaft** des Angriffs sicher aufzuklären.[30] Erschwerend kommt hinzu, dass gerade Schadprogramme (wenn überhaupt) häufig erst mit zeitlicher Verzögerung aufgespürt werden, wenn ein Schaden bereits eingetreten ist, und dass sie bis zu ihrer Beseitigung fortwährend operieren können.[31]

Die Einführung neuer Wirkmittel unterliegt den bestehenden völkerrechtlichen Maßstäben. Höhere Anforderungen für einzelne neue Wirkmittel können nur durch einen völkerrechtlichen Vertrag oder durch Völkergewohnheitsrecht entstehen. Da die Ausprägung einer einschränkenden Staatenpraxis und entsprechender Rechtsüberzeugung (*opinio iuris*) auf dem Gebiet von Cyber-Angriffen derzeit unwahrscheinlich erscheint, müssten solche **Sonderregelungen für die Kennzeichnung** ausgehandelt und – in der Regel nach einem langwierigen diplomatischen Prozess – in einem völkerrechtlichen Vertrag niedergelegt werden.

---

27 Nach Regel 41 des *Tallinn Manual*, Fn. 3, S. 141 f., sind Cyber-Waffen und Cyber-Systeme als **Wirkmittel** einzuordnen, Cyber-Techniken, -Taktiken und -Verfahren als **Methoden**. Siehe auch Kleine Anfrage der Fraktion DIE LINKE. mit Antwort der Bundesregierung vom 06.02.2015 (Drucksache 18/3963), Frage 20.

28 Zu den **Grenzen der Vergleichbarkeit des Cyber-Krieges mit traditionellen Kampfhandlungen** siehe aber *Krieger*, Krieg gegen anonymous, Fn. 18, S. 3.

29 So sieht auch *Tallinn Manual*, Fn. 3, Regel 72 (S. 206 ff.) – analog zu traditionellem Kampfgeschehen, siehe Art. 1 Abs. 4 des Annexes 1 zum 1. Zusatzprotokoll der Genfer Konventionen – nur die adäquate Kennzeichnung von Computern, Netzwerken und Daten **medizinischer Einrichtungen**, u.a. durch elektronische Markierungen, vor, damit deren Privilegien leichter gewährleistet werden können.

30 *Singer, Tassilo*, Cyberwarfare – Damoklesschwert für das Völkerrecht?, in: Sicherheit + Frieden, 2014, S. 17–23, S. 19, mit weiteren Nachweisen.

31 *Singer, Tassilo*, Cyberwarfare, Fn. 30, S. 22.

Von einer generellen **Inkompabilität** von **Cyber-Angriffen** mit dem Völkerrecht kann indes nicht ausgegangen werden. Dies hängt auch damit zusammen, dass diese Angriffe bei einer gezielten Anwendung gegen militärische Ziele Schäden – insbesondere an Rechtsgütern der Zivilbevölkerung – minimieren können.

Insofern aber erfüllen sie gerade das Ziel des humanitären Völkerrechts, unverhältnismäßiges Leid zu vermeiden.[32] Auch deshalb hätte ein generelles **Cyber-Krieg-Verbot** keine Chance auf Realisierung.[33] Einzig einzelne Angriffsformen – wie die Verwendung von **Bot-Netzen** – halten einige Autoren wegen gezielter Nicht-Offenlegung des Angreifers für völkerrechtswidrig.[34]

## 3. Attribution/ Zurechnung von Cyber-Angriffen

Die Frage nach der Zurechnung (Attribution, Herkunft) von Cyber-Attacken gilt als das **Kernproblem** der digitalen Kriegsführung. Stehen die **Konfliktparteien** nicht fest, so bleibt unklar, ob ein **bewaffneter Konflikt** (international oder nicht-international) im Sinne des Völkerrechts überhaupt vorliegt und ob die Grundsätze des humanitären Völkerrechts Anwendung finden.[35] Mehr noch als bei traditionellen Kriegshandlungen besteht bei der digitalen Kriegsführung die Möglichkeit, Angriffe zu verschleiern. Häufig besteht bei den Urhebern einer Cyber-Attacke kein unmittelbares Interesse, sich zu einem Cyber-Angriff zu bekennen.[36]

