Cyberwarfare – Damoklesschwert für das Völkerrecht?

Tassilo Singer*

Abstract: The technological developments in cyberspace enable worldwide economic growth and international communication networks but also pose new threats by criminality and new means and methods of warfare. Therefore, it is of great importance for all states to develop strategies to deal with these issues concerning the security, prosperity and freedom of their countries, but also the international community at large. As cyberspace operates across borders, cyberwarfare becomes a challenge for international law. This article summarizes the cybersecurity strategies of Germany and the USA in view of the classification of cyberwarfare, followed by an evaluation of international law and law of armed conflict regarding state responsibility, the principle of non-intervention, the use of force, the right of self-defense and the principles of the *ius in bello* also considering the status as combatant.

Keywords: Cyberwarfare, cyberterrorism, cyber (security) strategies, international law, law of armed conflict
Cyberkrieg, Cyberterrorismus, Cyber(sicherheits-)strategien, Völkerrecht, Humanitäres Völkerrecht

1. Einordnung von Cyberwarfare und Begriff der Cyberoperation

Glaubt man der Berichterstattung in den Medien, so droht früher oder später das digitale Schwert des sogenannten *Cyberwars* auf die Welt niederzugehen. Die Bedeutungsschwere dieses Urteils soll sich in den Augen des Betrachters aus der Neuheit der Technologie und damit aus ungeklärten Problemen und Gefahren, die diese mit sich bringen soll, ergeben.[1] Die technische Unkenntnis der Bevölkerung („Neuland") verhilft diesen Unkenrufen zu einem großen Echo. Leider wird dabei der Begriff des Cyberwars oft für jegliche Art von Vorfällen im Zusammenhang mit Computern, Computertechnik und dem Internet verwendet, ohne dabei klar von *Cyberkriminalität* abzugrenzen und festzustellen, dass *Cyberwar* eine Zustandsbeschreibung eines Krieges mit Cybermitteln meint, welcher so in der Realität (noch) nicht stattfindet.[2] Vielmehr muss man im Kontext einer Kriegführung mit Cybermitteln von dem Begriff der *Cyberwarfare* reden. Dieser Begriff muss weit verstanden werden und enthält dabei nicht nur direkte Angriffe i.S.v. Kampfhandlungen, sondern umfasst darüber hinaus auch unterstützende, allgemeine Aktivitäten wie Cyberoperationen. Eine Cyberoperation bedeutet die Nutzung von Cyberfähigkeiten mit dem Zweck, bestimmte Ziele durch die Nutzung des Cyberspace sowohl innerhalb als auch außerhalb desselben zu erreichen.[3] Davon ausgehend stellt sich die Frage, ob denn *Cyberwarfare* eine derartige Neuheit darstellt, dass dies in den für die Kriegführung relevanten Rechtsordnungen des internationalen Rechts (Anwendungs-)Probleme aufwirft, mithin also Rechtsetzungsbedarf besteht. Gleichwohl steht fest, dass eine große Zahl von Staaten eine Integration von Mitteln der Cyberkriegführung in zivile und militärische (Sicherheits-)Strategien bzw. in ihre Maßnahmenkataloge vorbereitet bzw. bereits vorgenommen hat. Im Folgenden wird daher ein Überblick über die Strategien Deutschlands und der USA gegeben, dem eine rechtliche Einordnung in die Systematik des internationalen Rechts folgt. Abgeschlossen werden die Ausführungen mit Erläuterungen über humanitär-völkerrechtliche Problemstellungen, insbesondere mit Blick auf Kombattanten und an Kampfhandlungen beteiligte Zivilisten.

2. Die Cyber(sicherheits-)strategien Deutschlands und der USA

Die Cyberstrategie Deutschlands orientiert sich vor allem am Bedürfnis der Sicherheit vor Cyberangriffen und Cyberkriminalität bei gleichzeitiger Bewahrung der Freiheit und der Verfügbarkeit des Internets. Dabei wird ein Gleichlauf von nationalen und internationalen Maßnahmen in Form von Rechtsetzung, Durchsetzungsmechanismen und der Erarbeitung von Mindeststandards angestrebt. Strategische Ziele sind v. a. der Schutz kritischer Informations-Infrastrukturen, die Sicherheit von IT-Systemen in Deutschland, die Stärkung von IT-Sicherheit der öffentlichen Verwaltung und die effektive Verbrechensbekämpfung im Cyberspace.[4] Erreicht werden sollen diese Ziele auf internationaler Ebene durch eine kooperative Vorgehensweise in internationalen Organisationen und Verbänden, insbesondere in den UN, der EU, der NATO aber auch der G8 und der OSZE.[5] Neben einem Fokus auf Cyberkriminalität soll insbesondere der Schutz vor Spionage und Sabotage verstärkt werden.[6] Eine Schaffung von gemeinsamen Fähigkeiten für Cyberangriffe mit Partnerländern ist nicht geplant.[7] Was die rechtliche Beurteilung von *Cyberwarfare* betrifft, geht die Bundeswehr von einer Anwendbarkeit des humanitären Völkerrechts aus; das 2013 veröffentlichte Tallinn Manual wird aber

* Tassilo Singer ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Öffentliches Recht, insb. Völkerrecht, Europarecht und ausländisches Verfassungsrecht an der Europa-Universität Viadrina in Frankfurt (Oder), singer@europa-uni.de.

1 Vgl. dazu die regelmäßige Nachrichtenberichterstattung bei den Themenseiten der ZEIT und Spiegel Online: http://www.zeit.de/schlagworte/themen/cyberwar/index, http://www.spiegel.de/thema/cyberwar/.

2 Zum heutigen Zeitpunkt hat die Staatengemeinschaft noch zu keinem Zeitpunkt die Rechtsauffassung vertreten, dass ein „Cyberkrieg" stattfindet oder stattgefunden habe: Tallinn Manual on the International Law Applicable to Cyberwarfare, Schmitt (Hrsg.) Cambridge University Press, 2013, S. 57f.

3 Tallinn Manual (Anm. 2), Glossary, S. 258.

4 Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Inneren, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, S. 4ff.

5 Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Inneren, S. 4f, 11.

6 Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Inneren, S.10, 14f.

