Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)633
17.02.2016 - 18/2686
5410

Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsschuss der Deutschen Bundestages

Prof. em. Dr. Michael Bothe
J.W. Goethe-Universität, Frankfurt/Main

Die folgende Stellungnahme behandelt in einer systematischen Auswahl die Rechtsfragen, die vom Verteidigungsausschuss zur Vorbereitung der Anhörung am 22.2.2016 gestellt wurden.

Zusammenfassung

Die Nutzung von Computernetzwerken zur Schädigung fremder Staaten (Cyber-Angriff) besitzt ein hohes Schadenspotenzial, das eine Klärung seiner rechtlicher Schranken erfordert. Dieses neue Phänomen ist keineswegs ein rechtliches Niemandsland. Vielmehr kann bestehendes Recht sinnvoll darauf angewandt werden.

Völkerrechtlich ist auch auf Cyber-Angriffe die Grundregel anzuwenden, die Staaten verbietet, andere Staaten zu schädigen, und die Staaten gebietet, mit der gebotenen Sorgfalt (due diligence) zu verhindern, dass von ihrem Territorium Schaden auf dem Gebiet anderer Staaten verursacht wird (no harm rule). Cyber-Angriffe sind sie als Verletzungen des völkerrechtlichen Gewaltverbots oder auch als bewaffnete Angriffe im Sinne des Art. 51 UN Charter zu qualifizieren, wenn sie hinsichtlich Umfang und Wirkung („scale and effects“) dem Einsatz von Waffengewalt vergleichbar sind. Es kommt für die Vergleichbarkeit wesentlich auf den Umfang der durch einen Cyberangriff verursachten physischen Schäden an. Ein solcherart als „bewaffneter“ Angriff zu qualifizierender Cyberangriff berechtigt zu Selbstverteidigung, d.h. zum militärischen Gegenschlag, und führt zur Anwendbarkeit von Art. 5 des NATO-Vertrages.
Bei der Frage, wann ein Cyber-Angriff solcherart bewaffneter Gewalt gleich zu achten ist, bestehen Interpretationsspielräume, die ein hohes Missbrauchspotenzial im Sinne einer falschen Rechtfertigung militärischer Gegengewalt in sich bergen. Selbstverteidigung ist nur gegen den Staat zulässig, der die Erstgewalt ausgeübt hat, d.h. dem ein erster Cyber-Angriff nachweisbar zuzurechnen ist. Selbstverteidigung auf Verdacht ist unzulässig. Diese Regel ist zu beachten, obwohl gerade bei Cyber-Angriffen der Nachweis des Urhebers schwierig ist. Von der Selbstverteidigung, die einen bewaffneten Angriff im Rechtssinne voraussetzt, sind reine Schutz- und Abwehrmaßnahmen (nicht immer einfach) zu unterscheiden, die ein Staat stets treffen darf.

Wenn ein bewaffneter Konflikt wie auch immer einmal entstanden ist, gilt auch für Cyber-Angriffe das allgemein für die Zulässigkeit von Schädigungshandlungen anwendbare Recht bewaffneter Konflikte (humanitäres Völkerrecht, ius in bello). Insbesondere ist das Unterscheidungsgebot zu beachten: Angriffe dürfen nur auf militärische Ziele, nicht auf zivile Objekte oder Zivilpersonen gerichtet werden. Der zivile Begleitschaden, der u.U. von

Angriffen auf zivile Objekte verursacht wird, darf nicht außer Verhältnis zu dem erwarteten militärischen Vorteil stehen. Die Anwendung dieser Regeln wirft Schwierigkeiten der Qualifizierung von Objekten und Abwägung zwischen zivilem Schaden und militärischem Vorteil nicht nur bei Cyber-Angriffen Schwierigkeiten auf.