### 3.1. Technische Parameter

Um die Frage der Attribution rechtlich bewerten zu können, sollen zunächst einmal die **technischen Parameter von Computernetzwerkoperationen** und die **Möglichkeiten ihrer Verschleierung** untersucht werden. *Katharina Ziolkowski*, Mitglied der Expertengruppe des *Tallinn Manual on the International Law applicable to Cyber Warfare*, führt dazu aus:

> „Die **Identifizierung des Urhebers eines Cyber-Angriffs** wird sich immer schwierig gestalten. Ein Cyber-Angriff zeichnet sich vor allem durch Schnelligkeit aus. Sobald er beendet ist, ist eine Rückverfolgung des Datenstroms (sog. *back-tracing*) und dadurch die Feststellung des Urhebers grundsätzlich recht unwahrscheinlich.

32 *Döge, Jenny, Cyber Warfare*, Fn. 2, S. 500.

33 Siehe auch im Vergleich zu historischen Vorhaben *Krieger*, Krieg gegen anonymous, Fn. 18, S. 7 ff.

34 *Stadtmeier/Unger*, Cyber War und Cyber Terrorismus, Fn. 2, S. 77.

35 *Linaki, Cyber Warfare*, Fn. 5, S. 175. Siehe auch *Tallinn Manual*, Fn. 3, Regel 20 (S. 77).

36 Siehe hierzu ausführlich *Linaki, Cyber Warfare*, Fn. 5, S. 175.

Erschwerend kommt hinzu, dass der Cyber-Angreifer weitgehend anonym bleiben kann, indem er z. B. einen der Anonymisierungsdienste nutzt, die heutzutage im Internet kostengünstig oder gar kostenlos angeboten werden. Vor allem bietet das **Internet aber Möglichkeiten der Identitätstäuschung**. Jeder Computer, der eine Verbindung zum Internet aufnimmt, verfügt über eine sog. IP-Adresse, eine Zahlenfolge, welche den Datenaustausch mit Internetknotenpunkten und anderen Computern bzw. Servern ermöglicht.

Zudem sendet der Computer während der Internetverbindung einige weitere technische Daten. Es besteht die Möglichkeit, eine **fremde IP-Adresse und andere technische Daten vorzutäuschen** (sog. *malicious misrepresentation* oder *spoofing*) und damit unter einer fremden Cyber-Identität im Internet zu agieren.

Auch kann eine satellitengestützte Verbindung zum Internet über ein Handy aufgebaut werden, dessen **Identifikationsnummer gefälscht** ist. Zudem kann der Datenstrom beim Einsatz von sog. Zombie-Programmen (teilweise im Internet kostenlos zum *download* bereitgestellt), die zuvor über sog. Trojanische Pferde auf Computern ahnungsloser Individuen installiert wurden, über eine Vielzahl zwischengeschalteter Computer über den gesamten Globus hinweg geleitet und dabei einer dieser Computer als Absender des Datenstroms missbraucht werden (sog. *Remote control*).

Wenn also ein Cyber-Angriff stattgefunden hat, wird es sehr wahrscheinlich im ersten Augenblick – und manchmal auch nach einer eingehenden technischen Analyse – schwer zu erkennen sein, ob ein Angriff durch einen übermütigen Jugendlichen, einen kriminellen Einzeltäter (inklusive Terroristen), eine Gruppierung mit extremistischem oder terroristischem Hintergrund, oder durch die gegnerische Partei eines bewaffneten Konflikts erfolgte oder aber bloß eine technische Fehlfunktion des eigenen Systems vorliegt. Damit verbunden ist die **Ungewissheit über den Ort, an dem sich dasjenige Computersystem befindet**, von dem aus der Angriff geleitet wurde."[37]

37 *Ziolkowski*, Computernetzwerkoperationen, Fn. 3, S. 204 f.