7 BT Drs. 17 Nr. 6971, S. 7, Nr.10d).

nicht notwendigerweise als rechtsverbindlich angesehen.[8] Die Bundesregierung hat 2011 die Auffassung vertreten, dass „ein Cyber-Angriff nur dann als bewaffneter Angriff im Sinne des Völkerrechts einzuordnen wäre, wenn dieser in seiner Wirkung die Schwelle zum bewaffneten Konflikt überschreiten würde und sich mit derjenigen herkömmlicher Waffen vergleichen ließe."[9] Ein solcher Cyberangriff könne, wenn er sich einem Staat zurechnen lässt und im Einzelfall diese Schwelle nach Beurteilung sämtlicher Umstände überschreitet, das Selbstverteidigungsrecht gem. Art. 51 der UN-Charta auslösen.[10]

Die „International Strategy for Cyberspace" der USA zielt darauf ab, eine offene, interoperable, sichere und zuverlässige Informations- und Kommunikationsstruktur zu schaffen, die mit dem internationalen Handel und der Wirtschaft im Einklang steht, die internationale Sicherheit stärkt und das Recht zur freien Meinungsäußerung sowie Innovationen fördert.[11] Um diese Ziele zu verwirklichen, sollen Verteidigung, Entwicklung und Diplomatie kombiniert werden, um auch im 21. Jahrhundert international einen Geist der Kooperation und kollektiven Verantwortung zu schaffen und damit ebenfalls ein Vorgehen im Rahmen von internationalen Organisationen, bi- und multilateralen Partnerschaften und eine Zusammenarbeit mit dem privaten Sektor anzustreben.[12] Die damit verbundene Rechtsauffassung der USA lässt dabei eine relative Kongruenz zu den im Tallinn Manual vertretenen Positionen erkennen.[13] Danach sind die anerkannten (Grund-)Prinzipien des internationalen Rechts auf den Cyberspace anwendbar und Staaten rechtlich für Aktivitäten durch „Proxy"-Akteure verantwortlich,[14] wenn diese auf staatliche Anweisungen oder unter staatlicher Kontrolle handeln.[15] Unter bestimmten Umständen können Cyberoperationen demnach eine Gewaltanwendung i.S.v. Art. 2 (4) UN-Charta darstellen. Wenn diese Tod, Verletzung oder Zerstörung unmittelbar nach sich ziehen, soll diese Annahme umso eher bejaht werden. Um einen Vorfall daraufhin zu untersuchen, soll der Gesamtzusammenhang des Vorfalls, der Urheber bzw. handelnde Akteur, das Ziel und der Ort, die Wirkung und der Vorsatz evaluiert und in Vergleich zur physischen Wirkung konventioneller Waffen gesetzt werden.[16] Darüber hinaus behalten die Vereinigten Staaten sich auch vor, auf Feindseligkeiten im Cyberspace genauso zu reagieren wie bei allen anderen Bedrohungen ihres Landes, sodass eine Cyberoperation, sofern sie die Schwelle eines bewaffneten Angriffs erreicht, nach der Rechtsansicht der USA auch das Recht auf Selbstverteidigung nach Art. 51 UN-Charta auslösen kann.[17] Schließlich wird die Anwendbarkeit von humanitärem Völkerrecht auch bei Cyberoperationen und -mitteln bejaht und damit auch die damit verbundenen Grundprinzipien, wie der Unterscheidungsgrundsatz, das Prinzip der Verhältnismäßigkeit und das Prinzip der Notwendigkeit i. R. der Selbstverteidigung und die Pflicht zur rechtlichen Überprüfung.[18]

3. Staatenverantwortlichkeit für Cyberoperationen

Cyberoperationen können bspw. durch einen Eingriff in die Handlungsfähigkeit eines anderen Staates eine Verletzung von internationalem Recht bewirken. Kann man diesen Akt einem Staat zurechnen, wird die Staatenverantwortlichkeit nach den völkergewohnheitsrechtlich anerkannten Regeln ausgelöst.[19] Die dazu notwendige Rechtsverletzung kann sich dabei aus einer Verletzung von Friedensrecht wie dem Interventionsverbot, der UN-Charta oder einem Verstoß gegen eine Verpflichtung aus humanitärem Völkerrecht ergeben.[20] Primär gilt im Rahmen der Staatenverantwortlichkeit, dass jedes Handeln oder Unterlassen eines Staatsorgans dem jeweiligen Staat zuzurechnen ist.[21] Weiterhin ist auch ein *Ultra-vires*-Handeln eines Staates demselben zurechenbar und weiterhin auch jeder Akt von Personen oder juristischen Personen, die, ohne Staatsorgane zu sein, durch nationale Gesetze zu staatlichem Handeln ermächtigt sind. Unter bestimmten Umständen können auch Akte von nichtstaatlichen Akteuren, die auf Anweisung oder unter Leitung bzw. unter Kontrolle des Staates handeln, diesem Staat als eigene Handlungen zugerechnet werden.[22] Bei Letzterem stellt sich aber das Problem, nach welchen Kriterien man die Kontrolle des Staates feststellen kann. Im internationalen Recht werden vor allem der Effective-Control-Test[23] und der Overall-Control-Test[24] verwendet.[25] In Bezug auf *Cyberwarfare* muss man aber feststellen, dass es, um die Rechtsfolgen der Staatenverantwortlichkeit auslösen zu können, eines Nachweises bedarf. Dies dürfte aus praktischen Erwägungen bei einem Overall-Control-Test deutlich schwieriger gelingen; gänzlich ausgeschlossen werden kann es dennoch nicht. Eine allgemeine Kontrolle in Form einer überblickenden Überwachung und groben Steuerung bspw. einer Hackergruppe durch einen staatlichen Akteur dürfte angesichts einer technisch schwierigen Grenzziehung zwischen polizei- und sicherheitsrechtlicher Überwachung und der Kontrolle im oben genannten Sinne

8 Bundesministerium der Verteidigung (Hrsg.), Humanitäres Völkerrecht in bewaffneten Konflikten – Handbuch – Zentrale Dienstvorschrift 15/2, Bonn, Mai 2013, S. 18, Nr. 131, S. 70, Nr. 486. Das Tallinn Manual stellt eine rechtlich unverbindliche Empfehlung dar und wurde von internationalen Experten im Rahmen des NATO Cooperative Defence Centers of Excellence erarbeitet. Es spiegelt aber nicht die Rechtsauffassung der NATO oder Ihrer Mitgliedsstaaten wider.
9 BT Drs. 17 Nr. 6971 (Anm. 7), S. 4, Nr. 5.
10 BT Drs. 17 Nr. 6971 (Anm. 7), S. 4, Nr. 7.
11 The White House, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, 2011, S. 8.
12 The White House (Anm. 11), S. 11.
13 Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, Online Volume 54, 2012, S. 15, aufgerufen am 08.11.2013: http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf.
14 Koh, International Law in Cyberspace, Harvard International Law Journal Online 54 (2012), S. 2f, aufgerufen am 08.11.2013: http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.
15 Koh (Anm. 14), S. 6f.
16 Koh (Anm. 14), S. 3f.
17 Koh (Anm. 14), S. 4; The White House (Anm.11), S. 14.
18 Koh (Anm. 14), S. 3, 5.
19 Art. 1, ILC, Draft articles on Responsibility of states for internationally wrongful acts, Rep. of the Int. Law Commission, 53d Sess., UN. Doc. A/56/10 (2001); Tallinn Manual (Anm.2), Rule 6, S. 29.
20 Tallinn Manual (Anm.2), S. 29f.
21 ILC (Anm. 19), Art. 4 (1), (2); Tallinn Manual (Anm. 2), S. 30f.
22 ILC (Anm. 19), Art. 5 ff; Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies, Volume 89, US Naval War College, 2013, S. 139; Tallinn Manual (Anm. 2), S. 31f.
23 ICJ, *Military and Paramilitary Activities in and against Nicaragua*, ICJ Reports 1986, S.14 (62), Rn. 109ff.
24 ICTY, *Prosecutor v Tadic*, Case No. IT-94-1-A, Judgment on Appeal (International Criminal Tribunal for the former Yugoslavia July 15, 1999), Rn. 131 ff.
25 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), I.C.J. Reports 2007, S. 43, para. 404; Tallinn Manual (Anm.2), S. 32f.

