Fachbereich WD 3

Verfassungsrechtlicher Rahmen staatlicher Cyberabwehr

Verbot friedensstörender Handlungen und Kompetenzverteilung

Verfassungsrechtlicher Rahmen staatlicher Cyberabwehr
Verbot friedensstörender Handlungen und Kompetenzverteilung

Aktenzeichen:	WD 3 - 3000 - 056/26
Abschluss der Arbeit:	06.07.2026
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Fragestellung

Vor dem Hintergrund des jüngst von der Bundesregierung in den Bundestag eingebrachten Entwurfes eines Gesetzes zur Stärkung der Cybersicherheit[1] wurden die Wissenschaftlichen Dienste des Deutschen Bundestages um eine Darstellung des verfassungsrechtlichen Rahmens für die aktive staatliche Cyberabwehr gebeten.

Dafür wird auftragsgemäß zunächst beleuchtet, inwieweit Art. 26 Abs. 1 Satz 1 Grundgesetz (GG)[2] das staatliche Handeln in diesem Bereich beschränken kann (dazu unter 2.). Zudem wird der Frage nachgegangen, ob und welche Behörden des Bundes für entsprechende Maßnahmen nach der grundgesetzlichen Kompetenzverteilung zuständig sein könnten, wobei sich die Ausführungen nicht auf die vom Gesetzentwurf betroffenen Akteure beschränken (siehe dazu unter 3.). Die Prüfung der Vereinbarkeit des Gesetzentwurfs mit der Verfassung ist nicht Gegenstand dieser Arbeit.

Eine Prüfung grundrechtlicher Gewährleistungen erfolgt nicht. Insoweit wird darauf verwiesen, dass staatliche Cybermaßnahmen die Grundrechte auf informationelle Selbstbestimmung, auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), das Fernmeldegeheimnis (Art. 10 Abs. 1 GG), das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) und die Eigentumsfreiheit (Art. 14 Abs. 1 GG) berühren können und im Hinblick darauf grundrechtskonform – insbesondere verhältnismäßig – ausgestaltet sein müssen, um verfassungsgemäß zu sein.[3]

Die Zulässigkeit staatlicher Cyberabwehrmaßnahmen nach dem Völkerrecht wird in diesem Sachstand nur so weit thematisiert, wie dies für Art. 26 GG von Belang ist. Eine vertiefte Darstellung der völkerrechtlichen Maßstäbe bietet jedoch der Sachstand „Aktive Cyberabwehr – Völkerrechtliche Rahmenbedingungen“ des Fachbereichs EU 6.[4] Dieser stellt auch die verschiedenen Begrifflichkeiten und Definitionsansätze dar, die in der Debatte um aktive Reaktionsmöglichkeiten auf Cyberangriffe diskutiert werden („aktive Cyberabwehr“, „Hackback“ etc.). Im Folgenden wird der Begriff der aktiven Cyberabwehr verwendet.

2. Verbot friedensstörender Handlungen

Maßnahmen der staatlichen Cyberabwehr, die grenzüberschreitenden Charakter haben, etwa weil bei einem Angriff, auf den reagiert werden soll, Angreifer, Server, Infrastruktur und Opfer in ver-

---

1 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Stärkung der Cybersicherheit vom 22.06.2026, BT-Drs. 21/6585.

2 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 22.03.2025 (BGBl. 2025 I Nr. 94).

3 Dazu etwa: Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GZS 2020, 251 (253).

4 Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26.

schiedenen Staaten liegen, müssen die Vorgaben des Völkerrechts beachten.[5] Diese sind grundsätzlich auch im Cyberraum anwendbar.[6] Daneben sind die staatlichen Stellen jedoch auch durch die Verfassung verpflichtet, bestimmte völkerrechtswidrige Handlungen zu unterlassen. Art. 26 Abs. 1 Satz 1 GG übernimmt insofern die „Grundwerte der Völkerrechtsordnung […] ins innerstaatliche Recht", bewehrt sie mit Sanktionen und sieht damit einen „grundsätzlichen Gleichlauf von Verfassungs- und Völkerrecht"[7] vor.[8]