Die Bundesrepublik ist nach Art. 26 GG verfassungsrechtlich verpflichtet, keine Cyber-Angriffe auszuführen oder sich an ihnen zu beteiligen, die den Tatbestand des Gewaltverbots erfüllen.
Werden Cyber-Angriffe von deutschen Streitkräften ausgeführt, so gilt das Erfordernis parlamentarischer Zustimmung. Diesem Erfordernis unterfallen nach dem Grundsatz der Vergleichbarkeit zumindest Maßnahmen, deren (auch indirekte) physische Wirkung („scale and effects“) so erheblich ist, dass sie als militärische Gewaltmaßnahmen zu qualifizieren sind. Welche Cyber-Operationen darüber hinaus Einbezug in militärische Operationen zu qualifizieren sind, die das Zustimmungserfordernis auslösen, ist ohne eingehende Analyse möglicher Szenarien kaum zu entscheiden.
Zu erwägen ist auch, ob unter Anwendung der Grundsätze des Bundesverfassungsgerichts für Cyber-Operationen, deren Wirksamkeit von der vorherigen Geheimhaltung abhängt, das Zustimmungsverfahren im Sinne des Geheimschutzes modifiziert werden kann.
Die in der völker- und verfassungsrechtlichen Analyse dargestellten Unsicherheiten und Unklarheiten werden die Frage nach der lex ferenda, nach neuen völkervertraglichen Regelungen auf. Streitig dabei insbesondere die Tragweite möglicher staatlicher Kontrollpflichten. Darüber hinaus stehen allerdings die Chancen für völkerrechtliche Neuregelungen zu Schranken militärischer Gewalt im gegenwärtigen Klima der internationalen Beziehungen eher schlecht.

1. Die Problematik

Maßnahmen des Cyberwar oder Cyberangriffe sind eine neue Form der grenzüberschreitenden Schädigung: Störung oder Vernichtung der Funktionsfähigkeit von Computern oder Computernetzwerken in einem anderen Staat mit Hilfe von Computer-Netzwerken. Die so gestörten Computer oder Computer-Netzwerke steuern ihrerseits eine Vielzahl von Vorgängen in der physischen Welt, insbesondere kritische Infrastruktur. In dem Verlust der Steuerungsfähigkeit oder der Verfälschung der Steuerung besteht das hohe Schadenspotenzial von Cyberangriffen.[1] Dieses Schadenspotenzial macht es erforderlich, die Rechtsregeln, insbesondere die Völkerrechtsregeln zu klären, die für solche Angriffe gelten. Dies ist der Zweck der folgenden Ausführungen.

Die Ausführungen gehen davon aus, dass die Neuheit des Phänomens keineswegs erfordert, dass das bislang geltende Recht davor kapitulieren muss, oder dass es sich um ein „völkerrechtliches Niemandsland" handelt, wo alle auftretenden Fragen und Konflikte neu geregelt werden müssten.[2] Eine Antwort auf die Frage nach den rechtlichen Schranken dieser Schädigungsvorgänge muss vielmehr versuchen, bestehende Regeln auf dieses neue Phänomen anzuwenden, d.h. in diesem neuen Phänomen die Tatbestandsmerkmale der vorhandenen Regeln zu erkennen und herauszuarbeiten. Das ist der konsequent durchgeführte Ansatz des Tallinn Manual on the International Law Applicable to Cyber Warfare,[3] ein von einer internationalen Expertengruppe erarbeitetes Regelwerk mit ausführlichem Kommentar. Diese Gruppe war von der NATO eingeladen, es handelt sich aber nicht um ein offizielles NATO-Dokument. Die Gruppe besitzt natürlich keine Rechtssetzungskompetenz, aber das fachliche Ansehen der Mitglieder der Gruppe verleiht ihrer Meinung zur Rechtslage ein hohes Gewicht in einem sich fortsetzenden rechtlichen Diskurs.

Auch die von der UN-Generalversammlung eingesetzte Arbeitsgruppe über internationale Sicherheit im Bereich der Telematik setzt auf die Anwendbarkeit des geltenden Völkerrechts.[4] Im internationalen Diskurs gibt es allerdings auch Stimmen, die stärker die Notwendigkeit von Neuregelungen betonen. Sie fordern insbesondere mehr staatliche Kontrolle von IT-Aktivitäten, so etwa Russland und China.[5] Dem wird von anderer Seite mit einer Betonung des freien Informationsflusses widersprochen.

---

[1] GA Resolution 66/24. Vgl. die Berichte der von der UN-Generalversammlung eingesetzten Expertengruppe, UN Doc. A/65/201 und A/68/98; vgl. ferner Sandro Gaycken, 'Die vielen Plagen des Cyberwar', in Roman Schmidt-Radefeldt/Christine Meissler (Hrsg.), Automatisierung und Digitaliserung des Krieges, Baden-Baden 2012, S. 89 ff, 91 ff.

[2] Wolff Heintschel von Heinegg, ‚Cyberspace – Ein völkerrechtliches Niemandsland?', in Schmidt-Radefeld/Meissler (Hrsg.). a.a.O. Anm. 1, S. 159 ff.

