SVEN-HENDRIK SCHULZE

Cyber-„War“ – Testfall der Staatenverantwortlichkeit

Jus Internationale et Europaeum
107

Mohr Siebeck

Jus Internationale et Europaeum

herausgegeben von
Thilo Marauhn und Christian Walter

107

Sven-Hendrik Schulze

Cyber-„War“ – Testfall der Staatenverantwortlichkeit

Mohr Siebeck

Sven-Hendrik Schulze, geboren 1987; Studium der Rechtswissenschaften in Trier; wissenschaftlicher Mitarbeiter an der Universität Trier; 2014 Promotion; seit 2014 Rechtsreferendar am Oberlandesgericht Koblenz.

e-ISBN PDF 978-3-16-153846-9
ISBN 978-3-16-153845-2
ISSN 1861-1893 (Jus Internationale et Europaeum)

Die Deutsche Nationalibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von epline in Kirchheim/Teck gesetzt und von Gulde-Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2014 vom Fachbereich Rechtswissenschaft der Universität Trier als Dissertation angenommen. Zum Zwecke der Publikation wurden Rechtsprechung und Literatur – soweit verfügbar – bis einschließlich Dezember 2014 einbezogen. Spätere Entwicklungen konnten keine Berücksichtigung mehr finden.

Großer Dank gilt an erster Stelle meinem Doktorvater, Herrn Prof. Dr. Meinhard Schröder, der nicht nur meine Dissertation stets mit großem Interesse und durch konstruktive Gespräche begleitet hat, sondern mich darüber hinaus seit den Anfängen meines Studiums vorbildlich unterstützt und gefördert hat. Die lehrreiche und persönlich prägende Zeit an seinem Lehrstuhl sowie am Institut für Umwelt- und Technikrecht der Universität Trier werde ich immer in bester Erinnerung behalten. Herzlich bedanken möchte ich mich des Weiteren bei Herrn Prof. Dr. Alexander Proelß, der für die rasche Erstellung des Zweitgutachtens verantwortlich zeichnet und mich nach der Emeritierung meines Doktorvaters sowohl fachlich als auch finanziell stets hervorragend unterstützt hat.

Den Herren Prof. Dres. Christian Walter und Thilo Marauhn bin ich dankbar für die Aufnahme meiner Arbeit in die von ihnen herausgegebene Schriftenreihe und ihre wertvollen Anregungen im Vorfeld der Veröffentlichung.

Dem Auswärtigen Amt danke ich für die Gewährung eines großzügigen Druckkostenzuschusses.

Mein besonderer Dank gilt außerdem Herrn Martin Weiler, der bereits während der Erstellung des Manuskripts jederzeit bei Fragen zur Verfügung stand und später bei dessen Durchsicht nützliche Hilfestellungen leistete. Herrn Norbert Golumbeck gebührt großer Dank für seine unermüdliche Korrektur des Manuskripts. Auch bei meinen „Trierer“ Freunden möchte ich mich herzlich für ihre Unterstützung, gleich welcher Art, bedanken.

Vor allem aber danke ich meiner Steffi, die mir während der nicht immer leichten Zeit der Dissertation unentwegt mit ihrem Rat, ihrem Verständnis und ihrer Liebe zur Seite stand. Ohne sie und ihre wunderbare Familie wäre mir diese Leistung nicht möglich gewesen.

Schließlich schulde ich meinen Eltern, insbesondere meinem Vater, Thomas Schulze, der mir ebenfalls bei den Korrekturarbeiten behilflich war, von Herzen Dank für ihre stete und vielfältige Unterstützung sowohl während des Studiums als auch der Promotion; ihnen ist diese Arbeit gewidmet.

Trier, im August 2015 *Sven-Hendrik Schulze*

Inhaltsübersicht

Inhaltsverzeichnis

2. Kapitel

Erfolgreiche Rückverfolgung: Identifizierung der Angreifer – Glücks- oder Testfall der Staatenverantwortlichkeit?

3. Kapitel

Misslungene Rückverfolgung: Der Umstand des Nicht-Wissens als Herausforderung für Technik und Recht

Abkürzungsverzeichnis

ABl.	Amtsblatt
Add.	Addendum
AFDI	Annuaire Français de Droit International
A. F. L. Rev.	Air Force Law Review
AJIL	American Journal of International Law
Alb. L. J. Sci & Tech.	Albany Law Journal of Science and Technology
ASEAN	Association of Southeast Asian Nations
Austl. Int'l L. J.	Australian International Law Journal
AVR	Archiv des Völkerrechts
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
B. C. Int'l & Comp. L. Rev.	Boston College International and Comparative Law Review
Begr.	Begründer
Berk. J. Int. Law	Berkeley Journal of International Law
Berkeley Tech. L. J.	Berkeley Technology Law Journal
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
Brook. J. Int'l L.	Brooklyn Journal of International Law
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BYIL	British Yearbook of International Law
Cal. L. Rev.	California Law Review
Cardozo J. Int'l & Comp. L.	Cardozo Journal of International and Comparative Law
CERT	Computer Emergency Response Team
Chi. J. Int'l L.	Chicago Journal of International Law
Colum. J. Transnat'l L.	Columbia Journal of Transnational Law
CR	Computer und Recht
c't	Magazin für Computertechnik
DDoS	Distributed Denial of Service
Denv. J. Int'l L. & Pol'y	Denver Journal of International Law and Policy
DoS	Denial of Service
DuD	Datenschutz und Datensicherheit
ECtHR	European Court of Human Rights
EG	Europäische Gemeinschaft/en
EGMR	Europäischer Gerichtshof für Menschenrechte
EJIL	European Journal of International Law
EMRK	Europäische Menschenrechtskonvention
ENISA	European Network and Information Security Agency
EPIL	Encyclopedia of Public International Law
ESIL	European Society of International Law
ETS	European Treaty Series
EU	Europäische Union
FAZ	Frankfurter Allgemeine Zeitung

