Ausarbeitung

Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland

Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland

Aktenzeichen:	WD 3 - 3000 - 159/18
Abschluss der Arbeit:	08.06.2018
Fachbereich:	WD 3: Verfassung und Verwaltung

1. Fragestellung

Die Ausarbeitung thematisiert die Vereinbarkeit von Angriffen auf ausländische Server in Form von sog. „Hackbacks“ mit Art. 26 GG. Insofern stellt sich die Frage, ob entsprechende Angriffe auf Server und die IT-Infrastruktur im Ausland mit dem in Art. 26 Abs. 1 GG normierten Verbot friedensstörender Handlungen in Einklang stehen kann. Ferner ist zu thematisieren, welche staatliche Stelle zur Ausführung etwaiger Cybermaßnahmen befugt ist.

Vorab ist anzumerken, dass die Verfassungsmäßigkeit solcher Maßnahmen in jedem Einzelfall festgestellt werden muss. Daher beschränken sich die Ausführungen vorliegend auf allgemeine Erwägungen.

2. Rechtliche Einordnung von Cyberangriffen

Die Bundesregierung geht davon aus, dass für Cyberangriffe keine besonderen rechtlichen Regelungen bestehen. Ihr Einsatz richte sich vielmehr nach den rechtlichen Vorgaben für militärische Einsätze. In einer Antwort auf eine Kleine Anfrage führt sie ausdrücklich aus:

> „Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. Grundlagen für Einsätze der Bundeswehr sind die einschlägigen Regelungen des Grundgesetzes sowie des Völkerrechts, Maßnahmen des Sicherheitsrates nach Kapitel VII der VN-Charta (Mandate), völkerrechtliche Vereinbarungen mit dem betreffenden Staat und das Parlamentsbeteiligungsgesetz. Im Falle eines Einsatzes im bewaffneten Konflikt gilt das humanitäre Völkerrecht.“[1]

In der Literatur wird daher überwiegend davon ausgegangen, dass auch Cyberangriffe eine Verletzung des völkerrechtlichen Gewaltverbots darstellen können, wenn eine bestimmte Erheblichkeitsschwelle überschritten wird. Hierzu wird auf das Ausmaß der Gewalt und ihrer Wirkung (scale and effects) abgestellt. Kommt dieses Ausmaß dem einer Anwendung konventioneller Waffen gleich, etwa weil Menschen verletzt oder getötet oder erhebliche Sachgüter zerstört wurden, kann dies als Verstoß gegen das Gewaltverbot bzw. als Angriff im Sinne von Art. 51 der UN-Charta gewertet werden.[2]

3. Einklang von Cybermaßnahmen mit Art. 26 Abs. 1 GG

Nach Art. 26 Abs. 1 GG sind Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören, insbesondere die Führung eines Angriffskrieges vorzubereiten, verfassungswidrig. Die Vorschrift schützt das friedliche Zusammenleben der Völker. Sowohl das Vorbereiten eines Angriffskrieges als auch sonstige darüber hinaus gehende friedensstörende Handlungen sind verfassungswidrig. Die genannten sonstigen

---

1 BT-Drs. 18/6989, S. 4.

2 Zum Ganzen m.w.N. Ladiges, Der Cyberraum – ein (wehr-)verfassungsrechtliches Niemandsland?, in: NZWehrr 2017, 221 (225 f.).

friedensstörenden Handlungen müssen, um den Anwendungsbereich des Art. 26 Abs. 1 GG zu eröffnen, in der konkreten Situation zu einer schwerwiegenden Beeinträchtigung des zwischenstaatlichen Verkehrs führen.[3] Insbesondere sind solche Handlungen verboten, die eine erhöhte Gefahr gewaltsamer staatlicher Konflikte mit sich bringen oder eine Bedrohung des Weltfriedens im Sinne von Art. 39 UN-Charta darstellen.[4]