[3] Michael N. Schmitt (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepare by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, Cambridge 2013.

[4] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. 68/98, Ziff. 16 ff.

[5] Sven-Hendrik Schulze, Cyber-"War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015, S. 177; Heike Krieger, ‚Krieg gegen anonymus. Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar', AVR 50 (2012), S. 1 ff., 18.

Der Ansatz des Tallinn Manual stößt zumindest an seine Grenzen wegen eines spezifischen Problems von Cyberangriffen, nämlich ihrer mangelnden Rückverfolgbarkeit,[6] d.h. der fehlenden Identifizierbarkeit des Urhebers. Dies ist eine Herausforderung für jede Rechtsordnung, deren Regelungsmöglichkeiten vorrangig auf Zurechnung beruhen.[7] Wo der Urheber eines Schadens nicht zu ermitteln ist, ist eine Ahndung der Schadensstiftung als Unrecht nicht möglich. Das ist an sich kein neues Phänomen. Wo allerdings die mangelnde Bestimmbarkeit des Schädigers für eine bestimmte Form der Schadensstiftung so typisch ist wie bei Cyberangriffen, stellt sich die Frage, ob es mit einem solchen unbefriedigenden Ergebnis sein Bewenden haben kann und ob es Wege gibt, das Problem der Rückverfolgbarkeit von Cyberangriffen angemessen zu regeln.

Im Folgenden soll versucht werden, für einige relevante Regeln des Völkerrechts und des Verfassungsrecht die Anwendung auf die besondere Form der Schadensstiftung durch Cyberangriffe zu untersuchen und dabei auch auf das besagte Problem der Rückverfolgung einzugehen.

2. Völkerrecht

Zur völkerrechtlichen Beurteilung sind folgende Normen zugrunde zu legen:

- Verbot der grenzüberschreitenden Schadensstiftung, sog. no harm rule;
- Interventionsverbot;
- Gewaltverbot;
- Verbot des bewaffneten Angriffs, eine qualifizierte Form des Gewaltverbots.

Diese Kategorisierungen beruhen auf der einschlägigen Rechtsprechung des Internationalen Gerichtshofs. Er hat sie insbesondere in dem Urteil in Sachen Nicaragua gg. USA 1986 entwickelt,[8] das bis heute als im wesentlichen unbestrittene Feststellung der Rechtslage nach Völkergewohnheitsrecht gilt. Verletzungen dieser Verbote können mit verhältnismäßigen Gegenmaßnahmen beantwortet werden, mit einem militärischen Gegenschlag, d.h. Selbstverteidigung i.S. Art. 51 UN Charter, nur der bewaffnete Angriff.

Das Verbot grenzüberschreitender Schadensstiftung ist eine Regel des allgemeinen Völkerrechts, die in den letzten Jahrzehnten vor allem bei Fragen des Ersatzes für grenzüberschreitende Umweltbelastungen eine Rolle gespielt hat. Sie gilt aber für jede Art von Schadensstiftung. Sie verbietet nicht nur direkte Schadensstiftung durch staatliche Organe, sondern verpflichtet auch die Staaten, keine grenzüberschreitende Schadensstiftung durch Private zuzulassen. Nach Völkergewohnheitsrecht müssen die Staaten zur Verhinderung grenzüberschreitender Schadensverursachung die gebotene Sorgfalt (due

[6] Schulze, a.a.O. Anm. 5, S. 36 ff.
[7] Krieger, a.a.O. Anm. 5, S. 3.
[8] *Military and Paramilitary Activities in and around Nicaragua, Nicaragua v. U.S.*, Merits, Urteil v. 27.6.1986, Ziff. 195; siehe auch Andreas v. Arnault, Völkerrecht, 2. Aufl., Karlsruhe 2014, S. 449

diligence) walten lassen.[9] Das gilt auch für Schädigungen mittels Cyber-Angriffen. Welche Sorgfaltspflichten allerdings insofern zur Verhinderung grenzüberschreitender privater Hacker-Tätigkeiten u.ä. folgen, ist noch weitgehend ungeklärt. Das Tallinn Manual formuliert diese Pflicht zur Verhinderung solcher schadenstiftender Cyberaktivitäten ein, die dem Staat bekannt sind:

> „A State shall not knowingly allow cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[10]

Damit bleibt das Manual meines Erachtens hinsichtlich des wissen Müssens hinter dem geltenden Gewohnheitsrecht zurück. In der Expertengruppe herrschte diesbezüglich Uneinigkeit.[11] Über die Tragweite staatlicher Pflichten zur Kontrolle von privaten schadensstiftenden Handlungen mittels und in Computer-Netzwerken ist de lege lata und de lege ferenda weiter nachzudenken.