kaum nachvollziehbar sein.[26] Eine abschließende Entscheidung kann aber nicht getroffen werden und muss sich letztlich an den Umständen des Einzelfalls orientieren. Abgesehen von einer rechtlich möglichen Einordnung in die Systematik stellen sich die größten Probleme bei dem technischen Nachweis der Urheberschaft,[27] was an der systemimmanenten Natur von Cyberoperationen und den ihnen zugrunde liegenden technischen Prozessen des Datenaustauschs liegt.[28] Einer rechtlichen Fiktion, eine Verpflichtung aus der territorialen Souveränität eines Staates zu konstruieren, ist aber zu widersprechen. Daraus würden zwangsläufig schwer zu bewältigende Kontrollverpflichtungen der Staaten erwachsen und zwingende Einschränkungen von Freiheitsrechten würden mit einer solchen Konstruktion einhergehen.[29] Teilnehmer an Cyberoperationen haben oft zum Ziel, unerkannt zu agieren bzw. falsche Fährten zur Verschleierung ihrer Herkunft zu legen. Dies kann durch die Kaskadierung von mehreren Computern oder Servern erreicht werden, die wiederum nur einzelne Funktionen oder *Command-&-Control*-Fähigkeiten aufweisen. Eine neue Erscheinung in diesem Zusammenhang stellt das Eindringen und Nutzen sog. *Peer-to-Peer*-Netzwerke dar,[30] durch welche einzelne Module im Rahmen der Cloud miteinander interagieren und kommunizieren können, ohne direkt einem Standort zugeordnet zu werden. Kann den aufgeführten Schwierigkeiten zum Trotz die Verantwortlichkeit eines Staates über die angeführten Regeln angenommen werden, ist der betroffene Staat dazu berechtigt, verhältnismäßige Gegenmaßnahmen i. S. d. Völkerrechts[31] gegen den anderen Staat auszuüben. Voraussetzung hierfür ist, dass der Angriff andauert und die Gegenmaßnahmen nur zum Zweck, den Staat zu völkerrechtskonformen Handeln zu bewegen, erfolgen.[32]

4. Völkerrechtliches Interventionsverbot

Die Rechtswidrigkeit von *Cyberwarfare* kann schon dann angenommen werden, wenn gegen das Interventionsverbot[33] verstoßen wird. Dies ist dann der Fall, wenn durch Cyberoperationen in die inneren Angelegenheiten eines Staates, die die Verfassungsordnung und das politische, wirtschaftliche, soziale und kulturelle System umfassen,[34] eingegriffen wird.[35] Wenn die erforderliche Schwelle der „Methods of Coercion" erreicht wird, kann auch Cyber-Spionage als Verstoß gegen das Prinzips der Nicht-Intervention qualifiziert werden. Diese Schwelle ist gegeben, wenn die Souveränität und Entscheidungsfreiheit eines Staates durch Maßnahmen eines anderen Staates betroffen werden.[36] Daraus folgt im Gegenzug aber, dass, wenn sie kein zwingendes Element aufweisen, sowohl Cyberoperationen, die nur Informationen erbeuten und auswerten (*Cyber-Exploitation*), als auch Cyberspionage nicht *per se* das Interventionsverbot verletzen.[37] Demgegenüber weisen alle Cyberoperationen, die die Anwendung von Gewalt i.S.v. Art. 2 (4) UN-Charta beinhalten, ein zwingendes Element auf und verletzen damit immer auch das Interventionsverbot.[38] Daraus folgt, dass für Verstöße gegen das Interventionsverbot unterhalb der Schwelle der Gewaltanwendung nur Gegenmaßnahmen auf einer niedrigeren Schwelle zur Verfügung stehen.[39]

5. Verbot der Gewaltanwendung

Das Verbot der Gewaltanwendung ist neben seiner Normierung in Art. 2 (4) UN-Charta auch als Völkergewohnheitsrecht anerkannt[40] und muss unabhängig von der Art der Waffe oder des Mittels anwendbar sein.[41] Dies ist erforderlich, um der sich in konstantem Wandel befindlichen technologischen Entwicklung Rechnung zu tragen und die Geltung des UN-Systems zu erhalten. Daher gilt das Verbot auch für Cyberoperationen i. R. von Cyberkriegführung.[42] Welche Art von Cyberoperationen das Gewaltverbot verletzen, muss mangels näherer international-rechtlicher Konkretisierung unter Bezugnahme auf die Schwellenwerte bei konventionellen Mitteln bestimmt werden. Diese sind anhand von Umfang und Wirkung („scale and effects")[43], also qualitativen und quantitativen Faktoren, zu bestimmen.[44] Taugliche Kriterien sind insbesondere Schwere und Ausmaß (Verbreitung) der Cyberoperation, die Spürbarkeit der Auswirkungen, die zeitliche Unmittelbarkeit und Dauer, der Grad der Beteiligung eines Staates sowie der Grad der Involvierung des staatlichen Militärs.[45] Diese Aufzählung darf allerdings nicht als vollständig betrachtet werden, um die nötige Flexibilität angesichts neuer oder unbekannter Mittel zu garantieren. Zusammenfassend muss somit eine Einzelfallprüfung für jede konkrete Cyberoperation erfolgen und diese muss anhand der obengenannten Kriterien und solchen, die bei der Beurteilung des Gewaltbegriffs bei konventionellen Waffen zu Rate gezogen werden, bewertet werden.

