Deutscher Bundestag **Drucksache 19/5472**

19. Wahlperiode 05.11.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/5076 –

Hackbacks als aktive digitale Gegenwehr

Vorbemerkung der Fragesteller

Die Debatte rund um die aktive Sicherung und Verteidigung digitaler Infrastrukturen im Cyberraum ist unter vielen Namen bekannt. Ob „digitaler Gegenangriff“, „digitaler Gegenschlag“, „aktive Cyberabwehr“, „finaler digitaler Rettungsschuss“ oder einfach nur „Hackback“. All diese Begriffe beschreiben die Suche nach Maßnahmen für die aktive, zivile und militärische Gegenwehr in einem Szenario eines Cyberangriffs auf deutsche Systeme (kritischer, staatlicher oder privater Natur). Der Terminus „Hackback“ soll in dieser Anfrage stellvertretend für alle verwendeten Termini in der Diskussion stehen.

Der Bundesminister des Innern, für Bau und Heimat Horst Seehofer wird in Medienberichten von August dieses Jahres mit den Worten zitiert, dass man in Bezug auf Cyberangriffe „nicht immer nur abwehren, sondern auch aktiv tätig werden“ müsse (u. a. www.sueddeutsche.de/digital/cyberkrieg-bundesregierung-1.4084810). Bereits 2017 äußerte sich der noch amtierende Verfassungsschutzpräsident Dr. Hans-Georg Maaßen Medienberichten zufolge mit folgenden Worten: „Wir halten es für notwendig, dass wir nicht nur rein defensiv tätig sind [...] Sondern wir müssen auch in der Lage sein, den Gegner anzugreifen, damit er aufhört, uns weiter zu attackieren“ (u. a. www.zeit.de/politik/deutschland/2017-01/cyberangriffe-verfassungsschutz-abwehrmassnahmen-gegenangriffe).

Die Wissenschaftlichen Dienste des Deutschen Bundestages haben in einer Ausarbeitung zum Thema Hackbacks auf ausländische Server (Ausarbeitung WD 3 - 3000 - 159/18) bereits festgestellt, dass die verfassungsrechtlichen Hürden für die Rechtfertigung von Hackbacks sehr hoch sind und nur durch eine Verfassungsänderung überhaupt erreicht werden könnten. Neben verschiedenen rechtlichen Fragen (völkerrechtlicher, verfassungsrechtlicher und sonstiger rechtlicher Natur) stellen sich auch grundsätzliche Kompetenzfragen. Welches Ressort, welche Behörde, welche Einheit ist zuständig für Hackbacks? Auch die Erweiterung von Kompetenzen oder die Schaffung neuer Zuständigkeiten wird debattiert.

Neben Kompetenzfragen und rechtlichen Erwägungen sind bei der Betrachtung von Cyberangriffen jedoch auch ganz praktische Fragen zu beachten, die wiederum für die rechtliche Bewertung von weitreichender Bedeutung sind. Etwa

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 1. November 2018 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

das Problem der Attribution oder auch die Betrachtung der Folgen von Gegenmaßnahmen. Die Erkennung eines geheimen Cyberangriffs an sich dauert im Schnitt schon etwa 150 bis 200 Tage. Wenn sich niemand zu der Attacke bekennt, bedarf es weiterer Zeit, um herauszufinden, woher die Attacke kam. Auch nachdem die Herkunft einer Attacke bekannt ist, ist die Attribution erst dann abgeschlossen, wenn klar ist, wer für den Cyberangriff verantwortlich war. Ähnliche Ausführungen ließen sich zu anderen praktischen Bereichen anführen.

Hackbacks waren teilweise bereits Gegenstand vergangener Kleiner Anfragen (z. B. Bundestagsdrucksachen 19/2009 und 19/2032). Wenn sich einzelne Fragen mit den in dieser Anfrage erfragten Informationen überschneiden, wird die Bundesregierung darum gebeten, explizit Fortschritte und neue Erkenntnisse im Rahmen der Prüfung von rechtlichen und technischen Möglichkeiten seit den Antworten (z. B. Bundestagsdrucksachen 19/2307 und 19/2645) auf die jeweiligen Fragen darzustellen.

Die Debatte um Hackbacks wirft insgesamt vielfältige rechtliche, technische, politische und ethische Probleme auf. Noch vor der Entscheidung, ob rechtliche Grundlagen geschaffen und technische Kapazitäten aufgebaut werden sollen, bedarf es demnach der Beantwortung einiger Fragen.