FIRST	Forum of Incident Response and Security Teams
GA	General Assembly
Geo. L. J.	Georgetown Law Journal
Georgetown J. Int. Law	Georgetown Journal of International Law
GG	Grundgesetz
GoJIL	Goettingen Journal of International Law
GYIL	German Yearbook of International Law
Harv. Int. Law J.	Harvard International Law Journal
Harv. J. L. & Pub. Pol'y	Harvard Journal of Law & Public Policy
Harv. Nat'l Sec'y J.	Harvard National Security Journal
HuV-I	Humanitäres Völkerrecht – Informationsschriften
IANA	Internet Assigned Numbers Authority
IAS	Information Assurance and Security
ICANN	Internet Corporation for Assigned Names and Numbers
ICJ	International Court of Justice
ICLQ	International & Comparative Law Quarterly
ICTY	International Criminal Tribunal for the former Yugoslavia
IGH	Internationaler Gerichtshof
ILC	International Law Commission
ILM	International Legal Materials
Ind. J. Global Legal Stud.	Indiana Journal of Global Legal Studies
Int'l L. Stud.	International Law Studies
Int. Rel.	International Relations
IP	Internet Protocol
IPbpR	Internationaler Pakt über bürgerliche und politische Rechte
IPv	Internet Protocol Version
IRRC	International Review of the Red Cross
ISGH	Internationaler Seegerichtshof
ISIS	Institute for Science and International Security
ISS Source	Industrial Safety and Security Source
IStGH	Internationaler Strafgerichtshof
ITLOS	International Tribunal for the Law of the Sea
JC & SL	Journal of Conflict and Security Law
JILT	Journal of Information, Law & Technology
JIR	Jahrbuch für Internationales Recht
JMSS	Journal of Military and Strategic Studies
J. Nat'l Sec. L. & Pol'y	Journal of National Security Law and Policy
JURA	Juristische Ausbildung
JZ	JuristenZeitung
KOM	Europäische Kommission
LCLR	Lewis & Clark Law Review
LJIL	Leiden Journal of International Law
Max Planck UNYB	Max Planck Yearbook of United Nations Law
MMR	MultiMedia und Recht
MPEPIL	Max Planck Encyclopedia of Public International Law
NATO	North Atlantic Treaty Organization
NILR	Netherlands International Law Review
NJ	Neue Justiz
NJW	Neue Juristische Wochenschrift
No.	Numero
NYIL	Netherlands Yearbook of International Law
N. Y. U. J. Int'l L. & Pol.	New York University Journal of International Law and Politics

NZWehrr	Neue Zeitschrift für Wehrrecht
OAS	Organisation Amerikanischer Staaten
OECD	Organisation for Economic Co-operation and Development
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
o. V.	ohne Verfasser
RdC	Recueil des Cours de l'Académie de Droit International
RECIEL	Review of European, Comparative & International Environmental Law
Res.	Resolution
RGDIP	Revue Générale de Droit International Public
RIAA	Reports of International Arbitral Awards
RUSI	Royal United Services Institute
SC	Security Council
SCADA	Supervisory Control and Data Acquisition
S. Cl. Comp. & High Tech. L. J.	Santa Clara Computer & High Technology Law Journal
SCO	Shanghai Cooperation Organisation
SPON	Spiegel Online
Stan. J. Int'l L.	Stanford Journal of International Law
Stan. L. Rev.	Stanford Law Review
StIGH	Ständiger Internationaler Gerichtshof
SZ	Süddeutsche Zeitung
TCP	Transmission Control Protocol
Tex. Int'l L. J.	Texas International Law Journal
Tex. L. Rev.	Texas Law Review
u. a.	und andere/unter anderem
UC Davis J. Int'l L. & Pol'y	UC Davis Journal of International Law and Policy
U. Ill. J. L., Tech. & Pol'y	University of Illinois Journal of Law, Technology & Policy
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
UNTS	United Nations Treaty Series
v.	vom/versus
VJTL	Vanderbilt Journal of Transnational Law
WTO	World Trade Organization
WVRK	Wiener Vertragsrechtskonvention
Yale J. Int'l L.	Yale Journal of International Law
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZöR	Zeitschrift für öffentliches Recht
ZP I	Zusatzprotokoll I zu den Genfer Abkommen v. 12. 08. 1949

Einführung und Gang der Untersuchung

„[…] cyberspace is real. And so are the risks that come with it."[1]

Estland 2007,[2] Georgien 2008,[3] die USA und Südkorea 2009,[4] der Iran 2010:[5] All diese Staaten sahen sich teils massiven Cyber-Angriffen auf unterschiedlichste staatliche und/oder private Ziele ausgesetzt. All diesen Fällen ist gemeinsam, dass im Nachgang weder die Frage des *wer* noch des *woher* zweifelsfrei geklärt werden konnte. Klar ist hingegen: Cyber-„War"[6] existiert und die Staatengemeinschaft muss dringend auf dieses bis dato unbekannte und mitunter emp-

---

[1] US-Präsident *Obama* anlässlich seiner Rede über die Sicherung der nationalen Cyber-Infrastruktur v. 29. 05. 2009, abrufbar unter: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (diese sowie alle im weiteren Verlauf der Untersuchung zitierten Internet-Fundstellen wurden zuletzt am 17. 12. 2014 abgerufen).

