Stiftung Neue Verantwortung

Aktive Cyberabwehr/ Hackback in Deutschland

– Leseliste 2017-2020 –

Version 3.0 | Stand: 06.03.2020

Kuratiert von Sven Herpig et al. (AC/BC)

1. Hintergrundinformationen

Autor:innen:	**Jörg Diehl, SPIEGEL und Fabian Reinbold, SPIEGEL**
Titel (Jahr):	Wenn der Staat zum Hacker wird (2017)
Beschreibung:	Übersichtsartikel mit Stimmen aus der Bundesregierung.
Link:	https://www.spiegel.de/netzwelt/netzpolitik/hackback-wenn-der-staat-zum-hacker-werden-will-a-1179423.html

Autor:innen:	**Hakan Tanriverdi, Bayerischer Rundfunk**
Titel (Jahr):	Bundesregierung skizziert Hackback-Pläne (2019)
Beschreibung:	BR Recherche zu einem internen Konzeptpapier der Bundesregierung zu Aktiver Cyberabwehr mit Erläuterung des „Vier-Stufen-Plans“, institutioneller Verordnung und verfassungsrechtlicher Einschätzung.
Link:	https://www.br.de/nachrichten/deutschland-welt/internes-papier-bundesregierung-skizziert-hackback-plaene,RRqyr1j

Autor:innen:	**Dr. Sven Herpig, Stiftung Neue Verantwortung e. V.**
Titel (Jahr):	Hackback ist nicht gleich Hackback (2018)
Beschreibung:	Definition von Hackback/ Aktiver Cyberabwehr, sowie Beschreibung und Kategorisierung von technischen Maßnahmen, die unter diese Definition fallen.
Link:	https://www.stiftung-nv.de/de/publikation/hackback-ist-nicht-gleich-hackback

2. Analysen und Perspektiven von Sachverständigen aus Politik und Recht

Autor:innen:	**Thomas Reinhold, TU Darmstadt und Dr. Matthias Schulze, Stiftung Wissenschaft und Politik**
Titel (Jahr):	Digitale Gegenangriffe - Eine Analyse der technischen und politischen Implikationen von „hack backs“ (2017)
Beschreibung:	Die Analyse präsentiert die gängigsten Argumente für und gegen Hackbacks. Die Autoren sind skeptisch, ob Hackbacks als Datenrettungsmission, zur Beweissicherung, zur Cyber-Hygiene bzw. als Ultima Ratio sinnvoll sind. Stattdessen wirken die Gegenargumente wie die Schwierigkeit der Feststellung der Urheberschaft, die Risiken politischer Eskalation, die unsichere Wirkungsfähigkeit des Mittels, die damit verbundenen Anschaffungskosten und die außenpolitische Signalwirkung schwerer. Hackbacks sind nur unter sehr begrenzten Umständen ein brauchbares Mittel der Außenpolitik.
Link:	https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf

Autor:innen:	**Dr. Sven Herpig, Stiftung Neue Verantwortung e. V.**
Titel (Jahr):	Aktive Cyber-Abwehr: Innenminister schaltet bei IT-Sicherheit schrittweise von Verteidigung auf Angriff (2019)
Beschreibung:	Analyse welche Maßnahmen von Aktiver Cyberabwehr/ Hackback in den Entwürfen vom IT-Sicherheitsgesetz 2.0 und der Harmonisierung des Verfassungsschutzgesetzes vorgesehen sind.
Link:	https://netzpolitik.org/2019/aktive-cyber-abwehr-innenminister-schaltet-bei-it-sicherheit-schrittweise-von-verteidigung-auf-angriff/

Autor:innen:	**Martin Schallbruch und Isabel Skierka, European School of Management and Technology Berlin**
Titel (Jahr):	Cybersecurity in Germany (2018)
Beschreibung:	Es handelt sich hierbei um eine Analyse der deutschen Cybersicherheitspolitik, ihre Evolution und aktuelle Prioritäten und Versäumnisse in englischer Sprache. Dabei spielt auch Aktive Cyberabwehr eine Rolle.
Link:	http://static.esmt.org/publications/other/2018-msch-cybersecurity-in-germany-manuscript.pdf

Autor:innen:	**Dr. Matthias Schulze, Stiftung Wissenschaft und Politik**
Titel (Jahr):	Überschätzte Cyber-Abschreckung (2019)
Beschreibung:	Der Text analysiert, ob aktive Cyberverteidigung abschreckende Effekte haben kann, ob die Angriffsmotivation eines Gegners sich verändert, wenn ihm Gegenangriffe drohen. Die Analyse zeigt, dass Abschreckungseffekte durch Cybermittel nur sehr schwer herstellbar sind, und das es zahlreiche Möglichkeiten des Abschreckungsversagens gibt.
Link:	https://www.swp-berlin.org/publikation/ueberschaetzte-cyber-abschreckung/