Das Interventionsverbot ist Bestandteil des völkerrechtlichen Gewohnheitsrechts. Es verbietet (so der IGH) die Ausübung von Zwang gegenüber einem Staat in Bereichen, die kraft der staatlichen Souveränität seiner freien Entscheidung unterliegen.[12]
Wo genau die Schwelle verbotener Einflussnahme liegt, ist schon für das Interventionsverbot im Allgemeinen umstritten. Wird ein solcher Eingriff durch Einflussnahme auf das Funktionieren von Computer-Systemen ausgeübt, ist diese Grenzziehung noch weitgehend ungeklärt. Das entscheidende Kriterium kann nur die Vergleichbarkeit mit Einflussnahmen traditioneller Art sein.[13]

Das Gewaltverbot nach der Satzung der Vereinten Nationen und nach völkerrechtlichem Gewohnheitsrecht verbietet nur militärische Gewalt. Wird die Gewalt nicht durch staatliche Organe selbst ausgeübt, so ist sie einem Staat dennoch zuzurechnen, wenn er in die betreffenden nicht staatlichen Aktivitäten erheblich involviert ist.[14] Darum ist zu prüfen, ob Schadensstiftung durch Computerangriffe ggf. einem militärischen Angriff gleich zu achten sind. In den einschlägigen völkerrechtlichen Diskursen setzt sich insofern das Kriterium von „scale and effects" (Umfang und Wirkung) durch. Dem folgt auch das Tallinn Manual. Schadensstiftung durch Computerangriffe ist also militärischer Gewalt gleich zu achten, wenn sie physische Zerstörungen von erheblichem Umfang verursacht, die denen vergleichbar sind,

---

[9] Eine Übersicht über die verschiedenen Rechtsbereiche, in denen due diligence eine Rolle spielt, bei Timo Koivurova, ‚Due Diligence', Rdn. 29 ff., in Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedia of Public International Law (www.mpepil.com); vgl. auch Schulze, a.a.O. Anm. 5, S. 118 ff., 143.
[10] Tallinn Manual, Rule 5.
[11] Tallinn Manual, S. 28; unklar Schulze, a.a.O. Anm. 5, S. 143.
[12] Philip Kunig, 'Intervention, Prohibition of', in MPEPIL (Anm.9).
[13] Vgl. Tobias O. Keber/Przemysław Roguski, ‚Ius ad bellum electronicum. Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis', AVR 49 (2011), S. 399 ff., 409 f.
[14] *Nicaragua*-Urteil, Anm. 8, Ziff. 195.

die durch gewöhnliche militärische Angriffe, insbesondere Angriffe mittels kinetischer Waffen, verursacht werden:[15]

> „A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of the use of force."[16]

Was in diesem Sinne „erheblich" ist, d.h. „rising to the level of the use of force", darüber ist Streit möglich und sogar wahrscheinlich. Das gilt auch und gerade für die Unterscheidung zwischen einer Verletzungen des Gewaltverbots von minderem Ausmaß und dem bewaffneten Angriff, der ein Selbstverteidigungsrecht auslöst:

> „A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[17]

Die Zulässigkeit eines militärischen Gegenschlags hängt also davon ab, ob die zuvor ausgeübte (oder unmittelbar drohende) Erstgewalt die Schwelle eines bewaffneten Angriffs erreicht oder überschreitet. Es bestehen erhebliche Interpretationsspielräume. Diese Interpretationsspielräume sind missbrauchsanfällig, da die als rechtliche Grundlage einer Entscheidung zum Einsatz militärischer Gewalt nicht nur ge-, sondern auch missbraucht werden können. Einzelheiten waren denn auch in der Expertengruppe des Tallinn Manual umstritten. Die Mehrheit der Gruppe war der Auffassung, dass ein bewaffneter Angriff in diesem Sinn jedenfalls nicht den Einsatz von Waffengewalt mit kinetischer Energie voraussetzt (dann könnte ein Cyber-Angriff wohl nie als bewaffneter angriff qualifiziert werden), sondern dass es auf die Wirkung des Angriffs ankommt. Gleicht diese Wirkung der eines Angriffs mit kinetischer Energie, d.h. führt sie zu Tod oder Verwundung von Personen bzw. Beschädigung oder Zerstörung von Sachgütern, liegt ein bewaffneter Angriff vor.[18] Gerade wegen der besagten Missbrauchsmöglichkeit müssen an den Umfang des physischen Schadens, dessen Verursachung das Selbstverteidigungsrecht auslöst, hohe Anforderungen gestellt werden.[19] Ob auch erhebliche Schäden anderer Art einen Cyber-Angriff zu einem „bewaffneten" Angriff machen, war in der Expertengruppe umstritten.[20] M.E. ist dies wegen der besagten Missbrauchsmöglichkeit abzulehnen.