[2] *Tikk/Kaska/Vihul,* International Cyber Incidents: Legal Considerations, S. 14 ff.; *Davis,* Hackers Take Down the Most Wired Country in Europe, Wired Magazine v. 21. 08. 2007, abrufbar unter: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[3] *Tikk u. a.,* Cyber Attacks Against Georgia: Legal Lessons Identified, S. 1 ff.; *Tikk/Kaska/Vihul* (Fn. 2), S. 67 ff.; *Swaine,* Georgia: Russia ‚conducting cyber war', The Telegraph v. 11. 08. 2008, abrufbar unter: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

[4] *Clarke/Knake,* World Wide War: Angriff aus dem Internet, S. 43 f.; *Sang-Hun/Markoff,* Cyberattacks Jam Government and Commercial Websites in U. S. and South Korea, New York Times v. 08. 07. 2009, abrufbar unter: http://www.nytimes.com/2009/07/09/technology/09cyber.html?_r=0.

[5] *Sanger,* Confront and Conceal, S. 188 ff.; *ders.,* Obama Order Sped Up Wave of Cyberattacks Against Iran, New York Times v. 01. 06. 2012, abrufbar unter: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&smid=tw-nytimes&seid=auto; *Nakashima/Miller/Tate,* U. S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, Washington Post v. 19. 06. 2012, abrufbar unter: http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

[6] Cyber-„War" im hiesigen Sinne ist untechnisch zu verstehen, d. h. als plakatives, gewisse, nicht notwendig einen bewaffneten Konflikt voraussetzende Aktivitäten im virtuellen Raum (Cyberspace) umschreibendes Schlagwort, ähnlich *Libicki,* Pulling Punches in Cyberspace, in: Committee on Deterring Cyberattacks, National Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U. S. Policy, S. 123 ff. (123); den Begriff wohl erstmals verwendend *Arquilla/Ronfeldt,* Comparative Strategy 12 (1993), S. 141 ff.; siehe aus neuerer Zeit nur *Gaycken,* Die vielen Plagen

findliche Auswirkungen zeitigende Phänomen reagieren. Neben Maßnahmen auf politischer und technischer Ebene ist hierbei auch und gerade die Perspektive des Rechts, angesichts des typischerweise grenzüberschreitenden Auftretens der Angriffe vor allem des Völkerrechts, zu Rate zu ziehen. Die Relevanz des Völkerrechts beschränkt sich nicht nur auf das Aufzeigen etwaiger rechtlicher Handhabungsmöglichkeiten, sondern kommt ebenfalls in anderen nicht minder entscheidenden Zusammenhängen zum Tragen. Denn einerseits lassen sich nur auf Grundlage des (Völker-)Rechts verlässliche Aussagen darüber treffen, ob potenzielle technische Ansätze überhaupt gestattet sind, und andererseits vermag das (Völker-)Recht die gegebenenfalls erfolgende Implementierung derartiger Ansätze durch korrespondierende Pflichten zu unterstützen.

Haupt*ursache* des vermehrten Aufkommens von Cyber-Angriffen ist die hohe Abhängigkeit der Staaten und ihrer Gesellschaften von Informations- und Kommunikationstechnologien. Computer sind inzwischen omnipräsenter Bestandteil des täglichen Lebens. Nahezu alle strategisch, wirtschaftlich und gesellschaftlich relevanten Vorgänge werden auf informationstechnischem Wege, insbesondere über das Internet, bewerkstelligt.[7] So nutzten in Deutschland nach Angaben des Statistischen Bundesamts[8] im ersten Quartal 2014 80 % der über 10-Jährigen das Internet. Mit jeweils 97 % bzw. 98 % dominierten die Altersgruppen der 10–15- und 25–44-Jährigen; die Altersgruppe der 16–24-Jährigen erreichte gar eine Quote von 99 %. Einzig ältere, d. h. über 65 Jahre alte Personen fielen mit nur 40 % deutlich ab. Die Nutzungshäufigkeit des Internets war ebenfalls hoch, waren mit 82 % doch über drei Viertel der Deutschen jeden bzw. fast jeden Tag im Internet aktiv. Die Informationsgesellschaftsstatistiken des Statistischen Amts der EU (Eurostat)[9] von August 2012 belegen, dass die Abhängigkeit von Informations- und Kommunikationstechnologien, speziell vom Internet, im europäischen Umland ähnlich hoch, in einzelnen Staaten gar noch höher ist. Potenziert werden die Auswirkungen dieser Abhängigkeit durch die stetig zunehmende Vernetzung einzelner Systeme und Netzwerke hin zu einem

---

des Cyberwar, in: Schmidt-Radefeldt/Meissler (Hrsg.), Automatisierung und Digitalisierung des Krieges, S. 89 ff.

[7] Näheres bei *Stelter,* Gewaltanwendung unter und neben der UN-Charta, S. 26; *Schmitt,* Colum. J. of Transnat'l L. 37 (1999), S. 885 ff. (886 f.); *Joyner/Lotrionte,* EJIL 12 (2001), S. 825 ff. (826); *Hollis,* LCLR 11 (2007), S. 1023 ff. (1030); *Gaycken* (Fn. 6), S. 89 ff. (92); *Clarke/Knake* (Fn. 4), S. 136; sehr instruktiv zur Bedeutung des Internets für moderne Gesellschaften *Woltag,* Cyber Warfare. Military Cross-Border Computer Network Operations under International Law, S. 13 ff.