Mangels des Vorliegens bisheriger Präzedenzfälle ist bei Cybermaßnahmen das allgemeine völkerrechtliche Gewaltverbot gem. Art. 2 Abs. 4 der UN-Charta als Auslegungshilfe zugrunde zu legen. Danach ist militärische Waffengewalt grundsätzlich untersagt, es sei denn, sie ist ausnahmsweise völkerrechtlich gerechtfertigt. Eine Rechtfertigung kann sich insbesondere aus dem Selbstverteidigungsrecht nach Art. 51 der UN-Charta als auch aus der Einordnung als kollektive Zwangsmaßnahme des Sicherheitsrates der Vereinten Nationen nach Art. 39 u. Art. 42 der UN-Charta ergeben. Weiterhin muss das Ausmaß des Einsatzes ein gewisses Gewicht besitzen.

Zur Beurteilung des Ausmaßes eines Cyberangriffs ist zu überprüfen, ob dieser hinsichtlich der oben genannten Kriterien „scale“ (Ausmaß) und „effect“ (Auswirkung) mit klassischen Formen militärischer Gewalt vergleichbar ist. Cybermaßnahmen sind insbesondere dann mit militärischer Gewalt gleichzusetzen, wenn sie physische Zerstörungen von einem erheblichen Umfang verursachen.[5] Die Anforderungen an eine gewaltsame Handlung werden im Bereich der Cybermaßnahmen von der Literatur insgesamt niedrig angesetzt. Grund dafür sei das erhebliche Eskalationspotenzial, das diesen Einsätzen inhärent ist. Wegen der Unsicherheiten bei der Rückverfolgung von Cyberangriffen könne regelmäßig nicht mit Gewissheit festgestellt werden, ob sich die (Gegen-)Maßnahme tatsächlich gegen den Verantwortlichen richte. Dadurch werde die Gefahr von Gegenmaßnahmen oder einer ungewollten Eskalation erhöht.[6]

Im Ergebnis ist zur Beurteilung eines Cyberangriffes im Lichte des Art. 26 Abs. 1 GG im Einzelfall festzustellen, ob ein Cyberangriff dem Ausmaß nach eine Verletzung des völkerrechtlichen Gewaltverbots darstellt. Ist dies der Fall, kann u.U. auch der Anwendungsbereich des Art. 26 Abs. 1 GG eröffnet sein, wenn sich der Einsatz nicht entsprechend rechtfertigen lässt. Eine mögliche Rechtfertigung der militärischen Gewalt ergibt sich auf völkerrechtlicher Ebene hierbei insbesondere aus dem in Art. 51 UN-Charta verankerten Recht der Selbstverteidigung.[7]

Art. 26 Abs. 1 GG verlangt auf subjektiver Ebene zudem die Beabsichtigung der Friedensstörung. Diese liegt vor, sofern dem Handelnden die konkrete Gefahr einer Friedensbedrohung bewusst

---

3 Vgl. Hillgruber, in: Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), Grundgesetz, 14. Aufl. 2018, Art. 26, Rn. 14.

4 Vgl. Herdegen, in: Maunz/Dürig (Hrsg.), Grundgesetz, 81. EL September 2017, Art. 26 Rn. 40.

5 Vgl. Bothe, Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsausschuss des Deutschen Bundestages vom 17.02.2016, Ausschussdrucksache 18(12)633, S. 5 f.; Ladiges, Der Cyberraum – ein (wehr-)verfassungsrechtliches Niemandsland?, in: NZWehrr 2017, 221 (225 f.) m.w.N.

6 Vgl. auch Marxsen, Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr, JZ 2017, 543 (550).

7 Vgl. Herdegen, in: Maunz/Dürig (Hrsg.), Grundgesetz, 81. EL, Art. 26 Rn. 29; umfassend hierzu: Bothe, Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsausschuss des Deutschen Bundestages vom 17.02.2016, Ausschussdrucksache 18(12)633, S. 6 ff.

war und er sie zumindest billigend in Kauf genommen hat.[8] Das alleinige Streben nach einer Veränderung der bestehenden Zustände reicht hierfür in der Regel nicht aus, wenn es den Grundsätzen des friedlichen Wandels entspricht.[9]