Bislang ist der einzige bekannte Fall eines Cyber-Angriffs, bei dem physische Schäden verursacht wurden, der Stuxnet-Angriff auf iranische Atomzentrifugen 2010. Die Expertengruppe des Tallinn Manual war sich in der Beurteilung nicht einig.[21] Ein Autor

---

[15] In diesem Sinn auch Daniel B. Silver, ‚Computer Network Attacks as a Use of Force under Article 2(4) 0f the United Nations Charter', in: Michael N. Schmitt/Brian T. O'Donnell (Hrsg.), Computer Network Attack and International Law, International Law Studies vol. 76, Newport 2002, S. 73 ff., 85.
[16] Tallinn Manual, Rule 11.
[17] Tallinn Manual, Rule 13.
[18] Talinn Manual, S. 55. In diesem Sinn auch Yoram Dinstein, 'Computer Network Attacks and Self-Defence', in Schmitt/O'Donnell (Hrsg.), a.a.O. Anm. 15, S. 99 ff., 103; Keber/Roguski, a.a.O. Anm. 13, S.408.
[19] Krieger, a.a.O. Anm. 5, S. 11.
[20] Tallinn Manual, S. 56.
[21] Tallinn Manual, S. 58.

äußert sich vorsichtig dahin, dass die Qualifizierung als bewaffneter Angriff „nicht von vornherein ausgeschlossen“ sei.[22]

Aus dem Gesagten folgt: Ein Cyber-Angriff auf einen NATO-Staat löst nur dann die Rechtsfolge des Art. 5 NATO-Vertrag aus, wenn er die dargestellte Schwelle eines bewaffneten Angriffs erreicht.

Selbstverteidigung ist diejenige militärische Gewalt, die erforderlich und verhältnismäßig ist, um einen bewaffneten Angriff abzuwehren. Die Selbstverteidigung richtet sich gegen den Angreifer, und nur gegen diesen. Nach der Rechtsprechung des IGH trifft insofern die Beweislast denjenigen, der sich auf Selbstverteidigung beruft. Er muss nachweisen, dass ein bewaffneter Angriff von dem Adressaten der Verteidigungsmaßnahme verübt worden ist,[23] d.h. einem bestimmten Staat zuzurechnen ist. So hat es der IGH in einem Fall unklarer Zuordnung des Erstangriffs entschieden und an diesen Nachweis hohe Anforderungen gestellt.[24] Selbstverteidigung auf Verdacht ist unzulässig.[25] Dies ist angesichts der Unsicherheit der zuverlässigen Beurteilung der Herkunft von Cyberangriffen ein schwieriges Problem. Nach dem Tallinn Manual ist jedenfalls die Tatsache, dass eine Schädigungshandlung von einem Server herrührt, der sich auf dem Gebiet eines bestimmten Staates befindet, nicht ausreichend, um die Schädigungshandlung diesem Staat zuzurechnen[26] und ihn somit zum Adressaten eines zulässigen militärischen Gegenschlages zu machen.

In diesem Zusammenhang stellt sich auch für Cyber-Angriffe die allgemeiner bezüglich terroristischer Angriffe umstrittene Frage, ob und inwieweit Angriffe, die von nicht-staatlichen Akteuren begangen werden, bewaffnete Angriffe im Sinne des Art. 51 UN Charter darstellen.[27] Das kann hier nicht im Einzelnen diskutiert werden. Jedenfalls kann die Verletzung von staatlichen Kontrollpflichten gegenüber privaten Cyber-Angriffen diese nicht zu einem bewaffneten Angriff seitens des Herkunftsstaates machen.