[8] Siehe *o. V.,* 80 % der Personen ab zehn Jahren nutzten im ersten Quartal 2014 das Internet, DESTATIS, abrufbar unter: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/ITNutzung/Aktuell_ITNutzung.html.

[9] Die Statistiken einschließlich eines sie detailliert vorstellenden Artikels sind abrufbar unter: http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics.

globalen Verbund.[10] Auch in diesem Kontext spielt das Internet als mittlerweile unverzichtbares Medium für zwischenmenschliche Kommunikation, sei es über E-Mail, Twitter, Facebook oder anderweitige Plattformen, sowie sonstige alltägliche Vorgänge, wie bspw. Online-Banking oder -Shopping, eine wesentliche Rolle. Gefahr dieser enormen Abhängigkeit und Vernetzung ist eine starke Verwundbarkeit: Moderne Staaten und ihre Gesellschaften sind ohne funktionsfähige Informations- und Kommunikationstechnik erheblich geschwächt.[11] Diese Schwäche ist für Militärs und andere Akteure der entscheidende Beweggrund zu teils folgenschweren Cyber-Angriffen. Vor diesem Hintergrund erklärt sich, dass diverse Staaten bereits mit dem Aufbau eigener Cyber-Kommandos begonnen oder diese Bemühungen gar bereits abgeschlossen haben. Zuletzt wurde etwa bekannt, dass sowohl die USA[12] als auch das Vereinigte Königreich[13] ihre Fähigkeiten auf dem Cyber-„Schlachtfeld" beträchtlich auszuweiten gedenken.

Haupt*problem* von Cyber-Angriffen ist, dass – dies haben die bisherigen Zwischenfälle eindrucksvoll gelehrt – im Regelfall eine Identifizierung ihrer Urheber und Ursprungsorte misslingt, ergo eine Rückverfolgungsproblematik besteht, und die Frage nach der (staatlichen) Verantwortlichkeit für derartige Angriffe aufgrund des Fehlens irgendwie gearteter Anknüpfungspunkte folglich oftmals unbeantwortet bleibt. Die Gründe hierfür sind vielfältig und differieren je nach Angriffsmedium. Im Rahmen von Internetangriffen kommt vor allem der missbrauchsanfälligen Architektur und Funktionsweise des Internets übergeordnete Bedeutung zu. Die Rückverfolgung sonstiger, etwa über präparierte USB-Sticks oder Innentäter ausgeführter Angriffe ist nochmals um ein Vielfaches schwerer, da regelmäßig und speziell seit der zunehmenden Einbeziehung staatlicher Nachrichtendienste keine Rückschlüsse zulassenden Spuren hinterlassen werden. In diesen Fällen ist eine etwaige Identifizierung

---

[10] *Drechsler/Lünstedt/Lacroix,* Vierteljahresschrift für Sicherheit und Frieden 18 (2000), S. 130 ff. (132).

[11] *Joyner/Lotriont*e, EJIL 12 (2001), S. 825 ff. (830); *Ziolkowski,* HuV-I 21 (2008), S. 202 ff. (204); *Schmitt,* Colum. J. of Transnat'l L. 37 (1999), S. 885 ff. (887), nach welchem mitunter das Überleben davon abhängt; *Clarke/Knake* (Fn. 4), S. 136 sprechen gar von Unverzichtbarkeit.

[12] So soll die schon seit 2010 operierende amerikanische Einheit USCYBERCOM, http://www.stratcom.mil/factsheets/Cyber_Command/, von ca. 900 auf etwa 4900 Mitarbeiter aufgestockt werden, siehe *Nakashima,* Pentagon to boost cybersecurity force, Washington Post v. 27. 01. 2013, abrufbar unter: http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity.

[13] Neben den Joint Cyber Units in Corsham und Cheltenham soll nun noch eine diese unterstützende Joint Cyber Reserve hinzutreten, die mit einem Budget von ca. 600 Millionen Euro ausgestattet sein und sich aus ausscheidenden Soldaten, aktuellen und ehemaligen Reservisten sowie mit entsprechendem Know-How versehenen Zivilisten zusammensetzen wird, siehe nur *o. V.,* New cyber reserve unit created, GOV.UK v. 29. 09. 2013, abrufbar unter: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit; *o. V.,* Neue Einheit: Briten gründen riesige Cyber-Armee, SPON v. 29. 09. 2013, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/grossbritannien-gruendet-cyber-armee-a-925166.html.

oft von bloßen Zufälligkeiten abhängig. Mit Blick auf die möglichen Folgen, welche nicht rückverfolgbare (staatliche) Cyber-Angriffe für die Stabilität der zwischenstaatlichen Beziehungen und damit letztlich für die internationale Sicherheit als solche zu bewirken im Stande sind, gilt es, zeitnah Lösungen für die Rückverfolgungsprobleme zu finden oder aber gangbare Alternativen darzulegen. Unterstrichen wird diese Notwendigkeit durch den Umstand, dass Angreifer ansonsten mangels zu befürchtender Konsequenzen jegliche Hemmungen ablegen und voraussichtlich noch gefährlicher zu Werke gehen werden.