### 3.2. Zurechnungsprobleme im Rahmen traditioneller (analoger) Kriegsführung

**Unsicherheiten bei der Identifizierung des Angreifers** sind auch in der traditionellen bzw. „analogen" Kriegführung **nichts gänzlich Neues**. Insbesondere die sog. „**hybride Kriegsführung**"[38] in der **Ukraine** verschleiert einmal mehr die Identität ihrer Akteure und Hintermänner[39] und lässt die rechtlichen Verantwortlichkeiten bzw. die Zurechnung von militärischen Aktionen und Unterstützungsleistungen verschwimmen.

Wo nicht einmal klar ist, ob und wann ein „*armed attack*" (bewaffneter Angriff) im Sinne von Art. 51 VN-Charta (der einem fremden Staat zugerechnet werden muss) vorliegt, gestalten sich **militärische Aufklärung** und die **Reaktionsmöglichkeiten unter Unsicherheitsbedingen** schwierig.[40]

### 3.3. Attribution im Rahmen digitaler Kriegsführung

Bei **Ungewissheit** über das Vorliegen eines **bewaffneten Angriffs** („Intensitätsschwelle" der Cyber-Attacke) bzw. über die **Identität des Angreifers** und den **Ursprungsort des Angriffs bleibt unklar**, ob die Polizei/Staatsanwaltschaft, die Streitkräfte (falls der Cyber-Angriff in seiner Wirkung einem konventionellen Angriff fremder Streitkräfte gleichkommt) oder aber die Administratoren des eigenen Computernetzwerkes tätig werden müssen. Ein bewaffneter Angriff durch Cyber-Attacken darf etwa nach überwiegender Auffassung nur dann mit militärischen Mitteln (in Ausübung des **Selbstverteidigungsrechts**) beantwortet werden, wenn der Angriff **einem Staat zurechenbar** ist.

Der Staat, der eine (militärische) Gegenmaßnahme ergreift, trägt auch die **Beweislast** für das Vorliegen eines Völkerrechtsverstoßes sowie für die Kausalität und die Identität des Verursachers. Insoweit stellt sich ganz zentral die Frage, **welcher Grad an Sicherheit für die Zurechnung** der Computernetzwerkoperation erforderlich ist, um das Ergreifen einer Gegenmaßnahme zu rechtfertigen.

---

38 Bei der sogenannten **hybriden Kriegsführung** kombinieren staatliche oder nicht-staatliche Akteure (Aufständische, Separatisten) konventionelle und verdeckte militärisch-strategische Mittel. Beteiligt an der Auseinandersetzung sind neben regulären Streitkräften auch irreguläre Kämpfer (Milizen, Freischärler) sowie eingeschleuste Geheimdienstler, Spezialkräfte u.a.m. Dazu werden neben konventionellen Waffen, Einheiten und Techniken auch irreguläre Mittel eingesetzt, die bis hin zu kriminellen und terroristischen Mitteln reichen können. Das Spektrum reicht von Partisanentaktiken über energiepolitische Maßnahmen bis hin zur **Cyber-Kriegsführung**. Besondere Bedeutung kommt überdies der **Desinformation** und der **Propaganda** zu.

39 Dies gilt insb. für die Unterstützung der Separatisten, aber auch der russischen Soldaten ohne Hoheitsabzeichen sowie der in den Konflikt eingeschleusten Geheimdienstler und Spezialkräfte.

40 Näher dazu *Krieger,* Krieg gegen anonymous, Fn. 18, S. 11 ff.

Die allgemeinen **Anforderungen an die völkerrechtliche Zurechenbarkeit** hat das **Iran-US Claims Tribunal** folgendermaßen formuliert: "*In order to attribute an act to the State, it is necessary to identify with reasonable certainty the actors and their association with the State.*"[41]

Um **Beweisschwierigkeiten bei der Identifizierung des Angreifers im Cyber-Raum** zu vermeiden, wollen Teile der Literatur für eine Zurechnung – abweichend vom Erfordernis der „*reasonable certainty*" – bestimmte **Vermutungen ausreichend** sein lassen.[42] Statt auf eine **nachweisbare Kausalität** sei vielmehr auf den **Kontext der Operation** abzustellen. Dabei wird vorrangig die Frage gestellt, **wem der Angriff nutze**. Demgemäß führe die Verweigerung, bei der Aufklärung einer Computernetzoperation Rechtshilfe zu leisten, zur **Vermutung der Urheberschaft des Angriffes**.[43]