Vorbemerkung der Bundesregierung:

Der von den Fragestellern verwendete Begriff „Hackback“ wird von der Bundesregierung konzeptionell grundsätzlich nicht verwendet, weder für Aktivitäten der Cyber-Abwehr noch der Cyber-Verteidigung. Der Beantwortung dieser Kleinen Anfrage legt die Bundesregierung die Begrifflichkeiten aus der Vorbemerkung der Bundesregierung zur Antwort auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 zugrunde. Im Kontext der Vorbemerkung der Fragesteller wird deren Fragestellung von der Bundesregierung so verstanden, dass sie in Ergänzung zur aktiven Cyber-Abwehr auch die Aspekte der Cyber-Verteidigung zum Wirken im Cyberraum für den Bereich der äußeren Sicherheit erfasst.

1. Welche rechtlichen Grundlagen hält die Bundesregierung bei der völkerrechtlichen, verfassungsrechtlichen und sonstigen rechtlichen Bewertung von Hackbacks für relevant?

2. Welche völkerrechtlichen, verfassungsrechtlichen oder sonstigen rechtlichen Vorschriften müssten nach Einschätzung der Bundesregierung geändert oder geschaffen werden, um Hackbacks zu ermöglichen?

3. Wären aus Sicht der Bundesregierung Hackbacks bei der Anwendung der bestehenden Rechtsgrundlagen auch heute schon möglich?

   Wenn ja, unter welchen Voraussetzungen?

Wegen des Sachzusammenhangs werden die Fragen 1 bis 3 gemeinsam beantwortet.

Aufgrund der Vielzahl der vorstellbaren Maßnahmen der aktiven Cyber-Abwehr werden vielfältige völker-, verfassungs- und einfachrechtliche Fragestellungen aufgeworfen. Zudem sind unterschiedlichste Fallgestaltungen im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr denkbar. Eine pauschalierende Betrachtungsweise ist daher nur eingeschränkt möglich. Bei jeder Betrachtung gilt jedoch, dass sich alle Maßnahmen der aktiven Cyber-Abwehr im Rahmen des geltenden Völker-, Verfassungs- und des einfachen Rechts bewegen müssen.

Die im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen u. a. rechtlichen Fragestellungen werden derzeit von der Bundesregierung geprüft. Aus dieser Prüfung kann sich unter anderem auch gesetzgeberischer Handlungsbedarf ableiten. Diese Prüfungen sind noch nicht abgeschlossen.

Militärische Maßnahmen im Cyber-Raum unterliegen dem gleichen rechtlichen Rahmen wie andere militärische Maßnahmen auch und können entsprechend durchgeführt werden. Nach dem Parlamentsbeteiligungsgesetz unterliegen bewaffnete Einsätze der Streitkräfte außerhalb des Geltungsbereichs des Grundgesetzes grundsätzlich der vorherigen konstitutiven Zustimmung des Deutschen Bundestages.

Ergänzend wird auf die Antwort der Bundesregierung zu Frage 20 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2307 verwiesen.

4. Beabsichtigt die Bundesregierung, die Zuständigkeit für die Abwehr von Cyberangriffen grundsätzlich oder für einzelne Fälle auf die Bundesebene zu verlagern?

   Wenn nein, warum nicht?

In der Cyber-Sicherheitsstrategie für Deutschland 2016 wird die Cyber-Sicherheit als eine permanente gesamtstaatliche Aufgabe beschrieben, die gemeinsam zu bewältigen ist. Dabei kommt der föderalen, ressort- und behördenübergreifenden Zusammenarbeit eine besondere Bedeutung zu. Ob für die Abwehr von Cyber-Angriffen in einzelnen Bereichen eine Zuständigkeitsverlagerung von den Ländern auf den Bund angezeigt sein kann, wird von der Bundesregierung derzeit geprüft.

5. Beabsichtigt die Bundesregierung im Hinblick auf Cyberangriffe, die Befugnisse und Zuständigkeiten zum Schutz ziviler Infrastrukturen zu erweitern?

   Wenn ja, inwiefern und an welcher Stelle?

Der strategische, rechtliche und institutionelle Rahmen der Cyber-Sicherheit in Deutschland wird fortlaufend geprüft und weiterentwickelt um die mit der hohen Dynamik der Digitalisierung einhergehenden Herausforderungen zu bestehen.

Derzeit prüft die Bundesregierung vielfältige u. a. rechtliche Fragen im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr. Diese Prüfungen sind noch nicht abgeschlossen.

6. Welche Fragen und Annahmen leiten die Bundesregierung bei der technischen, ethischen und politischen Bewertung von Hackbacks?