Folgender Fall stellt eine fiktive Konstellation dar, die einem realen Vorfall nachgebildet wurde und diesen abwandelt.[46]

26 Würde eine umfassende Kontrolle des Internets durch Staatsorgane verlangt, hätte dies fatale Auswirkungen auf Freiheitsrechte: Siehe S. 6 sowie FN 29.
27 Vergleiche dazu Mandiant Intelligence Center Report, APT1 Exposing One of China´s Espionage Units Report, 18.02.2013, aufgerufen am 08.11.2013: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; Heintschel von Heinegg (Anm. 22), S. 139f.
28 Vgl. hierzu den Beitrag von Thomas Reinhold in diesem Heft.
29 Heintschel von Heinegg, (Anm. 22), S. 137: *Aus der Duty to Prevention kann, trotz Aussagekraft zu der widerlegbaren Vermutung der Kenntnis eines Staates von Cyberoperationen nicht-staatlicher Akteure, nicht die Zurechenbarkeit einer Handlung zu dem Staat, aus dessen Gebiet die Operation erfolgt ist, gefolgert werden; Tallinn Manual (Anm. 2), Rule 5, S. 26.*
30 Gorodetsky/ Karsaev/ Samoylov/ Serebryakov, Multi-agent Peer-to-Peer Intrusion Detection, Computer Network Security, Gorodetsky Kotenko Skormin (Hrsg.), 2007, S. 260-271.
31 Vitzthum, Völkerrecht, 5.Auflage 2010, Abschnitt VII, S. 595f, Rdnr. 29f.
32 Tallinn Manual (Anm.2), Rule 9, S. 36ff.
33 ICJ (Anm. 23), para. 202ff (202), (205), (228).
34 ICJ (Anm. 23), para. 205; Heintze, Interventionsverbot, Interventionsrecht und Interventionspflicht im Völkerrecht, Maßnahmen zur internationalen Friedenssicherung, Reiter (Hrsg.), 1998, S. 2f.
35 Tallinn Manual (Anm.2), S. 44.
36 ICJ (Anm. 23), para. 205.
37 Das Nichteinmischungsgebot kann aber, anders als das Interventionsverbot, verletzt sein, ohne dass die Maßnahme Zwangswirkung haben muss.
38 ICJ (Anm. 23), para. 205; Tallinn Manual (Anm. 2) S. 44f., S. 51, Nr. 9 (h).
39 Tallinn Manual (Anm. 2), S. 45.
40 ICJ (Anm. 23), para 188; Das Gewaltverbot wird oftmals sogar als Ius Cogens qualifiziert: ICJ (Anm.23), para. 190.
41 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, para. 39.
42 Tallinn Manual (Anm. 2), Rule 10, S. 42ff.
43 ICJ (Anm. 23), para 195.
44 Tallinn Manual (Anm. 2), S. 45 ff; Lülf, International Humanitarian Law in Times of Contemporary Warfare – The new challenge of cyber attacks and civilian participation, Humanitäres Völkerrecht – Informationsschriften 2/2013, S. 74 (77f.); Vgl. Fallgruppen in: Tallinn Manual (Anm. 2), S. 46f.
45 Tallinn Manual (Anm. 2), S. 48 ff.; Vgl. dazu auch: Schmitt (Anm. 13), S. 19; Koh (Anm. 14), S. 4.
46 Tallinn Manual (Anm. 2), S. 58, 83.

Durch ein vom staatlichen Militär effektiv kontrolliertes privates Sicherheitsunternehmen wird eine schadhafte Software („Malware“) für ein konkretes Steuerungssystem, mit dem der Rotationsprozess von Gaszentrifugen bei der Urananreicherung gesteuert wird, entwickelt. Nach erfolgreicher Implikation in ein System eines gegnerischen Staates durch dieses Unternehmen kommt es zu massiven Fehlfunktionen in einer großen Zahl der Zentrifugen. Dadurch explodieren einige der Maschinen, Gas und radioaktive Stoffe treten aus und es kommt zu Verletzten und Toten. In diesem Fall hat eine Cyberoperation mit staatlicher (ggf. militärischer) Beteiligung, die eine klare kausale Verbindung zwischen Cyberoperation und Auswirkungen aufweist, einen Grad an Schwere und ein Ausmaß erreicht, die sich kongruent zu einer konventionellen Aktion wie der Zerstörung einer derartigen Anlage mit einer Sprengladung oder einer lasergesteuerten Rakete verhält. Der Akt weist durch die konkrete Angriffsvariante und Spezialisierung eine derartige Direktheit und Unmittelbarkeit auf, dass die Folgen für den einsetzenden Staat vorhersehbar waren. Somit stellt der Akt eine Ausübung von Gewalt i.S.v. Art. 2 (4) UN-Charta dar und ist damit als Verstoß gegen das Gewaltverbot nach Art. 2 (4) UN-Charta zu werten.

6. *Ius ad bellum* – Selbstverteidigungsrecht

Bei Betrachtung des Beispiels stellt sich mithin die Frage, ob dies nicht auch einen bewaffneten Angriff darstellen kann und damit das Selbstverteidigungsrecht oder „ius ad bellum“ i.S.v. Art. 51 UN-Charta ausgelöst wird. Ein bewaffneter Angriff („armed attack“) muss eine höhere Schwelle der Gewalt erreichen als bei Art. 2 (4) UN-Charta erforderlich ist. Erreicht eine Cyberoperation diese Schwelle, kann das Selbstverteidigungsrecht i.S.v. Art. 51 UN-Charta auslgelöst werden.[47] Eine Cyberoperation, die als ein bewaffneter Angriff i.S.v. Art. 51 UN-Charta qualifiziert werden kann, umfasst auch immer eine Gewaltanwendung i.S.v. Art. 2 (4) UN-Charta als schwerste Ausprägung derselben. Allerdings ist umgekehrt nicht jede Gewaltanwendung i.S.v. Art. 2 (4) ein bewaffneter Angriff.[48] Ein bewaffneter Angriff muss immer über ein grenzüberschreitendes Element verfügen.[49] In Fällen, in denen nichtstaatliche Akteure einen anderen Staat angreifen, ohne dass deren Handeln einem Staat nach den bereits erwähnten Regeln zurechenbar ist, ist dies problematisch.[50]

