Bundesministerium
des Innern

Bundesministerium des Innern, 11014 Berlin

Herrn
Arne Semsrott
Open Knowledge Foundation Deutschland e.V.
c/o Open Knowledge Foundation Deutschland e.V.
Singerstraße 109
10179 Berlin

Per E-Mail: arne.semsrott@okfn.de

HAUSANSCHRIFT
Alt-Moabit 140
10557 Berlin

POSTANSCHRIFT
11014 Berlin

TEL +49 30 18 681-11519
FAX +49 30 18 681-55038

IFG@bmi.bund.de
www.bmi.bund.de

Betreff: Informationsfreiheitsgesetz
hier: Gutachten und Vermerke zum Thema „Hack Back“
[#25481]

Bezug: Ihr Antrag vom 28. November 2017
Aktenzeichen: ZI4-13002/4#1466
Berlin, 21. Dezember 2017

Sehr geehrter Herr Semsrott,

Sie haben mit E-Mail vom 27. November 2017 um Zusendung folgender Unterlagen gebeten: *„Sämtliche Gutachten und Vermerke des BMI aus den Jahren 2016 und 2017, die die Legalität von Gegenangriffen nach einem Internetangriff (sog. Hack Backs") thematisieren.“*

Ihrem Antrag wird im Rahmen der Ausführungen zu (1.) teilweise stattgegeben. Im Übrigen wird der Antrag abgelehnt (2.).

Begründung:

1.)
Auf Ihre Anfrage können folgende Auskünfte gegeben werden:

Mit der „Cyber-Sicherheitsstrategie für Deutschland 2016“ hat die Bundesregierung strategische Ziele und Maßnahmen formuliert, um in den Feldern der Prävention,

Detektion und Reaktion Verbesserungen zum Schutz vor Cyber-Angriffen herbeizuführen. Dies betrifft in vier Handlungsfeldern die Bürgerinnen und Bürger ebenso wie den Staat, die Wirtschaft oder zum Beispiel auch die internationale Ebene.

Prävention und Schutz von IT-Systemen sind wichtig - helfen womöglich aber nicht in jeder denkbaren Fallkonstellation. Deswegen hat die Bundesregierung formuliert (Cyber-Sicherheitsstrategie für Deutschland 2016, S. 29): „*Darüber hinaus sind schwerwiegende Cyber-Angriffe vorstellbar, gegen die mit den klassischen präventiven Maßnahmen in der notwendigen Zeit nicht nachhaltig vorgegangen werden kann. Die Bundesregierung wird daher prüfen, unter welchen rechtlichen Rahmenbedingungen und mit welchen technischen Möglichkeiten in diesen Fällen durch staatliche Stellen Netzwerkoperationen durchgeführt werden könnten.*“ Anlass für diese Bewertung im Jahre 2016 war die Cyber-Bedrohungslage.

Die Aufbereitung der rechtlichen und technischen Rahmenbedingungen für Netzwerkoperationen wurde in der Bundesregierung bisher noch nicht abgeschlossen. Insbesondere wurde die Frage, ob und gegebenenfalls welche Behörde(n) entsprechende Zuständigkeiten und Befugnisse für eine aktive Cyber-Abwehr übernehmen könnte(n), noch nicht durch die Bundesregierung entschieden und die rechtlichen Rahmenbedingungen noch nicht abschließend geklärt.

Weitere Informationen zur Cyber-Sicherheitsstrategie 2016 und zur aktuellen Cyber-Bedrohungslage finden Sie unter:

- www.bmi.bund.de/cybersicherheitsstrategie/
- www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

Informationen zu Regulierungsvorschlägen auf EU-Ebene im Bereich Cyber-Sicherheit finden Sie unter:

- www.ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_de

2.)
Der Anspruch auf Informationszugang besteht nicht, wenn das Bekanntwerden der Information nachteilige Auswirkungen haben kann auf militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr (§ 3 Nr. 1 lit. b IFG) oder Belange der inneren oder äußeren Sicherheit (§ 3 Nr. 1 lit. c IFG), ferner wenn und solange die Beratungen von Behörden beeinträchtigt werden (§ 3 Nr. 3 lit. b IFG) oder wenn die Information einer durch Rechtsvorschrift oder durch die Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen geregelten Geheimhaltungs- oder Vertraulichkeitspflicht oder einem Berufs- oder besonderen Amtsgeheimnis unterliegt (§ 3 Nr. 4 IFG). Zudem besteht zu den Nachrichtendiensten eine Bereichsausnahme gemäß § 3 Nr. 8 IFG.

Die Voraussetzungen der vorgenannten Vorschriften sind in Bezug auf Unterlagen, von denen angenommen wird, dass Ihr Antrag darauf abzielt, erfüllt.

Ein Bekanntwerden von Unterlagen, die sich in rechtlicher Betrachtung mit den zivilen oder militärischen Cyber-Fähigkeiten Deutschlands auseinandersetzen, hätte Nachteile auf Belange der inneren Sicherheit und militärische Belange. Zudem sind die Beratungen der Behörden bzw. der Ressorts der Bundesregierung zu den Rechtsfragen einer aktiven Cyber-Abwehr noch nicht abgeschlossen; ein Bekanntwerden der Zwischenstände würde die Beratungen beeinträchtigen (§ 3 Nr. 3 lit. b IFG). Soweit bisher Teilergebnisse der laufenden rechtlichen Prüfungen in Form von Unterlagen niedergelegt wurden, sind diese, insbesondere, soweit sie sich auch mit Cyber-Fähigkeiten der Bundesverwaltung befassen, nach der Verschlusssachenanweisung des Bundes – VSA – mit verschiedenen Geheimhaltungsgraden eingestuft (§ 3 Nr. 4 IFG), die kein öffentliches Bekanntwerden zulassen.

Rechtsbehelfsbelehrung:
Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch beim Bundesministerium des Innern (BMI) erhoben werden. Dafür stehen folgende Möglichkeiten zur Verfügung:

1. Der Widerspruch kann schriftlich oder zur Niederschrift erhoben werden. Die Adresse lautet: Bundesministerium des Innern, Alt-Moabit 140, 10557 Berlin.
2. Der Widerspruch kann auch auf elektronischem Wege erhoben werden. Dafür stehen folgende Möglichkeiten zur Verfügung:

- Der Widerspruch kann durch E-Mail mit qualifizierter elektronischer Signatur nach dem Signaturgesetz erhoben werden. Die E-Mail-Adresse lautet: Poststelle@bmi.bund.de
- Der Widerspruch kann auch durch De-Mail in der Sendevariante mit bestätigter sicherer Anmeldung nach dem De-Mail-Gesetz erhoben werden. Die De-Mail-Adresse lautet: Poststelle@bmi-bund.de-mail.de

Mit freundlichen Grüßen
[redacted]