Für die Bundesregierung ist Cyber-Sicherheit der anzustrebende Zustand der IT-Sicherheitslage, in dem Risiken, die Deutschland aus dem Cyber-Raum erwachsen auf ein tragbares Maß reduziert sind.

Das bedeutet, die Bundesregierung betrachtet das Thema Cyber-Sicherheit ganzheitlich – eingebettet in das Thema der Gewährleistung der allgemeinen öffentlichen Sicherheit. Den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezügen zur Cyber-Sicherheit bildet die Cyber-Sicherheitsstrategie für Deutschland 2016, die die Cyber-Sicherheitsstrategie aus dem Jahr 2011 fortschreibt.

7. Welche Bundesministerien beschäftigen sich derzeit mit der Entwicklung eines Konzepts und konkreten gesetzgeberischen Maßnahmen zum Thema Hackback?

   Welche Abteilung ist jeweils für die Entwicklung zuständig?

Das Bundesministerium des Innern, für Bau und Heimat (BMI) befasst sich innerhalb der Bundesregierung federführend mit Fragestellungen der Cyber-Abwehr einschließlich IT-Sicherheit, die hauptsächlich in den Abteilungen Cyber- und Informationssicherheit (CI), Öffentliche Sicherheit (ÖS) sowie Bundespolizei (B) bearbeitet werden. Hierunter fallen auch Aufgaben im Sinne der Fragestellung.

Anlassbezogen stimmt sich das BMI unter anderem mit dem Bundeskanzleramt, dem Auswärtigen Amt (AA), dem Bundesministerium der Verteidigung (BMVg) sowie dem Bundesministerium der Justiz und für Verbraucherschutz (BMJV) ab. Dies erfolgt auch im Hinblick auf Fragestellungen zur aktiven Cyber-Abwehr.

Für den Geschäftsbereich des BMVg werden die politischen Vorgaben der Grundsätze für die Cyber-Verteidigung in der strategischen Leitlinie Cyber-Verteidigung festgelegt (Federführende Abteilung Cyber/IT BMVg). Für militärische Maßnahmen im Cyber-Raum gilt der rechtliche Rahmen für den Einsatz von Streitkräften. Ergänzende gesetzgeberische Maßnahmen sind aus Sicht der Bundesregierung nicht erforderlich.

8. Auf welcher Grundlage beschäftigt sich das Bundesministerium des Innern, für Bau und Heimat mit dem Thema Hackback?

Das BMI ist zuständig für die Aufgaben der Cyber- und IT-Sicherheit und der öffentlichen Sicherheit. Auf diesen Grundlagen befasst es sich mit dem Thema der aktiven Cyber-Abwehr.

9. Welches Bundesministerium und welche Behörde unterhalb des jeweiligen Bundesministeriums sind für den Aufbau technischer Kapazitäten für Hackbacks momentan zuständig?

Auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion der FDP auf Bundestagdrucksache 19/2645 wird verwiesen.

Für die Fähigkeitsentwicklung der Cyber-Verteidigung sind das BMVg und das Kommando Cyber- und Informationsraum zuständig.

10. Wäre aus Sicht der Bundesregierung eine ausreichende technische Ausstattung und Expertise zur Durchführung von Hackbacks bereits zum jetzigen Zeitpunkt gegeben?

    Welche Behörde oder Institution wäre aus Sicht der Bundesregierung hierzu bereits zum jetzigen Zeitpunkt technisch in der Lage?

Die Bundesregierung prüft derzeit unter anderem die rechtlichen, organisatorischen und technischen Rahmenbedingungen von Maßnahmen der aktiven Cyber-Abwehr. Diese Prüfungen sind noch nicht abgeschlossen.

Die Bundeswehr besitzt die technische Ausstattung und Expertise zum Wirken im Cyber-Raum im Rahmen der Cyber-Verteidigung.

11. Welche der in Frage kommenden Behörden oder Institutionen (namentlich BND – Bundesnachrichtendienst, BfV – Bundesamt für Verfassungsschutz, BKA – Bundeskriminalamt, BSI – Bundesamt für Sicherheit in der Informationstechnik, Zitis – Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Bundeswehr) wäre bei Bestehen der notwendigen Rechtsgrundlagen nach Ansicht der Bundesregierung für die Durchführung von Hackbacks zuständig?

    Welche weiteren Behörden oder Institutionen kommen für die Bundesregierung in Betracht?