Weiterhin ist fraglich, ob begriffsnotwendig der Einsatz einer *Waffe* erforderlich ist. Um im Einklang mit der „Nuclear Weapons“-Entscheidung und der „Nicaragua“-Entscheidung des IGH zu argumentieren,[51] muss aber vielmehr entscheidend sein, welche Wirkung das eingesetzte Mittel hat und ob dieses mit der Wirkung von kinetischen Waffen vergleichbar ist.[52] Diese Interpretation ermöglicht weiterhin, den Besonderheiten von *Cyberwarfare* Rechnung zu tragen, bei der eine eindeutige Qualifizierung von eingesetzten Cybermitteln als Waffe oft nicht möglich ist. Daraus folgt, dass die Sammlung und der Diebstahl von Informationen aufgrund der vergleichsweise geringen Wirkung nicht als bewaffnete Angriffe eingeordnet werden können.[53] Gegen die Einordnung von Spionage als Angriff i.S.v. Art.51 UN-Charta spricht weiterhin, dass der Tatbestand des Art. 51 UN-Charta aufgrund der Zielsetzung der Wiederherstellung des Weltfriedens und wegen des Ausnahmecharakters des Rechts auf Selbstverteidigung im Kontext der UN-Charter restriktiv zu verstehen ist.[54] Dies geschieht auch, um eine Ausdehnung des Selbstverteidigungsrechts auf Spionage, die mitunter als legal angesehen wird,[55] wegen einer sonst damit verbundenen Konflikteskalation zu vermeiden. Ein Vorgehen gegen Wirtschaftsspionage unter Berufung auf Art. 51 UN-Charta ist somit nicht möglich. Demgegenüber erreicht eine Cyberoperation, die Menschen verletzt oder tötet bzw. Eigentum beschädigt oder zerstört[56] angesichts der Vergleichbarkeit der Wirkung mit der eines konventionellen Waffeneinsatzes die Schwelle eines bewaffneten Angriffs. Im obengenannten Beispielsfall würde daher auch das Selbstverteidigungsrecht nach Art. 51 UN-Charta ausgelöst.[57]

7. *Ius in bello* – Humanitäres Völkerrecht und Cyberwarfare

Schließlich muss die Cyberkriegführung auch in das humanitäre Völkerrecht eingeordnet werden. Die Anwendbarkeit hängt dabei von dem Vorliegen eines bewaffneten Konflikts ab. Eine Cyberoperation muss hierfür einen Nexus zu einem bewaffneten Konflikt aufweisen.

7.1 Anwendbarkeit von Humanitärem Völkerrecht

Das humanitäre Völkerrecht ist einerseits bei Cyberkriegführung anwendbar, wenn der Konflikt die Kriterien international und bewaffnet erfüllt (internationaler bewaffneter Konflikt).[58] Neben einem (regulären) Konflikt zwischen zwei Staaten ist auch dann ein internationaler Konflikt gegeben, wenn Handlungen von nichtstaatlichen Akteuren einem Staat zugerechnet werden können. Die Zurechenbarkeit und die Frage, ob ein Konflikt durch die Zurechnung der nichtstaatlichen Akteure als international eingeordnet wird, bestimmen sich nach dem Overall-Control-Test.[59] Mangels eines präzisen, begriffsklaren Tests muss jedoch ein hoher Schwellenwert angelegt werden. Es reicht demnach nicht aus, wenn der Staat der Gruppe den Zugang zur Cyberinfrastruktur aufrechterhält. Ebenso genügt

47 Tallinn Manual (Anm. 2),Rule 13, S. 54.
48 ICJ (Anm. 23), para. 191; Tallinn Manual (Anm.2), S. 47 f., 6 ff.; S. 55.
49 Tallinn Manual (Anm. 2), S. 54, 2.
50 Ausführlich: Tallinn Manual (Anm. 2), S. 58f.; ICJ, *Armed Activities in Congo*, Judgment, para. 146f.
51 „Regardless of the weapons employed“: ICJ (Anm. 39), para. 39; ICJ (Anm. 23), para. 195.
52 Tallinn Manual (Anm. 2), S. 55.
53 Tallinn Manual (Anm.2), S. 55.
54 Lauterpacht, Oppenheim's International Law, 1952, S. 156; Brownlie, International Law and the Use of Force by States, 1963, S. 255, 265, 271-273.
55 Tallinn Manual (Anm. 2), S. 50f.
56 Ein solcher Angriff wird im Tallinn Manual als *Cyberangriff („Cyber attack“)* definiert: Tallinn Manual (Anm.2), Rule 30, S. 106.
57 Vergleiche dazu die Diskussion von Stuxnet: Tallinn Manual (Anm.2), S.58; Koh (Anm. 14), S. 4.
58 Gemeinsamer Artikel 2 der Genfer Konventionen von 1949, 12. August 1949.
59 ICTY (Anm. 24), paras. 131, 145, 162; ICJ (Anm. 25), para. 404; s.o. Staatenverantwortlichkeit, S. 2f.

es nicht, die Gruppe mit Werkzeugen für Cyberangriffe zu versorgen. Ausreichend ist es hingegen, wenn der Staat die Gruppe mit spezifischen (Geheim-)Informationen versorgt, die die Schwachpunkte des Gegners für Cyberangriffe aufzeigen.[60]

Das Merkmal „bewaffnet" erfordert das Bestehen von Feindseligkeiten. Feindseligkeiten setzen die kollektive Verwendung von Mitteln und Methoden der Kriegführung voraus. Cyberoperationen können den notwendigen Schwellenwert alleine erfüllen. Bei der Frage nach dem Ausmaß der Gewalt, das notwendig für eine Einordnung als Feindseligkeit ist, ist dem IKRK zu folgen. Demnach ist jede Differenz zwischen Staaten, die zur Intervention von bewaffneten Truppen führt, ein bewaffneter Konflikt, egal wie lange der Konflikt andauert und welche Opfer der Konflikt hat.[61] Eine andere Meinung hingegen verlangt, dass die bewaffnete Gewalt von größerem Ausmaß und gewisser Dauer und Intensität ist.[62] Letzteres hätte aber zur Folge, dass im Beispielsfall ein bewaffneter Konflikt abzulehnen wäre, obwohl es Tote und Verletzte gibt. Dem humanitären Völkerrecht liegt im Kern der Gedanke zugrunde, Individuen, die nicht in die Kampfhandlungen involviert sind, und deren Eigentum zu schützen.[63] Auch aus dieser Schutzfunktion ist daher zu folgern, dass ein niedriger Schwellenwert zu bevorzugen ist.[64]