Doch können Vermutungen, etwa auf der Grundlage fehlender Kooperationsbereitschaft des verdächtigten Staates, ausreichen, eine Zurechnung zu begründen?[44]

Noch weiterreichende Vorschläge der amerikanischen Literatur verzichten sogar **gänzlich auf den Nachweis von Zurechnung** auf der Grundlage von Kausalität, sofern sich die Computernetzwerkattacken gegen kritische Infrastrukturen richten.[45]

Überdies wurde überlegt, ob Staaten, die es **tolerieren**, dass Computernetzwerkoperationen von ihrem Territorium ausgehen oder es versäumen, derartige Operationen zu verhindern, nicht mit angemessenen Gegenmaßnahmen rechnen müssten. Ziel dieses Vorschlages ist es offenbar, auf Computernetzwerkoperationen mit eben solchen Mitteln reagieren zu können und dabei die Schwierigkeiten der Zurechnung zu umgehen.[46]

Auswege aus dem „**Attributionsdilemma**" werden zuletzt auch mittels **Internationaler Kooperationsrichtlinien** gesucht.[47]

---

41 *Yeager v. Islamic Republic of Iran*, Iran-U.S.C.T.R. 17 (1987), 92 (101 f.).

42 Vgl. *Heintschel von Heinegg*, *Wolff,* Cyberspace – ein völkerrechtliches Niemandsland, in: *Schmidt-Radefeldt/Meissler* (Hrsg.), Automatisierung und Digitalisierung des Krieges, Baden-Baden: Nomos 2012, S. 159 (172), der sich allgemein für andere Zurechnungsstandards außerhalb der Staatenverantwortlichkeit und eine widerlegliche Vermutung der Zurechenbarkeit bei der Prävention erheblicher Schädigungen ausspricht.

43 *Knake, Robert*, Untangling Attribution: Moving to Accountability in Cyberspace, 2010, S. 8 f., verfügbar unter: www.cfr.org/united-states/untangling-attribution-moving-accountabilitycyberspace/p22630 (letzter Zugriff: 23.02.2015).

44 Zweifelnd insoweit *Krieger*, Krieg gegen anonymous, Fn. 18, S. 15.

45 *S. Condron*, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, in: 20 Harvard Journal of Law and Technology (2007), S. 403 (416).

46 Rede der Staatssekretärin im Bundesinnenministerium, International Co-operation in Developing Norms of State Behaviour for Cyberspace, Berlin 13. Dezember 2011, 8, zitiert bei *Krieger*, Fn. 18, S. 14, Fn. 79.

47 Vgl. hierzu den Beitrag von *Reinhold, Thomas*, in: S+F 2014, S. 23-27 **- Anlage 2-**

## 4. Perfidieverbot und Kriegslist

Die technischen Eigenheiten von Computernetzwerkattacken bringen es mit sich, dass die **Verschleierung der Identität des Angreifers** zu den **typischen Instrumenten digitaler Kriegsführung** zählt.[48] Bei der humanitär-völkerrechtlichen Bewertung von verschleierten Cyber-Attacken ist zu unterscheiden zwischen der (erlaubten) **Kriegslist** und der (verbotenen) **Heimtücke (Perfidie)**. **Art. 37 des 1. Zusatzprotokolls (1977) zu den Genfer Konventionen** differenziert wie folgt:

> „(1) Es ist verboten, einen Gegner unter Anwendung von Heimtücke zu töten, zu verwunden oder gefangen zu nehmen. Als Heimtücke gelten Handlungen, durch die ein Gegner **in der Absicht**, sein **Vertrauen zu missbrauchen**, **verleitet wird**, darauf zu vertrauen, dass er nach den Regeln des in bewaffneten Konflikten anwendbaren Völkerrechts **Anspruch auf Schutz hat oder verpflichtet ist, Schutz zu gewähren**. Folgende Handlungen sind Beispiele für Heimtücke: (…)
>
> > c) das Vortäuschen eines zivilen oder Nichtkombattantenstatus;
> > d) das Vortäuschen eines geschützten Status durch Benutzung von Abzeichen, Emblemen oder Uniformen der Vereinten Nationen oder neutraler oder anderer nicht am Konflikt beteiligter Staaten.
>
> (2) Kriegslisten sind nicht verboten. Kriegslisten sind Handlungen, die einen Gegner **irreführen** oder ihn zu **unvorsichtigem Handeln veranlassen** sollen, die aber keine Regel des in bewaffneten Konflikten anwendbaren Völkerrechts verletzen und nicht heimtückisch sind, weil sie den Gegner nicht verleiten sollen, auf den sich aus diesem Recht ergebenden Schutz zu vertrauen. Folgende Handlungen sind Beispiele für Kriegslisten: Tarnung, Scheinstellungen, Scheinoperationen und irreführende Informationen."

Die **Grenze** zwischen Perfidie und Kriegslist verläuft **nicht immer trennscharf,** da beide Begriffe eine **Täuschungshandlung** voraussetzen. In der Praxis fallen **deutlich mehr Handlungen unter „Kriegslist",** da die tatbestandlichen Hürden beim Perfidieverbot – insbesondere das Erfordernis der „Absicht" (subjektiver Tatbestand) sowie das Vorliegen eines legitimen Vertrauens auf der Seite des Getäuschten – vergleichsweise hoch sind.

Im Bereich der digitalen Kriegsführung erfolgt die Täuschung in Form einer **Fehlinformation**. Fehlinformationen über einen geschützten Status bzw. Zivilisten-Status können z.B. per E-Mail oder als Information auf einer Web-Seite weitergegeben werden. Möglich ist auch die Vortäuschung einer bestimmten IP-Adresse oder anderer technischer Daten.

---

48 *Stadlmeier/Unger*, Cyber War und Cyber Terrorismus, Fn. 2, S. 75.

Ein „plakatives“ (wenn auch eher realitätsfernes) **Beispiel für das Perfidieverbot** ist die in der Literatur immer wieder auftretende E-Mail an die gegnerischen Streitkräfte, die im *header* als Absender das Rote Kreuz oder Microsoft Support aufweist, aber in Wahrheit einen Virus (Trojaner) enthält, der zu physischer Zerstörung auf der gegnerischen Seite führt.[49] In der Fachwelt ist in diesem Zusammenhang umstritten, ob der Verstoß gegen das Perfidieverbot Begleitfolgen wie Tod oder Verletzungen des Gegners aufweisen muss.[50]

Abgesehen davon stellt sich ganz generell die Frage, ob Staaten dem (vermeintlichen) Absender von E-Mails vertrauen dürfen, d.h. ob es im Völkerrecht eine **legitime Erwartung** hinsichtlich der **Authentizität von elektronischer Korrespondenz** gibt. Angesichts der leichten Manipulierbarkeit des E-Mail-Verkehrs spricht einiges gegen die Legitimität eines solchen Vertrauens, womit dem Perfidieverbot die Grundlage entzogen wäre.

Gegen das **Heimtückeverbot** verstoßen Hackerhandlungen, bei denen zur eigenen Tarnung technische Daten vorgetäuscht werden, die auf die **Cyber-Identität eines Zivilisten** schließen lassen (z.B. Gebrauch eines zivilen Netzwerks).[51] Verboten wäre auch die **Manipulation von Web-Seiten geschützter Entitäten** (Rotes Kreuz, VN) oder ein **Missbrauch ihrer Symbole**.[52] Ebenso unzulässig wäre das Manipulieren der gegnerischen Aufklärungs-Software mit der Folge, dass der Gegner z.B. ein Krankenhaus mit einem militärischen Hauptquartier verwechselt.