Für den Einsatz von Maßnahmen der aktiven Cyber-Abwehr sind besondere Fachkenntnisse erforderlich. Daher prüft die Bundesregierung neben den rechtlichen Fragen im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr u. a. auch technische und organisatorische Fragen. Diese Prüfungen sind noch nicht abgeschlossen.

Die Bundeswehr ist im Rahmen der Cyber-Verteidigung für militärische Maßnahmen im Cyber-Raum zuständig. Für militärische Maßnahmen im Cyber-Raum gilt der rechtliche Rahmen für den Einsatz von Streitkräften.

12. Wie beurteilt die Bundesregierung beim Thema Hackback das Trennungsgebot zwischen polizeilicher und geheimdienstlicher Tätigkeit?

    Wie wird dies von der Bundesregierung konkret berücksichtigt?

Die Frage, ob und wie Polizeien und Nachrichtendienste bei der Aktiven Cyber-Abwehr zusammenwirken können, ist Gegenstand der Prüfung der Bundesregierung. Sie ist noch nicht abgeschlossen.

13. Welche der folgenden Ziele verfolgt die Bundesregierung mit dem Aufbau rechtlicher Grundlagen und technischer Kapazitäten für Hackbacks als Gegenmaßnahme zu Cyberangriffen (und warum):

    a) Prävention von Angriffen

    b) Schutz von Systemen

    c) Aufklärung von Cyberangriffen

    d) Übernahme und Infiltration der Angreifer-Infrastruktur

    e) Sonstige Reaktion auf Cyberangriffe (z. B. Rückerlangung von Informationen, Zerstörung von Angreifer-Infrastrukturen)?

    Welche darüberhinausgehenden Ziele verfolgt die Bundesregierung, und warum?

Die Bundesregierung verfolgt das Ziel einer ganzheitlichen Gewährleistung von Cyber-Sicherheit – eingebettet in den Rahmen der Sicherstellung der allgemeinen öffentlichen Sicherheit.

Die Bundesregierung prüft derzeit noch unter anderem die technischen Möglichkeiten und den damit einhergehenden Umfang bspw. zur Prävention, Aufklärung und Reaktion im Rahmen einer aktiven Cyber-Abwehr.

14. Für welche konkreten Szenarien eines Cyberangriffs werden in der Bundesregierung Gegenmaßnahmen diskutiert:

a) Angriff auf staatliche Systeme und Infrastrukturen

b) Angriff auf kritische Infrastrukturen

c) Angriff auf sonstige private Systeme und Infrastrukturen

d) Angriff unter Verwendung ausländischer Server oder Systeme

e) Geheime Angriffe beziehungsweise angekündigte Angriffe?

Die Bunderegierung bezieht in die Prüfung u. a. rechtlicher Fragestellungen eine Vielzahl von Szenarien ein, die u. a. die in der Fragestellung genannten Szenarien einschließen. Die Prüfungen sind noch nicht abgeschlossen.

15. Welche Maßnahmen werden für die unterschiedlichen Stadien beziehungsweise Zeitpunkte eines Cyberangriffs in der Bundesregierung konkret diskutiert

a) im Vorfeld eines Cyberangriffs,

b) während eines Cyberangriffs bzw.

c) nach dem Abschluss eines Cyberangriffs?

Die Bundesregierung prüft eine Vielzahl unterschiedlichster Maßnahmen als mögliche Reaktion auf beispielsweise bevorstehende, laufende und abgeschlossene Cyber-Angriffe. Diese Prüfungen sind noch nicht abgeschlossen.

16. Welche Alternativen zu Hackbacks zieht die Bundesregierung in Bezug auf die konkreten Szenarien und Stadien bzw. Zeitpunkte eines Cyberangriffs (s. Fragen 14 und 15) in Betracht?

Eine Entscheidung, welche Maßnahmen als Reaktion auf einen Cyber-Angriff rechtlich zulässig und in der Sache zielführend sind, hängt von einer Vielzahl von Faktoren des Einzelfalles ab und kann somit nicht pauschal beantwortet werden. Grundsätzlich liegt der Schwerpunkt auf präventiven Maßnahmen der IT-Sicherheit. Darüber hinaus setzt sich die Bundesregierung unter anderem im Rahmen ihrer Cyber-Außen- und Sicherheitspolitik dafür ein, dass Staaten sich regelkonform und vertrauensbildend im Cyber-Raum bewegen. Auch während und nach Cyber-Angriffen sind unter anderem Maßnahmen der Cyber-Außen- und Sicherheitspolitik als mögliche Handlungsoptionen zu erwägen.