Die vorliegende Arbeit widmet sich der angesichts der geschilderten Probleme nur schwerlich zu beantwortenden Frage nach der staatlichen Verantwortlichkeit für Angriffe im Cyber-„War". Bis dato hat diese Fragestellung, obgleich äußerst problembehaftet, im völkerrechtlichen Schrifttum eine weitgehend stiefmütterliche Behandlung erfahren. Umfassende Untersuchungen, die sämtliche im Zusammenhang von Cyber-Angriffen relevant werdenden Gesichtspunkte der Staatenverantwortlichkeit einbeziehen, existieren nicht. Das Gros der Abhandlungen zum Problemfeld des Cyber-„War", auch monographischer Art – zu nennen sind hier insbesondere die deutschsprachige Dissertation von *Dittmar*[14] sowie die englischsprachige Darstellung von *Roscini*[15] –, richtet den Fokus auf andere Aspekte des Völkerrechts, zuvörderst das allgemeine Gewaltverbot, das Recht auf Selbstverteidigung oder das humanitäre Völkerrecht. Das Thema Staatenverantwortlichkeit wird zumeist, wenn überhaupt, nur am Rande erörtert. Die hiesige Untersuchung soll daher, anknüpfend an vereinzelte Publikationen in der Aufsatzliteratur[16] und erste zaghafte Ansätze in der Monographie von *Woltag*[17], einen Beitrag zur (weiteren) Erforschung dieser problembehafteten, noch wenig untersuchten Thematik liefern. Angezeigt ist hierbei, einen zweischrittigen hypothesenartigen Ansatz zugrunde zu legen, der einerseits die ungeachtet aller Rückverfolgungsprobleme keinesfalls auszuschließende potenzielle Möglichkeit einer erfolgreichen Rückverfolgung nicht unberücksichtigt lässt und andererseits den Regelfall einer misslingenden Rückverfolgung abdeckt, ergo eine (all-)umfassende Behandlung des Themen-

[14] Angriffe auf Computernetzwerke – *Ius ad bellum* und *ius in bello.*

[15] Cyber Operations and the Use of Force in International Law, der Identifizierungs- und Zurechnungsproblemen jedoch immerhin knapp acht Seiten (S. 33 ff.) widmet.

[16] Siehe etwa *Shackelford,* Berk. J. Int. Law 27 (2008), S. 191 ff.; *ders./Andres,* Georgetown J. Int. Law 42 (2011), S. 971 ff.; *Sklerov,* Military Law Review 201 (2009), S. 1 ff.; *Roscini,* Max Planck UNYB 14 (2010), S. 85 ff.; *Ryan u. a.,* Georgetown J. Int. Law 42 (2011), S. 1161 ff.; *Hollis,* Harv. Int. Law J. 52 (2011), S. 374 ff.; *Heintschel v. Heinegg,* Cyberspace – Ein völkerrechtliches Niemandsland?, in: Schmidt-Radefeldt/Meissler (Fn. 6), S. 159 ff.; *Krieger,* AVR 50 (2012), S. 1 ff.

[17] Der bedingt durch den weit gefassten Untersuchungsgegenstand seiner Arbeit, die neben Aspekten der Staatenverantwortlichkeit [siehe *ders.* (Fn. 7), S. 85 ff.] viele weitere Bereiche des Völkerrechts behandelt, genannt seien nur das Gewalt- und Interventionsverbot, das Recht auf Selbstverteidigung und vor allem das humanitäre Völkerrecht, freilich keine sonderlich tiefgehende Analyse der Thematik zu liefern vermag.

feldes ermöglicht. Ziel ist, die staatliche Verantwortlichkeit für Cyber-Angriffe auf diesem Wege anhand der völkerrechtlichen Regeln der Staatenverantwortlichkeit zu untersuchen und die Problematik einer brauchbaren Lösung zuzuführen respektive alternative Regelungsansätze aufzuzeigen, wenn und soweit dieses traditionelle Regelwerk an seine Grenzen stößt, sich also als partiell oder vollends unbrauchbar erweist.

Aus dem Vorstehenden ergibt sich eine dreigliedrige Konzipierung der Arbeit. In einem ersten, allgemeinen Teil wird zunächst die diffuse Terminologie um das Phänomen des Cyber-„War" näher beleuchtet und anhand dessen der Untersuchungsgegenstand – Angriffe auf Computernetzwerke – konkretisiert. Im Weiteren werden die Entstehungsgründe des so verstandenen Cyber-„War" sowie sein bisheriges Erscheinungsbild einschließlich der verschiedenen Angriffsformen beschrieben. Das eröffnende Kapitel schließt mit einer Analyse des Hauptproblems des Cyber-„War", der äußerst diffizilen Rückverfolgung von Angriffen, also dem Versuch der Identifizierung der Urheber und Ursprungsorte.