Autor:innen:	**Thomas Reinhold, TU Darmstadt**
Titel (Jahr):	Rechtlich-organisatorischer Rahmen militärischer Cyber-Operationen (2019)
Beschreibung:	Analyse der Pespektive der Bundesregierung, basierend auf einer kleinen Anfrage. Die Auswertung umfasst dabei die militärische Planungen zum Aufklären und Wirken im Cyberspace (Hackback) sowie internationale Kooperationen von Ministerien zu Cybersicherheit im Allgemeinen und Cyberrüstungskontrolle im Besonderen.
Link:	https://cyber-peace.org/analyse_antwort_bundesregierung_zu_offensiven_cyberoperationen/

Autor:innen:	**Dr. Matthias Schulze, percepticon Podcast und Dr. Sven Herpig, Stiftung Neue Verantwortung e. V.**
Titel (Jahr):	05 /invite Sven Herpig – aktive Cyber-Abwehr, Hackback und Deutschlands Cyber-Sicherheitsarchitektur (2019) [Podcast]
Beschreibung:	Diskussion über Aktive Cyberabwehr und dessen Voraussetzungen. Einbettung in den staatlichen Umgang mit Schwachstellen, strategische Implikationen und die Rolle der Privatwirtschaft.
Link:	https://percepticon.de/2019/07/05-invivite-sven-herpig-hackback/

Autor:innen:	**Dr. Matthias Schulze, percepticon Podcast**
Titel (Jahr):	13 /Hack back oder aktive Cyber-Abwehr einmal durchdacht (2020) [Podcast]
Beschreibung:	Der Podcaster führt verschiedene Gedankenstränge zu Aktiver Cyberabwehr zusammen und diskutiert aus mehreren Perspektiven, inklusive Abschreckungtheorie und mögliche Eskalationsspiralen.
Link:	https://percepticon.de/2020/03/13-hack-back-oder-aktive-cyber-abwehr-einmal-durchdacht/

Autor:innen:	**Dr. Matthias Schulze, Stiftung Wissenschaft und Politik**
Titel (Jahr):	Von Glashäusern und Steinewerfen (2020) [Podcast]
Beschreibung:	Neben der Frage der Effektivität, stellen sich laut des Vortragenden strategische, politische und rechtliche Fragen, bevor ein Gegenangriff initialisiert wird. Der Talk wirft die Fragen auf, die sich politische Entscheidungsträger stellen sollten, bevor sie (vorschnell) zum Mittel des Hackbacks greifen.
Link:	https://www.youtube.com/watch?v=Z1qQieYd7SY

Autor:innen:	**Dr. Matthias Schulze, Stiftung Wissenschaft und Politik**
Titel (Jahr):	Where Does Cyber Defense Stop and Offense Begin? (2018)
Beschreibung:	Der Text in englischer Sprache beschäftigt sich mit der Grauzone zwischen aktiver und passiver Verteidigung. Er entwickelt eine Typologie zur Beurteilung passiver und aktiver Gegenmaßnahmen nach Cyberangriffen. Er argumentiert, dass eine bloße perimeterbasierte Einteilung (eigenes vs. fremdes Netzwerk) bei zahlreichen Technologien wie Beacons nicht zielführend sind. Zur Beurteilung von passiven und aktiven Maßnahmen sind neben dem Ort des Effekts, auch die Intention, der Modus Operandi, die potenziellen Effekte eines Hacks, als auch der Interaktionskontext zwischen Angreifer und Verteidiger beachtet werden.
Link:	https://www.aicgs.org/site/wp-content/uploads/2018/08/PR68-HSS-Cybersecurity-FY19.pdf

Autor:innen:	**Dr. Sven Herpig, Stiftung Neue Verantwortung e. V., Robert Morgus, New America und Dr. Amit Sheniak, Hebrew University of Jerusalem**
Titel (Jahr):	Active Cyber Defense - A comparative study on US, Israeli and German approaches (2020)
Beschreibung:	Der Text analysiert in englischer Sprache die verschiedenen Stufen von aktiver Cyberabwehr von "Defense with a Twist" über "Hacking Backing" bis zu "Persistent Engagement" und "Defending Forward". In gebotener Kürze ordnet er dann komparativ die aktuellen Modelle der Vereinigsten Staaten, Israels und Deutschland ein und stellt sie gegenüber.
Link:	https://www.kas.de/documents/263458/263507/Active+Cyber+Defense-+A+comparative+study+on+US%2C+Israeli+and+German+approaches.pdf/30f8f8b2-5227-1ef1-8abe-8de53b734736?version=1.0&t=1583325334639