Ein Cyber-Angriff kann unter bestimmten Bedingungen einen bewaffneten Angriff im Sinne von Artikel 51 der VN-Charta darstellen. In diesem Fall steht der Bundesrepublik Deutschland das Recht auf Selbstverteidigung zu und sie könnte auf diesen bewaffneten Angriff mit allen zulässigen militärischen Mitteln reagieren.

17. Für wie wirkungsvoll hält die Bundesregierung passive Verteidigungs- und Sicherungsmaßnahmen, etwa die Stärkung der IT-Sicherheit?

    Welche defensiven Möglichkeiten der Cyberabwehr und der Cyberresilienz hält die Bundesregierung für wirksam?

Für die Bundesregierung sind präventive Maßnahmen u. a. der passiven IT-Sicherheit ein zentraler, essentieller und wirksamer Baustein eines ganzheitlichen Cyber-Sicherheits-Ansatzes.

Noch in dieser Legislaturperiode wird dieser Weg mit einem IT-Sicherheitsgesetz 2.0 fortgeschrieben.

18. Wie beurteilt die Bundesregierung das Problem der Attribution eines Angriffs in Bezug auf die konkreten Szenarien und Stadien bzw. Zeitpunkte eines Cyberangriffs?

    Wie beurteilt die Bundesregierung das Problem der Attribution in Bezug auf das völkerrechtliche Recht auf Selbstverteidigung?

    Wie schätzt die Bundesregierung generell die Möglichkeit einer zeitnahen Attribution von Angriffen ein?

    Wie soll nach Ansicht der Bundesregierung mit Zweifelsfällen umgegangen werden?

Die Bundesregierung prüft derzeit u. a. die rechtlichen und technischen Möglichkeiten von Maßnahmen der aktiven Cyber-Abwehr. Fragestellungen der Zurechnung (Attribution) werden in diesem Kontext auch beleuchtet. Die genannten Prüfungen sind noch nicht abgeschlossen.

Im Rahmen der Cyber-Verteidigung müssen sich alle Maßnahmen grundsätzlich gegen denjenigen Staat richten, dem der Angriff in Form einer Cyberoperation zugerechnet werden kann. Die Zurechnung erfolgt im Rahmen einer Gesamtwürdigung der Gegebenheiten des konkreten Einzelfalls.

19. Wie beurteilt die Bundesregierung die Möglichkeit von Hackbacks für den Fall, dass die Angreifer

    a) Server von Unbeteiligten für ihren Angriff verwenden,

    b) Kritische Infrastrukturen für ihren Angriff verwenden bzw.

    c) Szenario a) oder b) aus dem Ausland heraus oder mithilfe ausländischer Infrastruktur durchführen?

Auf die Antwort zu den Fragen 14 und 15 wird verwiesen.

20. Welche Rolle spielen bei den Überlegungen der Bundesregierung zu Hackbacks auf ausländischem Territorium Mittel der internationalen Amtshilfe bzw. Zusammenarbeit oder Rechtshilfeersuchen?

Die genannten Mittel werden in die Prüfungen der Bundesregierung mit einbezogen. Diese Prüfungen sind noch nicht abgeschlossen.

21. Wie soll die Nutzung von Hackbacks international bilateral oder multilateral abgestimmt werden?

    Bei welcher Gelegenheit gedenkt die Bundesregierung, eine solche Abstimmung voranzutreiben?

Entscheidungen über eventuelle bilaterale oder multilaterale Abstimmungen können solange nicht getroffen werden, wie die Prüfung der Grundsatzfragen noch nicht abgeschlossen ist. Auf die Antwort zu Frage 10 wird verwiesen.

22. Wie schätzt die Bundesregierung die Wahrscheinlichkeit ein, dass Gegenangriffe auf im Ausland stehende Server oder Infrastrukturen als militärischer Angriff angesehen werden?

    Wie schätzt die Bundesregierung in diesem Zusammenhang die Möglichkeit der Eskalation von Cyberabwehrangriffen ein?

Eine Beantwortung dieser Frage wäre spekulativer Art und erfolgt aus diesem Grunde nicht. Eine fundierte Einschätzung ist nur im jeweiligen Einzelfall möglich und hängt von einer Vielzahl von Faktoren ab.

23. Plant die Bundesregierung die Einführung von Verpflichtungen für nichtstaatliche Akteure, bei der Abwehr von Cyberangriffen mit den durchführenden Sicherheitsbehörden zu kooperieren?

    Was sollen solche Kooperationsverpflichtungen umfassen?

Auf die Antwort zu Frage 5 wird verwiesen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333