Selbstverteidigung rechtfertigt militärische Gewalt, die ohne diese Rechtfertigung unzulässig wäre. Darum sind von Selbstverteidigung in diesem Sinne zu unterscheiden passive Abwehr- und Schutzmaßnahmen, die ein Staat stets treffen kann. Beispiele in der materialen Welt ist etwa, wenn ein in den staatlichen Luftraum eingedrungenes Flugzeug zur Landung gezwungen wird, selbst wenn das Eindringen noch nicht einen bewaffneten Angriff darstellt. Gegen Computer-Operationen ist eine vergleichbare Maßnahme etwa ein Firewall. Solche Maßnahmen sind ohne Vorliegen eines bewaffneten Angriffs im dargestellten Sinne zulässig. Die Abgrenzung im Einzelnen mag nicht immer einfach sein.

---

[22] Schulze, a.a.O. Anm. 5, S. 127.
[23] *Oil Platforms, Iran v. U.S.*, Merits, Urteil v. 6.11.2003, Ziff. 57 ff., 71 f.; vgl. Marco Roscini, ‚Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, in Jens David Ohlin (Hrsg.), Cyberwar, Oxford 2015, S. 215 ff.
[24] Zu Einzelheiten der Beweismaßstäbe Roscini, a.a.O. Anm. 23, S. 217.
[25] Vgl. auch Michael Bothe, ‚Terrorism and the Legality of Pre-emptive Force‘, EJIL 14 (2003), S. 227 ff., 232: zweifelnd Keber/Roguski, a.a.O. Anm. 13, S. 416.
[26] Tallinn Manual, Rule 8.
[27] Vgl. zum Streit Tallinn Manual , 58 f.; Dinstein, a.a.O. Anm. 18, 111 f.

Von den besagten Verbotsnormen sind zu unterscheiden die Regeln des humanitären Völkerrechts über zulässige oder unzulässige Mittel der Schädigung des Gegners im Rahmen eines bewaffneten Konflikts. Es gilt insbesondere das Unterscheidungsgebot: Angriffe dürfen nur gegen militärische Ziele gerichtet werden, nicht gegen zivile Objekte. Militärische Ziele sind solche Objekte, die zu den militärischen Anstrengungen des Gegners beitragen und deren Zerstörung bzw. sonstige Ausschaltung einen militärischen Vorteil erwarten lässt. Zivile Begleitschäden sind verboten, wenn der zu erwartende zivile Schaden eines Angriffs außer Verhältnis zu dem erwarteten unmittelbaren militärischen Nutzen steht. Wenn einmal ein bewaffneter Konflikt besteht, wie immer er begonnen wurde, stellt sich die Frage, ob und inwieweit Cyberangriffe an diesen Maßstäben zu messen sind. Diese Frage wird heute allgemein bejaht, wenn durch eine Cybermaßnahme die von einem militärischen Angriff gemeinhin ausgehenden Folgen eintreten oder zu erwarten sind: Tod oder Verletzung von Personen bzw. Zerstörung oder Beschädigung von Sachgütern.[28]

Angesichts der Unsicherheiten einer Rückverfolgung von Angriffen und der damit verbundenen faktischen und rechtlichen Schwierigkeit von Gegenmaßnahmen ist die Pflicht zu Vorsichtsmaßnahmen, wie sie z.B. in Art. 58 ZP I formuliert ist, für den Cyberwar besonders wichtig.[29]

Im internationalen bewaffneten Konflikt sind nur Kombattanten, d.h. Angehörige der Streitkräfte berechtigt, an Kampfhandlungen teilzunehmen, d.h. Angriffe auf den Gegner auszuführen. Das macht für den Cyberwar das Problem nicht-staatlicher Akteure (z.B. Hacker) rechtlich besonders heikel.[30]

3. Verfassungsrecht

Eine erste verfassungsrechtliche Folgerung, die aus der völkerrechtlichen Analyse gezogen werden muss, folgt aus Art. 26 GG, dem Verbot des Angriffskrieges. Sie geht dahin, dass die Bundesrepublik keine Cyber-Angriffe unternehmen oder sich an ihnen beteiligen darf, die nach dem Gesagten den Tatbestand des Gewaltverbots erfüllen und nicht als Selbstverteidigung nach Art. 51 UN Charter gerechtfertigt sind. Die bei der völkerrechtlichen Analyse dargestellten Unsicherheiten gelten entsprechend für die verfassungsrechtliche Bewertung. Es ist auch in diesem Zusammenhang zu betonen, dass eine Selbstverteidigung auf Verdacht nicht zulässig ist und damit unter das Verbot des Art. 26 GG fällt.