Das zweite Kapitel der Ausarbeitung befasst sich ausführlich mit der Möglichkeit einer erfolgreichen Rückverfolgung und untersucht, ob sich diese als Glücks- oder eher als Testfall der Staatenverantwortlichkeit erweist. Dabei werden eingangs die allgemeinen Grundsätze des Rechts der Staatenverantwortlichkeit erörtert, wobei die Darstellung nicht allumfassend, sondern auf grundlegende Fragen, insbesondere das Zurechnungsregime und die sich aus der Verantwortlichkeit ergebenden Rechtsfolgen, reduziert ist. Darauf aufbauend kann im zweiten Unterkapitel speziell der Problematik von Angriffen auf Computernetzwerke im Kontext der Staatenverantwortlichkeit nachgegangen werden. Im Fokus stehen hierbei zunächst potenzielle Pflichtenverstöße, bspw. gegen das Gewalt- oder das Interventionsverbot, verbunden mit einer völkerrechtlichen Einordnung der bisher bedeutsamsten, für internationales Aufsehen sorgenden Zwischenfälle in Estland 2007, Georgien 2008 und dem Iran 2010. Nach Herausarbeitung des Zurechnungsgegenstands werden die relevanten Zurechnungskonstellationen, insbesondere das Verhalten Privater, aufgezeigt und untersucht, um sich sodann dem zutage tretenden Zurechnungsdilemma bezüglich privater Angriffe auf Computernetzwerke zu widmen. Neben Lösungsansätzen nach geltendem Völkerrecht, etwa dem zurechnungsunabhängigen Abstellen auf ein eigenes staatliches Fehlverhalten im Kontext privater Angriffe auf Computernetzwerke, befasst sich die dahingehende Abhandlung auch mit möglichen Ansätzen *de lege ferenda,* bspw. einer Lockerung der bestehenden Zurechnungsmaßstäbe oder einer Umkehr der Beweislast zu Gunsten der Angriffsopfer. Des Weiteren werden die rechtlichen Folgen von Angriffen auf Computernetzwerke näher beleuchtet, u. a. der Möglichkeit einer zukünftigen Modifizierung des herkömmlichen Rechtsfolgenkonzepts in Fällen umgekehrter Beweislast nachgegangen. Das zweite Kapitel schließt mit theoretischen und

praktischen Überlegungen zur Realisierung der getätigten Vorschläge *de lege ferenda,* innerhalb derer vor allem die bisherige Staatenpraxis ausführlich dargestellt und entsprechend interpretiert wird.

Der dritte Teil der Arbeit behandelt eingehend die Folgen einer misslungenen Rückverfolgung, d. h. den Umgang mit der Situation des Nicht-Wissens. In diesem Zusammenhang wird eine sich anbietende Untergliederung in technische sowie rechtliche Ansätze vorgenommen. Im Rahmen der technischen Ansätze werden u. a. die gängigen Rückverfolgungstechniken, eine Überarbeitung des Internets oder aber eine verstärkte internationale Kooperation und Zusammenarbeit als Lösungsvorschläge diskutiert. In rechtlicher Hinsicht erfolgt ein durch den Umstand des Nicht-Wissens bedingter Perspektivenwechsel. Statt den Fokus auf die völkerrechtliche, einen wie auch immer gearteten – fehlenden – Anknüpfungspunkt voraussetzende Zuordnung der eigentlichen Angriffe zu richten, konzentrieren sich die Ausführungen auf den Schutz vor den mit diesen einhergehenden Auswirkungen bzw. Schädigungen. Zu diesem Zweck wird einerseits der Vorschlag zur Schaffung einer Beistandspflicht im Falle von durch Cyber-Angriffe ausgelösten Notlagen („e-SOS“) genauer beleuchtet und andererseits der Aspekt der Vorsorge erörtert, d. h. Maßnahmen besprochen, die besagte Auswirkungen bzw. Schädigungen bereits im Vorfeld durch geeignete rechtliche Schritte zu vermeiden oder zumindest abzumildern versuchen.

1. Kapitel

Das Phänomen Cyber-„War“

Eine fundierte und vor allem sinnvolle Analyse des Cyber-„War“ im Kontext der Staatenverantwortlichkeit lässt sich nicht zufriedenstellend bewerkstelligen, ohne das Phänomen als solches vorab einer näheren Betrachtung unterzogen zu haben. Wie einleitend bereits bemerkt, bedarf insbesondere der Klärung, was sich hinter dem Begriff des Cyber-„War“ verbirgt, d. h. was genau den Untersuchungsgegenstand der Arbeit bildet, ferner wie es zu dessen Entstehung kam und letztlich wie das Phänomen momentan in Erscheinung tritt. Auch die bei Begründung der staatlichen Verantwortlichkeit im Cyber-„War“ auftretenden Schwierigkeiten erschließen sich nicht oder nur unzureichend, wenn nicht zuvor die diesbezüglichen Ursachen, speziell die (technische) Problematik der Rückverfolgung, eingehend erörtert wurden. Das nun folgende erste Kapitel der Ausarbeitung widmet sich all diesen grundlegenden für die weitere Untersuchung äußerst bedeutsamen Fragen.

A. Terminologie und Konkretisierung des Untersuchungsgegenstands

Die Terminologie um das im Rahmen dieser Arbeit zu untersuchende Problemfeld des Cyber-„War“ ist keineswegs einheitlich. Abgesehen von dem hier verwendeten Begriff, der – dies gilt es zur Vermeidung etwaiger Missverständnisse nochmals zu betonen – lediglich als Schlagwort der öffentlichen, fachübergreifenden Diskussion, nicht aber im tatsächlichen Sinne als kriegerische Auseinandersetzungen voraussetzend verstanden wird,[1] existieren weitere der Umschreibung des Phänomens dienende Termini wie *Information Operations*[2]

[1] Zu dessen Verständnis bereits Einführung, Fn. 6.

[2] *Anderson/Dooley,* Information Operations in the Space Law Arena: Science Fiction Becomes Reality, in: Schmitt/O’Donnell (Hrsg.), Computer Network Attack and International Law, S. 265 ff.; *Hollis,* LCLR 11 (2007), S. 1023 ff.; *Kuehl,* Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age, in: Schmitt/O’Donnell (a. a. O.), S. 35 ff.; *T. Stein/Marauhn,* ZaÖRV 60 (2000), S. 1 ff. (1); *Theuerkauf,* Europäische Sicherheit 2 (2000), S. 14 ff.