Andererseits ist das humanitäre Völkerrecht auch im nichtinternationalen Konflikt anwendbar. Notwendige Voraussetzungen hierfür sind das Vorliegen ausgedehnter bewaffneter Gewalt (protracted violence), ein Mindestmaß an Intensität des Konflikts und die Tatsache, dass die erforderliche Gewalt zwischen einem Staat und einer oder mehreren organisierten bewaffneten Gruppierungen (organized armed group – OAG) oder zwischen diesen Gruppierungen untereinander ausgeübt werden muss.[65] Hierbei stellt sich das Problem, dass oftmals Cyberoperationen nicht die Schwelle der Intensität erreichen, die konventionelle Angriffe beinhalten.[66] Ferner ist problematisch, ob die notwendigen Voraussetzungen einer organisierten bewaffneten Gruppierung[67] durch eine „Cyber"-OAG erfüllt werden können. Dazu gehört auch, dass die Konfliktparteien über ein Mindestmaß an Organisation verfügen müssen. Bei Cyber- oder Hackergruppen gibt es hierbei erhebliche Schwierigkeiten, u. a. deren Anonymität, die oftmals fehlende hierarchische Befehlsstruktur, die Kontinuität des Zusammenwirkens, das Teilen von Angriffsmitteln, das kooperative Zusammenwirken, die Kontrolle von Gebiet und generell die Kapazitäten zu mehr als einzelnen Cyberoperationen. Jedenfalls ist bei Hackergruppen eine Entscheidung im Einzelfall notwendig. In den meisten Fällen dürften Hackergruppen nicht die Voraussetzungen einer organisierten bewaffneten Gruppierung erfüllen. Grundsätzlich ist es aber möglich, dass ein nicht-internationaler bewaffneter Konflikt auch *Cyberwarfare* (mit-)beinhaltet. *Cyberwarfare* wird dabei aber meist nur einen Teil der Mittel und Methoden der Konfliktführung darstellen.

7.2 Grundprinzipien des Humanitären Völkerrechts

Ist der Anwendungsbereich eröffnet, finden die Grundprinzipien des humanitären Völkerrechts Anwendung auf *Cyberwarfare*. Diese Prinzipien sind unabhängig von der Differenzierung der Konfliktarten als Völkergewohnheitsrecht anerkannt und müssen daher immer bei Kampfhandlungen beachtet werden.[68] Der Unterscheidungsgrundsatz verpflichtet zur Unterscheidung zwischen legitimen und illegitimen Zielen bei einer Kampfhandlung.[69] Ein Mittel von Cyberattacken stellen sog. Würmer dar. Diese Programme haben neben ihrer Primärfunktion (bspw. Spionage oder Sabotage) einen Vervielfältigungsmechanismus integriert, mit dessen Hilfe sie sich ohne zusätzlichen Befehl von außen autonom vervielfältigen, d. h. kopieren und ausbreiten können.[70] Daher kann der Angreifer, sobald der Wurm einmal eingesetzt wird, nicht mehr kontrollieren, wohin sich die Malware verbreitet. Hat der Wurm eine Primärfunktion, die die Störung oder Zerstörung von Steuerungsmechanismen von Infrastruktur oder Militäranlagen zum Ziel hat, kann diese Kombination (Vervielfältigung und Zerstörung) bewirken, dass auch Zivilisten von der Wirkung betroffen sind, bspw. wenn dadurch Raketen ungesteuert abgefeuert würden oder Umspannwerke explodieren. Daher kann der Einsatz von Computerwürmern gegen den Unterscheidungsgrundsatz verstoßen. Gleiches gilt für das Verbot unterschiedsloser Angriffe, also solchen, bei denen von der Natur des Mittels aus nicht der Unterscheidungsgrundsatz eingehalten werden kann, das Mittel also nicht zwischen Zielen differenzieren kann.[71] Daher sind auch diejenigen Mittel und Methoden der *Cyberwarfare* untersagt, die unterschiedslos kinetische Wirkung hervorrufen können. Dies kann sowohl Malware sein, die auf öffentlich zugänglichen Webseiten platziert wird, das können aber auch Würmer oder Viren sein, die freigesetzt werden. Weiterhin muss ex ante zwischen den Folgen des Angriffs für die Zivilbevölkerung und dem durch den Angriff erwarteten militärischen Vorteil abgewogen werden. Steht das Leid der Zivilbevölkerung in grobem Missverhältnis zu dem erzielten

60 Tallinn Manual (Anm. 2), S. 81.
61 ICRC, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field: commentary, Volume I, Pictet (Hrsg.), 1952, S. 32; ICRC, Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea: commentary, Volume II, Pictet (Hrsg.), 1960, S. 28; ICRC, Geneva Convention Relative to the Treatment of Prisoners of War, Volume III, Pictet (Hrsg.), 1960, 23; ICRC, Geneva Convention Relative to the Protection of Civilian Persons in Time of War: commentary, Volume IV, Pictet (Hrsg.),1958, S. 20.
62 Tallinn Manual (Anm. 2), S. 82f.
63 Schmitt, Wired warfare: Computer network attack and jus in bello, IRRC June 2002, Vol. 84, No. 846, S. 373f.
64 Tallinn Manual (Anm. 2), S. 83.
65 Tallinn Manual (Anm. 2), Rule 23, S. 84ff.; Gemeinsamer Artikel 3 der Genfer Konventionen von 1949, 12. August 1949; ICTY, *Prosecutor v Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2. October 1995, para. 70.
66 Tallinn Manual (Anm. 2), S. 87.
67 ICTY, *Prosecutor v Fatmir Limay, Haradin Bala, Isak Musliu*, Case No. IT-03-66-T, Judgment, 30 November 2005, paras. 94-129; Tallinn Manual (Anm. 2), S. 88ff.
68 ICJ (Anm. 39), S. 226ff., Rdnr. 78.
69 Henckaerts/Doswald-Beck, Customary International Humanitarian Law, Volume I: Rules, Hrsg. ICRC, Cambridge University Press, Part I, Chapter 2, Rule 7, S. 25; Vgl. Art. 48 ZP I, Art. 51, 52 ZP I; Völkergewohnheitsrecht: Henckaerts/Doswald-Beck, Customary International Humanitarian Law, Part I, Chapter 1, Rule 1, S. 3; Vgl. dazu: Lülf (Anm. 42), die den Unterscheidungsgrundsatz im Zusammenhang mit kontrollierten, auf ein spezifisches Ziel gerichteten Cyberoperationen erörtert, S. 78.
70 Lülf (Anm. 42), S. 76; Tallinn Manual (Anm. 2), Glossary, S. 262.
71 Henckaerts/ Doswald-Beck (Anm. 64), Part I, Chapter 3, Rule 12, S. 40; Vergleiche hierzu: Gauseweg, Computerwürmer und Cyberwarfare, WiSi – Band VIII, Aktuelle Einsatzszenarien der Bundeswehr – rechtliche Herausforderungen (AT),Forster/Vugrin/Wessendorff (Hrsg.), im Erscheinen 2014.