Eine wesentliche und noch nicht hinreichend diskutierte verfassungsrechtliche Frage ist die Anwendung des Erfordernisses der Parlamentsbeteiligung auf Cyber-Angriffe. Dieser Parlamentsvorbehalt gilt für Beteiligung der deutschen Streitkräfte an militärischen Unternehmen. Eine erste Antwort auf diese Frage liegt in einer angemessenen Anwendung des scale and effects-Kriteriums. Denn wenn für die völkerrechtliche Definition eines Angriffs, der eine Verletzung des Gewaltverbots oder gar einen bewaffneten Angriff im Sinne

[28] Ausführlich: Tallinn Manual, Rules 30-59. Vgl. auch Heintschel von Heinegg, a.a.O. Anm. 2, 162 ff.
[29] Krieger, a.a.O. Anm. 5, S. 17.
[30] Nicolò Bussolati, ‚The Rise of Non-State Actors in Cyberwarfare', in Ohlin (Hrsg.), a.a.O. Anm. 23, S. 102 ff.

des Art. 51 UN Charter darstellt, von der Notwendigkeit eines Waffeneinsatzes abgesehen und auf die Wirkung abgestellt wird, dann sollte das auch für den Einbezug von Soldaten „in bewaffnete Unternehmungen“, der nach der Rechtsprechung des Bundesverfassungsgerichts[31] das Zustimmungserfordernis auslöst, relevant sein.

Bei Computer-Angriffen durch deutsche Staatsorgane ist zu beachten, dass das Erfordernis der Parlamentsbeteiligung nur für Handlungen der Streitkräfte gilt. Für andere Staatsorgane, etwa für (nichtmilitärische) Geheimdienste gilt es nicht. Für den internationalen bewaffneten Konflikt gilt allerdings, dass Kampfhandlungen, d.h. Maßnahmen zur Schädigung des Gegners, nur durch Kombattanten, Mitglieder der Streitkräfte ausgeführt werden dürfen. Das gilt auch für Cyber-Angriffe.

Handelt es sich bei Computer-Angriffen um Maßnahmen der Streitkräfte, so gilt der Parlamentsvorbehalt jedenfalls, wenn diese Maßnahmen nach dem scale and effects-Kriterium einer militärischen Maßnahme gleich zu achten sind. Relevant ist diese Frage natürlich nur, soweit Cyberangriffe isolierte Maßnahmen darstellen. Geschehen sie im Rahmen einer ohnehin stattfinden militärischen Aktion, gilt der Parlamentsvorbehalt für die gesamte Aktion.

Bei separaten Cyber-Operationen ist es eine Frage des konkreten Szenarios, ob die Schwelle zu einer militärischen Aktion nach dem scale and effects-Kriterium erreicht oder überschritten ist. Dazu eine Übersicht von Szenarien zu liefern, kann nicht Aufgabe dieser Stellungnahme sein.

Zu bedenken ist in diesem Zusammenhang allerdings darüber hinaus, dass nach der Rechtsprechung des Bundesverfassungsgerichts die Schwelle für den Parlamentsvorbehalt ja viel niedriger liegt als bei dem Einsatz von Waffengewalt, die entweder eine Verletzung des Gewaltverbots darstellt oder der besonderen Rechtfertigung als Selbstverteidigung bzw. durch ein Mandat des Sicherheitsrats bedarf. Welche Cyber-Operationen in diesem Sinne einen Einbezug in militärische Maßnahmen darstellen, ist ohne eine gründliche Diskussion einschlägiger Szenarien kaum zu entscheiden.

In diesem Zusammenhang stellt sich die weitere Frage, ob für Cyber-Angriffe möglicherweise eine vom Bundesverfassungsgericht zugelassene Ausnahme vom Parlamentsvorbehalt vorliegt. Das Bundesverfassungsgericht führt in seiner grundlegenden Entscheidung zur Tragweite des Parlamentsvorbehalts aus, dass durch die Mitwirkung des Bundestages „die militärische Wehrfähigkeit und die Bündnisfähigkeit der Bundesrepublik Deutschland“ nicht beeinträchtigt werden dürfe. Als einziges Beispiel für dieses Prinzip führt das Gericht aus, die Bundesregierung sei bei Gefahr im Verzug berechtigt, vorläufig den Einsatz von Streitkräften zu beschließen. Diese Formulierung ist in § 5 des Parlamentsbeteiligungsgesetzes übernommen worden. Dabei wird eine Situation gleich behandelt, bei der eine vorgängige

[31] Urteil vom 12.7.1994, 2 BvE 3/92, BVerfGE 90, 286; ferner die Urteile vom 7.5.2008, 2 BvE 1/03, BVerfGE 121, 135 (AWACS Türkei) und vom 23.9.2015, 2 BvE 6/11 (Libyen).