Autor:innen:	**Wissenschaftliche Dienste, Deutscher Bundestag**
Titel (Jahr):	Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland (2018)
Beschreibung:	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.
Link:	https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf

Autor:innen:	**Dr. Dennis-Kenji Kipker, Verfassungsblog**
Titel (Jahr):	Hackback in Deutschland: Wer, was, wie und warum? (2020)
Beschreibung:	Der Text analysiert vornehmlich die Frage welche Behörden auf welcher verfassungsrechtlichen Grundlage für die Durchführung von Hackbacks in Frage kommen könnten.
Link:	https://verfassungsblog.de/hackback-in-deutschland-wer-was-wie-und-warum/ - umfassendere Version in der Zeitschrift für das Gesamte Sicherheitsrecht (GSZ) 2020, 26

Autor:innen:	**Dr. Dennis-Kenji Kipker, Verfassungsblog**
Titel (Jahr):	Hackback in Deutschland: Wer, was, wie und warum? (2020) [Video]
Beschreibung:	In dieser Präsentation widmet sich der Vortragende den Fragestellungen: Warum wird der Hackback aktuell politisch überhaupt diskutiert? Wer könnte einen Hackback durchführen? Und wer darf das rechtlich überhaupt?
Link:	https://www.youtube.com/watch?v=WTV3MIn_9NA

Autor:innen:	**Wissenschaftliche Dienste, Deutscher Bundestag**
Titel (Jahr):	Völkerrechtliche Aspekte der Zulässigkeit geheimdienstlicher Aktivitäten (2019)
Beschreibung:	Der Text beschäftigt sich zwar allgemeiner mit den völkerrechtlichen Aspekten der Zulässigkeit geheimdienstlicher Aktivitäten ist aber dann relevant, wenn die Aktive Cyberabwehr/ Hackback nicht von Strafverfolgungsbehörden, sondern von Nachrichtendiensten durchgeführt werden soll.
Link:	https://www.bundestag.de/resource/blob/662186/597c52614beaa29b64f6dec6cdb0b305/WD-2-094-19-pdf-data.pdf

Autor:innen:	**Janine Schmoldt, Universität Erfurt**
Titel (Jahr):	Hacking Back aus völkerrechtlicher Perspektive (2020) [Video]
Beschreibung:	Ein Vortrag, der die völkerrechtlichen Prinzipien auf den Cyberraum überträgt und auf den Fall von Aktiver Cyberabwehr anwendet.
Link:	https://www.youtube.com/watch?v=dYMTO-Mjhzk

Autor:innen:	**Dr. Sven Herpig, Stiftung Neue Verantwortung**
Titel (Jahr):	Strategieunfähig: Deutschland braucht eine Resilienzstrategie (2020) [Video]
Beschreibung:	In dieser Präsentation analysiert der Vortragende die aktuelle deutsche Cybersicherheitspolitik und stellt heraus welche dringenden Herausforderungen beantwortet werden müssen und warum Aktive Cyberabwehr dazu vermutlich keinen Beitrag leisten können wird.
Link:	https://www.youtube.com/watch?v=qTRmKHoRSZo

Autor:innen:	**Ann Cathrin Riedel, LOAD e.V.**
Titel (Jahr):	Warum Angriff nicht die beste Verteidigung ist (2020) [Video]
Beschreibung:	Die Vortragende stellt in ihrem Vortrag dar, warum Deutschland sich lieber auf rein-defensive Maßnahmen in der Abwehr von Cyberangriffen fokussieren sollte und führt dabei unter anderem die Thematik der Kritischen Infrastrukturen und Cyberabschreckung an.
Link:	https://www.youtube.com/watch?v=JP86QU2eW54

Autor:innen:	**Ann Cathrin Riedel, LOAD e.V. und Dr. Payam Ghaledar, Hertie School of Governance**
Titel (Jahr):	Der Cyberkrieg hat längst begonnen (2020)
Beschreibung:	Vor dem Hintergrund der Eskalation des Konflikts zwischen den Vereinigten Staaten und dem Iran Anfang des Jahres fordern die Autor:innen in diesem Gastbeitrag einen konsequenten Schwerpunkt auf Defensive im Cyberraum.
Link:	https://background.tagesspiegel.de/digitalisierung/der-cyberkrieg-hat-laengst-begonnen