(Informationsoperationen), *Information Warfare*[3] (Informationskriegsführung) oder *Cyber Warfare*[4] (Cyberkriegsführung). Zur Durchleuchtung dieses Begriffswirrwarrs und vor allem im Hinblick auf die Konkretisierung des Untersuchungsgegenstandes werden die jeweiligen Definitionen herangezogen und diskutiert. Vor dem Hintergrund, dass jene überwiegend in der in diesem Bereich federführenden US-amerikanischen Militärdoktrin wurzeln, die im Gros der themenbezogenen Abhandlungen entweder zugrunde gelegt wird oder sich nur geringfügig modifiziert in jeweils eigenen Definitionsansätzen wiederfindet, beschränkt sich die Darstellung weitgehend auf das Begriffsverständnis des US-Militärs.

I. Informationsoperationen

Das Verständnis des Begriffs der Informationsoperationen hat sich bereits des Öfteren gewandelt. Zunächst wurden solche Operationen von den primär für die Entwicklung der Militärdoktrin verantwortlich zeichnenden Vereinigten (General-)Stabchefs der US-Armee (Joint Chiefs of Staff)[5] definiert als:

„Actions taken to affect adversary information and information systems while defending one's own information and information systems.“

Unter Informationen waren „facts, data, or instructions in any medium or form“[6] zu verstehen. Als Informationssysteme wurden „the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information“[7] angesehen. Der Begriff der Informationsoperationen war demzufolge sehr weit gefasst. Ferner wurde zwischen offensiven und defensiven Informationsoperationen differenziert.[8]

---

[3] *G. Stein,* Airpower Journal 9 (1995), S. 30 ff.; *Libicki,* What is Information Warfare?, S. 1 ff.; *Greenberg/S. Goodman/Soo Hoo,* Information Warfare and International Law; *Heintschel v. Heinegg,* Informationskrieg und Völkerrecht – Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung, in: Epping/Fischer/ders. (Hrsg.), Brücken bauen und begehen, Festschrift für Knut Ipsen, S. 129 ff.; *Haslam,* JC & SL 5 (2000), S. 157 ff.; *Barkham,* N. Y. U. J. Int'l L. & Pol. 34 (2001), S. 57 ff.; *Joyner/Lotrionte,* EJIL 12 (2001), S. 825 ff.

[4] *Woltag,* Cyberwarfare (2010), in: Wolfrum (Hrsg.), MPEPIL online edition (im Folgenden: MPEPIL online edition); *Hoisington,* B. C. Int'l & Comp. L. Rev. 32 (2009), S. 439 ff.; *Döge,* AVR 48 (2010), S. 486 ff.; *Turns,* JC & SL 17 (2012), S. 279 ff.

[5] Joint Chiefs of Staff, Joint Doctrine for Information Operations (1998), Joint Publication 3–13, GL 7; Näheres zu diesen unter: http://www.jcs.mil.

[6] Joint Chiefs of Staff (Fn. 5), GL-7.

[7] Ebd.

[8] Joint Chiefs of Staff (Fn. 5), Chapter II und III; zu diesen Ausführungen und zur alten Definition im Allgemeinen *Dittmar,* Angriffe auf Computernetzwerke – *Ius ad bellum* und *ius in bello,* S. 35 f.

Mitte Februar 2006[9] gaben die Joint Chiefs of Staff diese Differenzierung[10] auf und modifizierten die obige Definition. Unter einer Informationsoperation war nunmehr Folgendes zu verstehen:

„The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[11]

Trotz der Tatsache, dass die Begrifflichkeiten Information und Informationssysteme nicht mehr aufgeführt waren, blieb deren Bedeutung für Informationsoperationen als Angriffsmittel bzw. -ziel unverändert.[12] Die im Rahmen des ersten Definitionsversuches noch schwammig umschriebenen „actions" wurden in der zweiten Definition spezifiziert und in mehrere Kategorien unterteilt.

Der aktuelle aus dem Jahre 2012 datierende dritte Definitionsansatz der Joint Chiefs of Staff knüpft eng daran an, verkürzt aber – wohl der Übersichtlichkeit wegen – den eigentlichen Definitionstext. Informationsoperationen sind danach:

„The integrated employment […] of information related-capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision-making of adversaries or potential adversaries while protecting our own."[13]

Abgesehen von der Wiedereinbeziehung des Begriffs der Information gehen mit dieser Aktualisierung auf den ersten Blick keine sich auswirkenden Änderungen einher, da die vormals noch zum Inhalt der Definition zählenden Arten von Informationsoperationen über einen ausdrücklichen Verweis mit dieser assoziiert sind.[14] Die Aspekte des *Electronic Warfare* (elektronische Kriegsführung), der *Psychological Operations* (psychologische Kriegsführung), der *Military Deception* (Täuschungsoperationen) sowie der *Operations Security* (Absicherung der eigenen Operationsführung) sind zwar, vor allem im Hinblick auf das humanitäre Völkerrecht, von völkerrechtlicher Relevanz, vermögen allerdings

[9] Siehe Joint Chiefs of Staff, Information Operations (2006), Joint Publication 3–13, Revision of Joint Publication 3–13 v. 1998 (Fn. 5).

[10] Nicht jedoch die Ansicht, dass Informationsoperationen sowohl offensive als auch defensive Zielrichtungen haben können, Joint Chiefs of Staff (Fn. 9), S. iii.

[11] Joint Chiefs of Staff (Fn. 9), GL-9.

