Nr. 508D
27.06.2018
BOFAXE

„Hackback“ – Darf Deutschland zurückschlagen?

Autor / Nachfragen

Stephan Koloß**a**
Wiss. Mit. am Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht (IFHV) und Mitglied des SecHuman-Fortschrittskollegs

Nachfragen:
stephan.kolossa@rub.de

Webseite

http://www.ifhv.de

Fokus

Die Bundesregierung rüstet sich mehr und mehr zur aktiven Bekämpfung von Cyber-Angriffen. Ein solcher Gegenschlag ist jedoch nur selten im Einklang mit dem Völkerrecht und Art. 26 GG.

Quellen:

https://www.tagesschau.de/inland/hacker-angriff-101.html

https://www.tagesschau.de/inland/cyberangriffe-hacking-101.html

https://cdn.netzpolitik.org/wp-upload/2018/06/WD-3-159-18.pdf

Es häufen sich die Berichte in den Medien über Hackerangriffe auf staatliche Einrichtungen wie Ministerien oder das Parlament. Auch einzelne hohe Beamte sind Ziel von Attacken aus dem Internet. Diese Vorfälle sind international kein Einzelfall. Medienberichten zufolge betraf der Angriff auf das deutsche Regierungsnetz, der vor wenigen Monaten begann, weitere Staaten, darunter solche in Skandinavien, Südamerika sowie ehemalige Sowjet-Staaten. Laut wird daher der Ruf nach einer effektiveren Verteidigung mittels eines Cyber-Gegenangriffs, um die Quelle des digitalen Angriffs zu eliminieren und den Angriff zu unterbinden. Der Wissenschaftliche Dienst des Bundestages hat nun zu der maßgeblichen Frage Stellung bezogen, ob ein solcher Verteidigungsgegenschlag mit der deutschen Verfassung, namentlich mit dem Verbot des Angriffskrieges aus Art. 26 Abs. 1 S. 1 GG in Einklang steht.

Technisch gesehen wird bei einem „Hack“ eine Sicherheitslücke in einem Computersystem ausgenutzt, um sich Zugang zu diesem zu verschaffen. Ist der Angreifer einmal in das System eingedrungen, kann er sowohl Informationen auslesen als auch das System vollständig lahmlegen oder zerstören. Auf diese Weise würde auch Deutschland bei einem Gegenschlag vorgehen.

Ein solcher Gegenschlag kann im Einzelfall das „friedliche Zusammenleben der Völker“ stören. Aufgrund der Völkerrechtsfreundlichkeit des Grundgesetzes kann zur Auslegung des Merkmals auf das völkerrechtliche Gewaltverbot (u.a. Art. 2 Nr. 4 VN-Charta) verwiesen werden. Trotz mangelnder ausdrücklicher Vereinbarung ist es völkerrechtlich wohl weitgehend unbestritten, dass ein Verstoß gegen das Gewaltverbot durch einen Cyberangriff dann gegeben ist, wenn ein bewaffneter Angriff vorliegt und sich der Angriff physisch-kinetisch auswirkt, es also zu einem Sachschaden kommt (vgl. Tallinn Manual 2.0, Regel 71). Schwieriger ist Rechtslage bei Cyberangriffen unterhalb dieser Schwelle. Der Internationale Gerichtshof hat in seinem Nicaragua-Urteil [Nicaragua v. US, § 195] maßgeblich darauf abgestellt, ob Ausmaß und Wirkung („*scale and effect*“) des Angriffs einem bewaffneten Angriff nahekommen. Hierbei kommt es vor allem auf die Schwere („*severity*“) des Angriffs und seine Folgen an. Ein gezielter Hack eines (privaten) Computers eines (privaten) Angreifers einschließlich permanenter Verschlüsselung der Festplatte erreicht wohl selten das erforderliche Ausmaß.

Ein solches Vorgehen ist jedoch fern der Realität. Faktisch relevanter ist etwa die Unbrauchbarmachung eines gesamten Servers, der sich häufig in einem Drittstaat befindet. Zerstört Deutschland einen solchen Server ließe sich ein Angriff auf diesen Staat sehr wohl bejahen. Bliebe Deutschland unterhalb der genannten Schwelle, so könnte es sich hinsichtlich des involvierten Drittstaates auf die Rechtfertigung der Gegenmaßnahme (vgl. Art. 22 ASR) nur dann berufen, wenn dem Staat seinerseits ein Völkerrechtsbruch vorzuwerfen wäre, etwa die Verletzung seiner Pflicht zur *due diligence* (Tallinn Manual 2.0, Regel 6). Auch kann sich Deutschland wohl nur selten auf das Recht auf Selbstverteidigung (vgl. Art. 51 VN-Charta) berufen, da es hierfür eines bewaffneten Angriffes bedürfte, der regelmäßig physisch-kinetische Konsequenzen erfordert.

Insgesamt ist nach derzeitigem Verfassungsrecht ein „Zurückhacken“ in den allermeisten Fällen unzulässig. Dem Bericht ist insoweit zuzustimmen. Änderungen unserer Verfassung sind bereits in der Diskussion. Bei allem wird aber das in der Praxis höchst relevante Problem verkannt – die akkurate Feststellung des Urhebers. Aufgrund der dezentralen Struktur des Internets und aktueller Technik lässt sich der Pfad eines Angreifers äußerst effektiv verschleiern. Es bleibt daher abzuwarten wie sich die Bundesregierung weiter verhalten wird und ob sie tatsächlich zurückschlägt. Gelegenheiten wird sie sicherlich zur Genüge haben.

Verantwortung

Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, NA 02/33, Ruhr-Universität Bochum, 44780 Bochum, Tel.: +49 (0)234/32-27366, Fax: +49 (0)234/32-14208, Web: http://www.ruhr-uni-bochum.de/ifhv/. Die BOFAXE werden vom Deutschen Roten Kreuz unterstützt. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de.