Vorteil, ist ein Angriff rechtswidrig.[72] Daher dürfen im Rahmen von *Cyberwarfare* keine Mittel eingesetzt werden, die nach ihrem ersten Einsetzen unkontrollierbar sind und grenzenlos weitere Schäden als die ex ante antizipierten hervorrufen oder sich selbstständig verbreiten können. Auch ist der Einsatz von Cybermitteln verboten, die unnötige Leiden verursachen.[73] Dies können unter Umständen spezielle Programme sein, die gezielt zur Sabotage von kritischer Infrastruktur eingesetzt werden, wie bspw. Steuerungssoftware von Dämmen oder Kernkraftwerken. Würde durch *Cyberwarfare* ein Kernkraftwerk beschädigt, sodass Strahlung austritt und von dessen Strahlung Kombattanten oder Zivilbevölkerung betroffen wären, wäre dieses Verbot verletzt. Schließlich müssen bei *Cyberwarfare*, ebenso wie bei allen anderen Mitteln und Methoden der Kriegführung, alle praktisch möglichen Vorsichtsmaßnahmen getroffen werden, um zivile Opfer und unverhältnismäßige Angriffe zu vermeiden.[74] Dies hat zur Folge, dass unkontrollierbare, selbstständig (autonom) agierende Cyberoperationen und -mittel in den meisten Fällen für rechtswidrig anzusehen sind. Das Prinzip besagt weiterhin, dass potenzielle Ziele so genau wie möglich identifiziert und verifiziert werden müssen, was ebenfalls bedeutet, dass bei der *Cyberwarfare* keine unkontrollierbaren Angriffe durchgeführt werden dürfen. Letztlich verpflichtet das Prinzip schon bei der Auswahl, das Mittel oder diejenige Methode zu wählen, welches bzw. welche die wenigsten zivilen Opfer und Schäden hervorrufen kann.

7.3 Kombattanten und an Kampfhandlungen beteiligte Zivilisten

Ein weiteres Problem bereitet Cyberwarfare in Bezug auf den Status als Kombattanten im internationalen bewaffneten Konflikt. So wird bezweifelt, ob die bisher angewandten Kriterien für die Bestimmung des Kombattantenstatus[75] im Zusammenhang mit Cyberwarfare anwendbar sind und nicht stattdessen das Kriterium der Zugehörigkeit zu einem Staat ausreichend ist.[76] Dies resultiert insbesondere daraus, dass die traditionellen Voraussetzungen für eine virtuelle Organisation kaum einhaltbar sind.[77] Dennoch dürfen diese Anforderungen nicht aufgeweicht oder abbedungen werden, da dies weitreichende Folgen für die Einhaltung des Rechts hätte. Die Privilegierungen, die mit dem Kombattantenstatus verbunden sind,[78] dürfen nicht an Gruppierungen verliehen werden, die keine Erkennbarkeit als solche aufweisen und noch viel mehr über kein Disziplinarsystem verfügen, das die Einhaltung des humanitären Rechts garantieren kann.

Wenn die entsprechende Person keinen Kombattantenstatus aufweist, muss diese als Zivilist eingeordnet werden. Zivilisten sind aber nur dann als legitime Ziele zu erachten, wenn und *solange* diese direkt an den Feindseligkeiten teilnehmen.[79] Durch die zeitliche Limitierung der Legitimität eines Angriffs entsteht dabei ein Drehtüreffekt,[80] der die Unterscheidung zwischen legitimen und illegitimen Zielen erheblich erschwert. Da Cyberoperationen sehr schnell und zeiteffizient sind, verschärft sich dieser Effekt erheblich und es dürfte ein Akt der Unmöglichkeit sein, einer einzelnen Attacke eines Zivilisten, die wenige Sekunden gedauert hat, entsprechend legitim zu begegnen. Eine Lösung hierfür wäre bei der Feststellung der direkten Beteiligung nicht nur an die Handlung i.S. des Startens oder des Versendens der Malware anzuknüpfen, sondern an den schadhaften Akt selbst. Das bedeutet, dass die jeweilige Malware entsprechend qualifiziert werden muss und wenn diese weiterhin aktiv ist oder ihre Wirkung entfalten kann, ist von einer direkten Teilnahme an Kampfhandlungen für diese Dauer auszugehen. Einen Cyberangriff mit (zeitlich) verzögertem Effekt einzusetzen ist dabei von einem Menschen, der Minen legt, abzugrenzen. Bei einer Mine läuft einerseits kein Prozess in der Mine selbst weiter. Auch ist das Zeitfenster für einen legitimen Angriff bei einem Minenleger wesentlich größer. Wird hingegen ein Cyberangriff gestartet, wird ein Rechenprozess in Gang gesetzt, d.h. es findet kontinuierlich eine Aktivität im jeweiligen Schadprogramm statt, selbst wenn dieses ruht und einen Countdown oder eine Bedingung abwartet, um danach wieder aktiv zu werden. Der Prozess läuft also meist noch, nachdem der Mensch seine Aktivität schon längst eingestellt hat. Aufgrund der systemimmanenten schweren Erkennbarkeit derartiger Programme, entdeckt man in den meisten Fällen ein Schadprogramm erst mit Eintritt des Schadens. Würde man den Anknüpfungspunkt für einen legitimen Angriff auf den Zivilisten, bei der nur sekundenlangen Aktivität des Menschen belassen, würde man damit den Teilnehmer, der verzögerte, schwer entdeckbare Mittel einsetzt, gegenüber einem regulär kämpfenden Zivilisten und einem Kombattanten privilegieren.[81] Eine endlose Ausdehnung dieses Zeitraums ist weiterhin nicht gegeben, da die Aktivität und Wirkung der Malware unter Beachtung der Erfordernisse der Kausalität und des *belligerent nexus*[82] betrachtet werden müssen und diese Voraussetzungen insofern begrenzend wirken. Derjenige, der unkontrollierbare und daher von der Dauer (theoretisch) unbegrenzte Mittel einsetzt, schafft dadurch eine Risikosphäre, zu der sich das Recht kongruent verhalten muss. Darüber hinaus muss im Zweifelsfall die direkte Beteiligung eines Zivilisten abgelehnt werden.[83]