Die erlaubte **Kriegslist** im Sinne des Art. 37 Abs. 2 ZP I, die den Gegner **irreführen** oder zu unvorsichtigem Handeln veranlassen soll, bietet demgegenüber ein weites Anwendungsfeld für **völkerrechtlich zulässige Computernetzwerkoperationen**. So ist vorstellbar, dass eine der Konfliktparteien um das eigene Computernetzwerk herum ein sog. „*honey net*“ aufbaut, d.h. ein gegen *hacking* nur leicht geschütztes Netzwerk, welches dem eigenen Netzwerk technisch gesehen zum Verwechseln ähnlich sieht, aber **falsche Informationen** über die geplanten militärischen Operationen oder über die eigenen Kräfte und deren Lokalisierung beinhaltet und den Gegner damit fehlinformiert.[53]

---

49 Vgl. insoweit *Ziolkowski,* Computernetzwerkoperationen, Fn. 3, S. 209; *Döge, Jenny*, Cyber Warfare, Fn. 2, S. 496; *Dinniss, Heather H.*, *Cyber Warfare and the Law of War*, Cambridge Univ. Press 2012, S. 264.

50 Zum Streitstand vgl. *Tallinn Manual*, Fn. 3, Regel 60, para. 7. In diesem Sinne z.B. *Dinniss, Heather H.*, *Cyber Warfare and the Law of War*, Fn. 49, S. 264.

51 Ebenso *Stadlmeier/Unger*, Cyber War, Fn. 2, S. 75; *Dinniss, Heather H.*, *Cyber Warfare and the Law of War*, Fn. 49, S. 262.

52 Vgl. insoweit Art. 38 ZP I: Verbot des Missbrauchs von international anerkannten, Schutz verleihenden Kennzeichen, Abzeichen oder Signalen.

53 *Ziolkowski,* Computernetzwerkoperationen, Fn. 3, S. 210.

Unter **erlaubte Kriegslisten** fallen u.a.:[54]

- **Aufbau eines *„dummy"-Computernetzwerks,*** das nicht-existierende Streitkräfte simuliert und die gegnerische Aufklärung entsprechend irreführt

- **Vorgetäuschte Cyber-Attacken**

- **Gebrauch von Signalen oder Passwörtern des Gegners**

- **Übermittlung falscher Nachrichten,** die den Anschein erwecken, als stammten Sie aus dem gegnerischen Hauptquartier. Allerdings dürfen diese Informationen den Gegner nicht dazu verleiten, zivile Ziele in der Annahme anzugreifen, es handele sich um militärische Ziele

- **Führen eines Cyber-Angriffs über verschiedene Router, Server und Netzwerke** in unterschiedlichen Staaten, um die Herkunft des Angriffs zu verschleiern

- **Manipulation von Aufklärungs-Sensoren**

Amerikaner und Israelis verwenden dazu das sog. **Suter-Computersystem**, das entwickelt wurde, um feindliche Computernetzwerke und Kommunikationssysteme anzugreifen und integrierte Luftabwehrsysteme zu stören. Das Suter-System ermöglicht u.a. die Übernahme der Kommunikationsverbindungen strategischer Ziele des Feindes, wie beispielsweise stationärer oder mobiler Flugabwehrraketen.

54 Beispiele für digitale Kriegslisten z.B. im *Tallinn Manual*, Fn. 3, Regel 61 para. 2; vgl. auch *Dinniss, Heather H.*, *Cyber Warfare and the Law of War*, Fn. 49, S. 261 f.

## 5. Zusammenfassung und Ausblick

Die Anwendung der Regeln des Völkerrechts auf Computernetzwerkoperationen stellt weder prinzipiell noch methodisch ein unüberwindbares Hindernis dar. So können die hier erörterten Fragen der Kennzeichnungspflicht sowie die Unterscheidung zwischen Perfidie und Kriegslist im Cyberraum auch mit dem herkömmlichen juristischen Instrumentarium zufriedenstellend gelöst werden.