3. Analysen und Perspektiven von Sachverständigen aus der Technik

Autor:innen:	**Manuel Atug, AG KRITIS**
Titel (Jahr):	Wie Hackback mit der Gesellschaft spielt (2019) [Video]
Beschreibung:	Betrachtung verschiedener Aspekte von Hackbacks aus Perspektive der Gesellschaft mit Fokus auf Kritische Infrastrukturen.
Link:	https://media.ccc.de/v/2019-218-wie-hackback-mit-der-gesellschaft-spielt

Autor:innen:	**Felix von Leitner, Fefes Blog**
Titel (Jahr):	Hackback - tolle Idee? (2019) [Vortragsfolien]
Beschreibung:	Realitätscheck von Hackbacks aus der technischen Sicht einer Hackers.
Link:	http://ptrace.fefe.de/Hackback/#10

Autor:innen:	**Manuel Atug, AG KRITIS**
Titel (Jahr):	#Defensive statt #Offensive am Beispiel von KRITIS (2019) [Video]
Beschreibung:	Gegenüberstellung von Defensive und Offensive im Cyberraum aus Perspektive der Gesellschaft mit Fokus auf Kritische Infrastrukturen.
Link:	https://media.ccc.de/v/Camp2019-10208-defensive_statt_offensive_am_beispiel_von_kritis

4. Perspektiven aus der Industrie

Autor:innen:	**Steven Heckler, Bundesverband der Deutschen Industrie e. V.**
Titel (Jahr):	Staatliches Wirken im Cyberraum (2019)
Beschreibung:	Vorschlag aus der deutschen Industrie zur Entwicklung von Prinzipien für das staatliche Handeln und Wirken im Cyberraum unter Vermeidung von Eskalation zwischen Staat und Cyberkriminellen.
Link:	https://e.issuu.com/embed.html?d=201911_position_bdi_digitale_gegenangriffe&hideIssuuLogo=true&u=bdi-berlin

5. Perspektiven aus Regierung und Politik

Autor:innen:	**Anke Domscheit-Berg, MdB DIE LINKE**
Titel (Jahr):	Riskante Kriegsspiele (2019)
Beschreibung:	Diskussion der Vereinbarkeit von Instrumenten der Aktiven Cyberabwehr mit dem Grundgesetz, mögliche Kollateralschäden und Eskalationsgefahr.
Link:	http://www.ethikundmilitaer.de/fileadmin/ethik_und_militaer/Ethik-und-Militaer-2019-1.pdf

Autor:innen:	**Andreas Könen, Bundesministerium des Innern, für Bau und Heimat**
Titel (Jahr):	Cybersicherheit und Cyberverteidigung (2019)
Beschreibung:	Einbettung der Notwendigkeit von Cyberabwehr-Maßnahmen für den äußersten Notfall in die gesamtstaatliche Cybersicherheits- und verteidigungsstrategie.
Link:	http://www.ethikundmilitaer.de/fileadmin/ethik_und_militaer/Ethik-und-Militaer-2019-1.pdf

Autor:innen:	**Deutsche Bundesregierung**
Titel (Jahr):	Hackbacks als aktive digitale Gegenwehr (2018)
Beschreibung:	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
Link:	https://dip21.bundestag.de/dip21/btd/19/054/1905472.pdf

Autor:innen:	**Deutsche Bundesregierung**
Titel (Jahr):	Digitaler Verteidigungsfall (2019)
Beschreibung:	Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/11734 – „Digitaler Verteidigungsfall“
Link:	http://dipbt.bundestag.de/dip21/btd/19/122/1912235.pdf

Autor:innen:	**Deutsche Bundesregierung**
Titel (Jahr):	IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von Angriffen (2019)
Beschreibung:	Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Agnieszka Brugger, Tabea Rößner, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/11755 – IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von Angriffen
Link:	https://dipbt.bundestag.de/dip21/btd/19/122/1912280.pdf

Autor:innen:	**SWR Wissen**
Titel (Jahr):	Hackbacks bei der Bundeswehr? (2020) [Video]
Beschreibung:	odysso-Recherche zum Thema Hackbacks bei der Bundeswehr, bei der u. a. der Kommandeur des Zentrums Cyber-Operationen (ZCO) der Bundeswehr zu Wort kommt.
Link:	https://www.ardmediathek.de/ard/player/Y3JpZDovL3N3ci5kZS9hZXgvbzEyMDUxNDE