72 Henckaerts/ Doswald-Beck (Anm. 64), Part I, Chapter 4, Rule 14, S. 46ff; Art. 51 Abs. 5 lit. b, 57 Abs. 2 lit. a iii ZP I.
73 Henckaerts/ Doswald-Beck (Anm. 64), Part I, Chapter 20, Rule 70, S. 237ff.; Vgl. Art. 35 Abs. 2 ZP I; Art. 23 lit. e Abkommen, betreffend die Gesetze und Gebräuche des Landkriegs vom 18. Oktober 1907, RGBl. 1910, S. 107.
74 Henckaerts/ Doswald-Beck (Anm. 64), Part I, Chapter 5, Rule 15ff, S. 51ff.; Art. 57 Abs. 1 und Abs. 2 ZP I.
75 Art. 4 A (1), (2), (3) und (6) GC III; Vergleiche dazu Tallinn Manual (Anm. 2), S. 96f.
76 Watts, Combatant Status and Computer Network Attack, Virginia Journal of International Law 50 (2010), S. 392 (447).
77 Siehe oben: Voraussetzungen einer OAG, 7.1. Anwendbarkeit von Humanitärem Völkerrecht; Tallinn Manual (Anm. 2), S. 98f.
78 Tallinn Manual (Anm.2), S. 96; Watts (Anm. 71), S. 420ff.
79 Art. 51 (3) ZP I; Art. 13 (3) ZP II ; Zu Voraussetzungen der direkten Teilnahme: Tallinn Manual (Anm. 2), S. 119.
80 Vergleiche dazu Singer, Humanitär Völkerrechtliche Implikationen der Drohnenkriegführung, Sonderprobleme, Targeted Killing, Problemkreis 2: Rechtmäßige Ziele, Tagungsband zum 38. Österreichischen Völkerrechtstag, im Erscheinen 2014.
81 Andeutungen hierfür finden sich im Tallinn Manual, vgl. S. 114, 119.
82 Zur Vss.: Tallinn Manual (Anm. 2), S. 119.
83 Tallinn Manual (Anm. 2), S. 122, Analogiebildung und Verweis auf: Regel 33, S. 114.

8. Abschließende Zusammenfassung

Zusammenfassend ist festzustellen, dass die Entwicklung und Herausbildung von Staatenpraxis für die künftige Anwendung und Auslegung des Völkerrechts auf *Cyberwarfare* entscheidend ist. Die vorgestellte Cyberstrategie Deutschlands spiegelt in den allermeisten Fragen das geltende Recht wider. Für die USA gilt dies allerdings nur mit Abstrichen, da diese mitunter eine progressive Auffassung vertreten, insbesondere was das Selbstverteidigungsrecht betrifft.[84] In der Zukunft sollte weiter die Erarbeitung einer internationalen Strategie im Rahmen von internationalen Organisationen, Staatenverbänden und Militärbündnissen angestrebt werden, um eine weitest mögliche Rechtssicherheit und Rechtsgeltung zu erreichen. Die technologische Entwicklung von Cybermitteln und damit auch *Cyberwarfare* wird sich nicht aufhalten lassen, weswegen eine bestmöglichste Vorbereitung, die Absteckung von Grenzen und die Festlegung eines einheitlichen rechtlichen Rahmens von höchster Bedeutung sind.

84 Schmitt (Anm. 14), S. 23; Tallinn Manual (Anm. 2), S. 54, S. 58ff.

Internationale Kooperationsrichtlinien – ein Ausweg aus dem Attributionsdilemma

Thomas Reinhold*

Abstract: The attribution is a key element for international legitimacy of national self defence against cyber attacks. In many debates, the anonymity of the internet is pointed out as a main advantage for attackers, as it successfully prevents detection and sanctioning. A more technical perspective on the infrastructures and processes of data transmission reveals possibilities for identifying attackers that may prove sufficient for attribution. The article discusses when this might be the case and argues that the internet is not a place of anonymity at all. Deficient national and international norms are identified as the main obstacles for cyber attack attribution. These findings are considered in the light of individual rights, privacy and data protection. The objective of this article is the demystification of the internet as an anonymous space for further debates and to point out the importance of the development of rules and regulations for international cooperation to a special degree.

Keywords: Cyberwarfare, international cooperation, anonymity, identification, cyber attacks, IT
Cyberkriege, internationale Zusammenarbeit, Anonymität, Identifikation, Cyberattacken, IT

1. Cyberattacken und deren Verortung

Seit 2010 der Computerwurm Stuxnet durch einen Sabotageangriff gegen das iranische Atomprogramm bekannt wurde, berichten Medien regelmäßig von größeren Hacker-Attacken, dem Diebstahl immenser Datenmengen oder Vorfällen von Computerspionage. Neben der normalen Kriminalität im Internet sorgen dabei die Angriffe staatlicher Akteure wie die langjährigen Zugriffe chinesischer Hacker auf Computersysteme der US-amerikanischen Militärindustrie (Madiant 2013) oder die Enthüllungen über US-amerikanische Hackergruppen, die weltweit Daten aus Computersystemen stehlen (Business Week 2013), zunehmend auch in den internationalen politischen Beziehungen für Beunruhigung. Dem gegenüber steht die oft widerspruchslos akzeptierte These vom Internet als einem rechtsfreien Raum mit unbekannten und anonymen Angreifern, die ihre Aktivitäten beliebig tarnen und verbergen können und sich auf diese Weise einer effektiven Strafverfolgung und der Durchsetzung internationaler Rechtsnormen entziehen. Zentrales Argument dieser Sichtweise ist die postulierte faktische Unmöglichkeit der Attribution, also die Zuordnung und Verortung der Herkunft einer Cyberattacke und die Identifikation der menschlichen Angreifer. Im Gegensatz zu diesen Annahmen bieten die technischen Grundlagen des Internets und die paketbasierte Übertragung von Informationen zwischen Computern über bestehende Netzwerke eine sehr gute Grundlage für die Identifikation von Cyberattacken. Des Weiteren stellt sich im Falle von Cyberattacken staatlicher Akteure die Frage, welcher Grad an Attribution hinreichend ist und ob für eine angemessene Reaktion eines Staates die exakte Kenntnis der Identität des menschlichen Akteurs notwendig ist. Anhand dieser Fragestellungen kann deutlich gezeigt werden, dass die aktuellen Probleme der Attribution nicht auf der vermeintlichen Anonymität des Internets beruhen. Das entscheidende Problem bei der Rückverfolgung von Angriffen sind vielmehr fehlende internationale, mit demokratischen Werten zu vereinbarende Maßnahmen zur Speicherung von Daten über Internetverbindungen, mangelnde verbindliche Regularien zu Kommunikations- und Datenaustauschkanälen sowie den Speicherfristen dieser Informationen. Unter diesen Gesichtspunkten ist die zentrale Frage des Artikels, welche Bedingungen für eine erfolgreiche Attribution von staatlichen Cyberattacken notwendig sind, welche technischen Grundlagen dafür benötigt werden und welche Anforderungen sich daraus

* Thomas Reinhold ist Diplom Informatiker (TU) und Fellow am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH); Email: reinhold@ifsh.de.
Dieser Artikel wurde einem anonymen Begutachtungsverfahren (double-blind peer reviewed) unterzogen.