Angesichts der unaufhaltsamen und dynamischen technischen Entwicklung gilt es aber auch, den (völker-)rechtlichen Rahmen für den Einsatz von elektronischen Wirkmitteln anzupassen und ggf. fortzuentwickeln.[55] Insbesondere beim Unterscheidungsgebot zwischen Kombattanten/Kombattantinnen und Zivilpersonen sowie zwischen militärischer und ziviler Infrastruktur steht das Recht vor bislang noch ungelösten Herausforderungen.[56]

[redacted] [redacted]

55 So kürzlich *Singer,* Cyberwarfare, Fn. 30, S. 23; *Linaki, Cyber Warfare*, Fn. 5, S. 175 f. Andere vertreten die Auffassung, dass das traditionelle Völkerrecht sich so auslegen lasse, dass es keinen Handlungsbedarf gebe. Siehe etwa mit ausführlicher Prüfung *Ziolkowski*, Computernetzwerkoperationen, Fn. 3, S. 213 sowie 209–212. Dagegen *Krieger*, Krieg gegen anonymous, Fn. 18, S. 19 f.

56 So befasst sich etwa das Internationale Rote Kreuz seit mehreren Jahren mit der Thematik des Verhältnisses zwischen neuen Technologien und humanitärem Völkerrecht, siehe etwa den Forschungs- und Debattenzyklus "*New technologies and the modern battlespace: Humanitarian perspectives*" 2014, https://www.icrc.org/eng/resources/documents/event/2014/03-06-research-and-debate-cycle-1.htm (mit Podcasts, Videos und weiteren Nachweisen; letzter Zugriff: 19.02.2015). Siehe auch "*Cyber warfare: Legal experts and programmers search for solutions*" (November 2014), https://www.icrc.org/en/document/cyber-warfare-legal-experts-and-programmers-search-solutions (letzter Zugriff: 19.02.2015).

## 6. Anlagen

**Anlage 1:**
*Woltag, Johann-Christoph*, *Cyber Warfare*, in: Max Planck Encyclopedia of Public International Law (Bearbeitungsstand: Mai 2010), erhältlich über http://opil.ouplaw.com/ (letzter Zugriff: 20.02.2015).

**Anlage 2:**
*Reinhold, Thomas*, Internationale Kooperationsrichtlinien – ein Ausweg aus dem Attributionsdilemma, in: Sicherheit + Frieden 2014, S. 23–27.

## 7. Liste vertiefender Literaturweise

Aufgrund der Aktualität und Zukunftsträchtigkeit der Thematik der elektronischen Kriegsführung als solche sollen folgende Aufsätze zur vertiefenden Lektüre empfohlen werden:

- *Caton, Jeffrey L.*, *Distinguishing acts of war in cyberspace: assessment criteria, policy considerations, and response implications*, Strategic Studies Institute, United States Army War College, Oktober 2014.

- *Dinniss, Heather Harrison*, Cyber Warfare and the Law of War, Cambridge: Cambridge University Press 2012.

- *Döge, Jenny, Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime*, in: Archiv des Völkerrechts, Band 48 (2010), S. 486–501.

- *Droege, Cordula*, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*, in: International Review of the Red Cross, Band 94 (2012), S. 533–578.

- *Farwell, James P./Rohozinski, Rafal, Stuxnet and the future of cyber war*, in: Survival: global politics and strategy, Band 53 (2011), S. 23–40.

- *Geiß, Robin/Lahmann, Henning, Cyber warfare: applying the principle of distinction in an interconnected space*, in: Israel Law Review, 2012, Band 45 (3), S. 381–399.

- *Hathaway, Oona A./Crootof, Rebecca/Levitz, Philip/Nix, Haley/Nowlan, Aileen/Perdue, William/Spiegel, Julia*, *The Law of Cyber-Attack*, in: California Law Review, Band 100 (2012), S. 817–886.

- *Heintschel von Heinegg*, *Wolff*, Cyberspace – ein völkerrechtliches Niemandsland, in: *Schmidt-Radefeldt/Meissler* (Hrsg.), Automatisierung und Digitalisierung des Krieges, Baden-Baden: Nomos 2012, S. 159.

- *Jensen, Eric Talbot, Cyber Attacks: Proportionality and Precautions in Attack*, in: International Law Studies, U.S. Naval War College, Band 89 (2013), S. 198–217.