4. Zwischenergebnis

Auch Cyberangriffe müssen grundsätzlich im Einklang mit dem in Art. 26 Abs. 1 GG verankerten Verbot friedensstörender Handlungen stehen.[10]

5. Durchführung von Cybermaßnahmen durch Militär oder Nachrichtendienste?

Für die Einordnung von Cybermaßnahmen im Lichte des Art. 26 Abs. 1 GG oder die völkerrechtliche Beurteilung ist es zunächst irrelevant, welche staatliche Stelle eine ungerechtfertigte Cybermaßnahme durchführt und gegen das Gewaltverbot verstößt. Der Anwendungsbereich des Art. 26 Abs. 1 GG beschränkt sich nicht auf Handlungen der Bundeswehr.[11] Auch völkerrechtlich würden entsprechende Handlungen, unabhängig davon welche staatliche Institution diese ausführt, dem Staat zugerechnet werden.

Kampfhandlungen im Rahmen internationaler Konflikte dürfen jedoch auch im Bereich der Cybermaßnahmen nach der derzeitigen Rechtslage nur durch Kombattanten, also Mitglieder der Streitkräfte, ausgeführt werden.[12] Folglich ist nur die Bundeswehr zu entsprechenden Cybermaßnahmen befugt.

Nach derzeitiger Rechtslage haben die Nachrichtendienste zudem grundsätzlich keine klassischen Eingriffsbefugnisse. Ihr Zuständigkeitsbereich beschränkt sich auf Aufklärungsmaßnahmen. An dieser Stelle soll dahinstehen, ob sich aus dem sog. Trennungsgebot auch ein Verbot für die Einräumung entsprechender Eingriffsbefugnisse herleiten lässt.[13] Eine Durchführung von Cyberangriffen durch Nachrichtendienste würde jedenfalls zu einer erheblichen Erweiterung der bisherigen nachrichtendienstlichen Befugnisse führen.

---

8 Vgl. Herdegen, in: Maunz/Dürig (Hrsg.), Grundgesetz, 81. EL September 2017, Art. 26 Rn. 42.

9 Streinz, in: Sachs (Hrsg.), GG, 8. Aufl. 2018, Art. 26 Rn. 29.

10 Ladiges, Der Cyberraum – ein (wehr-)verfassungsrechtliches Niemandsland?, in: NZWehrr 2017, 221 (240).

11 Vgl. Streinz, in: Sachs, GG, 8. Aufl. 2018, Art. 26 Rn. 22 f.

12 Ladiges, Der Cyberraum – ein (wehr-)verfassungsrechtliches Niemandsland?, in: NZWehrr 2017, 221 (226 f.); Bothe, Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsausschuss des Deutschen Bundestages vom 17.02.2016, Ausschussdrucksache 18(12)633, S. 9.

13 Zum Ganzen: Cremer in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, 3. Aufl. 2014, § 278 Organisationen zum Schutz von Staat und Verfassung, Rn. 22 ff.

6. Strafbarkeit

Nach Art. 26 Abs. 1 S. 2 GG sind Handlungen im oben genannten Sinne unter Strafe zu stellen. Bisher enthielten die §§ 80, 80a StGB einen bis dahin nur unvollständigen strafrechtlichen Schutz, da die Tatbestände nicht sämtliche Handlungen i.S.d. Art. 26 Abs. 1 GG erfassten.[14] Nunmehr stellt § 13 des Völkerstrafgesetzbuches sowohl die Planung als auch die Durchführung eines Angriffskrieges unter Strafe. Der Gesetzgeber geht davon aus, mit dieser Regelung das verfassungsrechtliche Aggressionsverbot in Art. 26 GG zu berücksichtigen.[15]

***

14 Vgl. Hillgruber, in: Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), Grundgesetz, 14. Aufl. 2018, Art. 26 Rn. 20; Herdegen, in: Maunz/Dürig (Hrsg.), Grundgesetz, 81. EL September 2017, Art. 26 Rn. 55.

15 BT-Drs. 18/8621, S. 16.