öffentliche Debatte das Leben von zu rettenden Menschen gefährden würde.[32] Ob in diesem Sinne bei Cyberangriffen, die durch die Bundeswehr durchgeführt werden, Gefahr im Verzug ist, ist eine Frage des Einzelfalls.

In der Praxis hat sich daneben, offenbar auf dem Boden der Forderung des BVerfG, dass die militärische Wehrfähigkeit nicht beeinträchtigt werden dürfe, eine besondere Behandlung von Operationen herausgebildet, von denen angenommen wird, dass sie ihrer Natur nach geheimhaltungsbedürftig sind.[33] Dieses Verfahren beruhte zunächst auf einer Absprache zwischen Bundesregierung und den Fraktionsvorsitzenden und sieht nur eine Unterrichtung bestimmter Abgeordneter unter Wahrung des Geheimschutzes vor. Es soll in die Neufassung des Parlamentsbeteiligungsgesetzes (§ 6a) übernommen werden. Diese Vorschrift betrifft nur den geheimhaltungsbedürftigen Einsatz von Spezialkräften. Cyberangriffe werden in der neuen Bestimmung nicht geregelt. Es wäre freilich zu erwägen, ob der Grundsatz der Nichtbeeinträchtigung der Wehrfähigkeit, wie ihn das BVerfG formuliert hat, nicht auch für bestimmte Cyberangriffe gelten könnte. Es könnte argumentiert werden, dass solche Angriffe nur wirksam sind, wenn sie den Gegner unvorbereitet treffen. Sie könnten deshalb als ihrer Natur nach geheimhaltungsbedürftig angesehen werden. Das Verfahren zum geheimhaltungsbedürftigen Einsatz von Spezialkräften könnte dafür als Vorbild dienen. Die Bundesregierung könnte also nicht einseitig von der Parlamentsbeteiligung absehen, sondern müsste zusammen mit den Funktionsträgern der Fraktionen angemessene Lösungen finden. Allein eine solche kooperative Lösung entspräche dem Sinn des Parlamentsvorbehalts.

4. Sinnhaftigkeit und Möglichkeit neuer völkerrechtlicher Verträge

Die praktische Anwendung des scale and effects-Kriteriums lässt sich wohl kaum in allgemeiner Form durch völkerrechtlichen Vertrag regeln. Immerhin wäre eine allgemeine Formulierung des Prinzips in einem Vertragstext ein Schritt zu mehr Rechtssicherheit.

Auch für die Fragen der Zurechnung oder von Sorgfaltspflichten bei der Kontrolle privater Tätigkeiten auf eigenem Staatsgebiet wäre eine angemessene Regelung wohl sinnvoll. Allerdings scheiden sich die Geister bei der Frage der Intensität staatlicher Kontrollpflichten,[34] wie insbesondere die Beratungen in den Vereinten Nationen ergeben haben.

Ob die Zeit für eine solche Regelung schon reif ist, ist nicht nur deshalb fraglich. Es liegt nicht nur an den dargestellten Schwierigkeiten der Materie, dass die Chancen für den Versuch einer vertraglichen Regelung, was immer ihr Inhalt, schlecht stehen.[35] Gegenwärtig besteht in der internationalen Gemeinschaft ein verbreiteter Unwille, Fragen der Ausübung militärischer

[32] § 5 Abs. 1 Satz 2 ParlamentsbeteiligungsG.
[33] Bericht der sog. Rühe-Kommission, BT Drs. 18/5000, S. 43 f.
[34] Schulze, a.a.O. Anm. 5, S. 177, 182 ff.; Krieger, a.a.O. Anm. 5, S. 18; Keber/Roguski, a.a.O. Anm. 13, S. 420 ff.
[35] Vgl. auch Philip A. Johnson, , Is It Time for a Treaty on Information Warfare?‘, in Schmitt/O’Donnell (Hrsg.), a.a.O. Anm. 15, S. 439 ff., 453.

Gewalt und insbesondere offene Fragen des humanitären Völkerrechts sowie Fragen der Haftung vertraglich zu regeln.

Deshalb scheint gegenwärtig die wichtigere Option für die Eindämmung der durch Cyber-Angriffe zu befürchtenden Schäden die Entwicklung technischer Schutzmechanismen zu sein.