- *Keber, Tobias O./Roguski, Przemysław Nick*, Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis, in: Archiv des Völkerrechts, Band 49 (2011), S. 399–434.

- *Kenney, Michael, Cyber-Terrorism in a Post-Stuxnet World*, in: Foreign Policy Research Institute, Orbis, Band 59 (2015), S. 111–128.

- *Knake, Robert*, Untangling Attribution: Moving to Accountability in Cyberspace (2010), www.cfr.org/united-states/untangling-attribution-moving-accountabilitycyberspace/p22630 (letzter Zugriff: 23.02.2015).

- *Krieger, Heike*, Krieg gegen anonymous: völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, in: Archiv des Völkerrechts, Band 50 (2012), S. 1–20.

- *Lin, Herbert*, *Cyber conflict and international humanitarian law*, in: International Review of the Red Cross, Band 94 (2012), S. 515–531.

- *Linaki, Evangelia*, *Cyber Warfare and International Humanitarian Law: a Matter of Applicability*, in: Humanitäres Völkerrecht – Informationsschriften, 2014, S. 169–176.

- *Lubell, Noam, Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, in: International Law Studies, U.S. Naval War College, Band 89 (2013), S. 252–275.

- *Lülf, Charlotte*, *International Humanitarian Law in Times of Contemporary Warfare – The New Challenge of Cyber Attacks and Civilian Participation,* in: Humanitäres Völkerrecht – Informationsschriften, 2013, S. 74–82.

- *Melzer, Nils*, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research (UNIDIR) Resources (2011), http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (letzter Zugriff: 23.02.2015).

- *Meulenbelt, Stephanie, The "worm" as a weapon of mass destruction: how to respond legally to cyber-warfare?*, in: RUSI journal, Band 157 (2012), S. 62–67.

- *Padmanabhan, Vijay M., Cyber Warriors and the Jus in Bello,* in: International Law Studies, U.S. Naval War College, Band 89 (2013), S. 288–308.

- *Plate, Tobias*, Völkerrechtliche Fragen bei Gefahrenabwehrmaßnahmen gegen Cyber-Angriffe, in: Zeitschrift für Rechtspolitik (ZRP), Band 44 (2011), S. 200–202.

- *Schaller, Christian*, Internationale Sicherheit und Völkerrecht im Cyberspace: für klarere Regeln und mehr Verantwortung, Berlin, Stiftung Wissenschaft und Politik, Studie 18/2014.

- *Schmitt, Michael N., International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, in: Harvard International Law Journal, Band 54 (2012), S. 13–37, http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (letzter Zugriff: 18.02.2015).

- *Ders., Classification of Cyber Conflict*, in: International Law Studies, U.S. Naval War College, Band 89 (2013), S. 233–251.

- *Singer, Tassilo*, Cyberwarfare – Damoklesschwert für das Völkerrecht?, in: Sicherheit + Frieden, 2014, S. 17–23.

- *Stadlmeier, Sigmar/Unger, Walter J.*, Cyber War und Cyber Terrorismus aus völkerrechtlicher Sicht, in: *Schmalenbach, Kirsten* (Hrsg.), Aktuelle Herausforderungen des Völkerrechts, Frankfurt/Main: Peter Lang (2012), S. 63–80.

- *Theeuwen, Wieteke, Cyberspace Operations in International Armed Conflict: The Principles of Distinction and Proportionality in Relation to Military Objects*, in: Humanitäres Völkerrecht – Informationsschriften, 2013, S. 188–194.

- *Watts, Sean, Combatant Status and Computer Network Attack*, in: Virginia Journal of International Law, Band 50 (2010), S. 392–447.

- *Waxman, Matthew C., Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in: Yale Journal of International Law, Band 36 (2011), S. 421–459.

- *Ziolkowski, Katharina*, Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen: zum „virtuellen Raum“ des Internet und dem Schutzstandard der vor 30 Jahren in Kraft getretenen Protokolle“, in: Humanitäres Völkerrecht – Informationsschriften, 2008, S. 202–213.