[12] Siehe hinsichtlich der gleichlautenden Definition von „information" und des geringfügig geänderten Begriffs des „information system", ebd.; siehe auch U. S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1–02, Stand: 15. 11. 2014, welches die Begrifflichkeiten zwar nicht mehr separat definiert, aber an diversen Stellen darauf Bezug nimmt.

[13] Joint Chiefs of Staff, Information Operations (2012), Joint Publication 3–13, Revision of Joint Publication 3–13 v. 2006 (Fn. 9), GL-3; dies., Information Operations (2014), Joint Publication 3–13, Change 1 to Joint Publication 3–13 v. 2012 (ebd.), GL-3; U. S. Department of Defense (Fn. 12), S. 121.

[14] Siehe U. S. Department of Defense (Fn. 12), S. 121.

bei ihrer Durchführung keine neuartigen Schwierigkeiten zu zeitigen.[15] Zudem sind sie für die Regeln der Staatenverantwortlichkeit von allenfalls untergeordnetem Interesse, sodass in dieser Ausarbeitung von einer näheren Untersuchung abgesehen wird.

Weitaus bedeutender für den Untersuchungsgegenstand sind hingegen die in früherer Zeit noch in den Verweis einbezogenen, aber mit Wirkung vom 15. Dezember 2012 aus für den Verfasser nicht ersichtlichen Gründen entfernten *Computer Network Operations* (Computernetzwerkoperationen).[16] Neben der weniger relevanten *Computer Network Defense*[17] (Verteidigung von Computernetzwerken) und der – völkerrechtlich – weitgehend unproblematischen, nur einen Fall von grundsätzlich[18] nicht verbotener Spionage darstellenden[19]

---

[15] Diesbezüglich und hinsichtlich der einzelnen Definitionen *Heintschel v. Heinegg* (Fn. 3), S. 129 ff. (131 ff.); *Dittmar* (Fn. 8), S. 36 f.

[16] Zur Entfernung des Begriffs und seiner Untergliederungen siehe U. S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1–02, Stand: 15. 12. 2012, BL-3. Der Vorgang geht zurück auf Joint Chiefs of Staff (Fn. 13, 2012), GL-3. Noch zu finden ist er in Joint Chiefs of Staff (Fn. 9), GL-6 sowie U. S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1–02, Stand: 15. 11. 2012, S. 60.

[17] Definition: „Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.“ U. S. Department of Defense (Fn. 16), Stand: 15. 11. 2012, S. 60; ähnlich Joint Chiefs of Staff (Fn. 9), GL-5 f.

[18] *Kanuck,* Harv. Int. Law J. 37 (1996), S. 272 ff. (276) verweist auf etwaige Verstöße gegen das Interventionsverbot; ebenso *Gill,* Non-Intervention in the Cyber Context, in: Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace, S. 217 ff. (224 ff.); *Keber/Roguski,* AVR 49 (2011), S. 399 ff. (411); siehe auch *Woltag,* Cyber Warfare. Military Cross-Border Computer Network Operations under International Law, der die seitens staatlicher Organe in hoheitlicher Eigenschaft erfolgte Zugriffnahme auf nicht öffentlich zugängliche Daten in anderen Staaten mitunter als Verstoß gegen das Interventionsverbot, S. 119 ff., in jedem Fall aber als Verletzung der territorialen Integrität des betroffenen Staats begreift, S. 125 f.; demgegenüber nur eine mögliche Verletzung der Souveränität des Zielstaats annehmend *Roscini,* Cyber Operations and the Use of Force in International Law, S. 66.

[19] Eingehend *Ziolkowski,* Peacetime Cyber Espionage – New Tendencies in Public International Law, in: dies. (Fn. 18), S. 425 ff.; siehe ferner *Schaap,* A. F. L. Rev. 64 (2009), S. 121 ff. (139 f.); *Ryan u. a.,* Georgetown J. Int. Law 42 (2011), S. 1161 ff. (1178); *Heintschel v. Heinegg* (Fn. 3), S. 129 ff. (134); *T. Stein/Marauhn,* ZaöRV 60 (2000), S. 1 ff. (32 f., 36); *Woltag* (Fn. 18), S. 124; *ders.* (Fn. 4), Rn. 3; *ders.,* Computer Network Operations Below the Level of Armed Force, ESIL Conference Paper No. 1/2011, S. 14; *Roscini* (Fn. 18), S. 66; *Krieger,* AVR 50 (2012), S. 1 ff. (8, 15); allgemein zur Zulässigkeit von Spionageaktivitäten im Völkerrecht *Chesterman,* Secret Intelligence (2009), MPEPIL online edition, Rn. 23; *Schaller,* Spies (2009), MPEPIL online edition, Rn. 2. Auch der jüngst bekannt gewordene weitreichende, insbesondere die Bespitzelung der Privatsphäre von Bürgern sowie der Bundeskanzlerin einschließende National Security Agency (NSA)-Abhörskandal ist wohl (noch) als völkerrechtmäßige Spionage einzustufen, siehe dazu nur den Gastbeitrag von *Talmon,* NSA-Affäre: Abhören des Kanzler-Telefons völkerrechtlich nicht verboten, FAZ v. 31. 10. 2013, abrufbar unter: http://www.faz.net/aktuell/politik/staat-und-recht/nsa-affaere-abhoeren-des-kanzler-telefons-voelkerrechtlich-nicht-verboten-12642973.html; zur Zulässigkeit der damaligen Aktivitäten der NSA (2000) bereits *Heintschel v. Heinegg* (ebd.). Gleichwohl nahm die