2.1. Voraussetzungen von Art. 26 Abs. 1 Satz 1 GG

Art. 26 Abs. 1 Satz 1 GG legt fest, dass Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören, insbesondere die Führung eines Angriffskrieges vorzubereiten, verfassungswidrig (und damit rechtlich unwirksam) sind. Adressaten von Art. 26 Abs. 1 Satz 1 GG sind staatliche Organe und Privatpersonen.[9]

Die „Vorbereitung eines Angriffskriegs" (und erst recht die Durchführung[10]), ist als Sonderfall einer Friedensstörung („insbesondere")[11] zu sehen und umfasst jede gewaltsame, völkerrechtlich nicht zu rechtfertigende Aggression.[12] Das Verbot friedensstörender Handlungen setzt einen Verstoß gegen Normen des Völkerrechts voraus, die zum Schutz des Friedens bestehen,[13] d.h. insbesondere gegen das Gewaltverbot gemäß Art. 2 Nr. 4 UN-Charta.

---

5 Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26, S. 8.

6 Siehe dazu: Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26, S. 8 mit Verweis auf Schaller, Internationale Sicherheit und Völkerrecht im Cyberspace, Für klarere Regeln und mehr Verantwortung, Stiftung für Wissenschaft und Politik, Oktober 2014, S. 7.

7 Herdegen, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 26 Rn. 2 m.w.N.

8 Mit der Frage der Vereinbarkeit von „Hackbacks" mit Art. 26 Abs. 1 Satz 1 GG beschäftigt sich bereits die Arbeit: Wissenschaftliche Dienste des Deutschen Bundestages, Verfassungsmäßigkeit von sog. „Hackbacks" im Ausland, Ausarbeitung vom 08.06.2018, WD 3 - 3000 - 159/18.

9 Heintschel von Heinegg/Frau, in: Epping/Hillgruber, BeckOK Grundgesetz, 65. Edition, Stand: 01.03.2026, Art. 26 Rn. 3; Jarass, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 26 Rn. 6; indem Art. 26 Abs. 1 Satz 1 auch Handlungen Privater einbezieht, geht Art. 26 Abs. 1 Satz 1 GG über völkerrechtliche Verbote hinaus; Herdegen, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 26 Rn. 4.

10 BVerwGE 127, 302 (314 f.); Jarass, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 26 Rn. 3.

11 Streinz/Wiater, in: Sachs, Grundgesetz, 10. Aufl. 2024, Art. 26 Rn. 17 m.w.N.

12 Jarass, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 26 Rn. 3.

13 Hierbei fallen unmittelbare Verursachung, Anstiftung und Beihilfe unter die Störungshandlung, Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 26.

Nach überwiegender Ansicht geht Art. 26 Abs. 1 Satz 1 GG angesichts seines Wortlautes (der nicht auf das Gewaltverbot, sondern auf die Friedensstörung abstellt) darüber hinaus,[14] wobei die Einzelheiten umstritten sind. Diskutiert wird etwa die Einbeziehung des völkerrechtlichen ius cogens (zwingendes Recht) und völkerrechtlicher Verbrechen (Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen und Aggression) sowie gravierender, systematischer Menschenrechtsverletzungen (Folterverbot, Verbot der Sklaverei).[15] Ein Einbezug des völkerrechtlichen Interventionsverbots wird dagegen als zu weitgehend angesehen.[16] Auch im Hinblick auf den Schutz vor Bedrohungen durch international agierende Terrororganisationen als „neue Formen" der Friedensbedrohung wird davon ausgegangen, dass sie von Art. 26 Abs. 1 Satz 1 GG erfasst sind, „weil sie durchgehend durch eine völkerrechtswidrige Ausübung von Gewalt gekennzeichnet sind und dadurch die strukturelle Nähe" zum völkerrechtlichen Gewaltverbot gewahrt bleibt.[17]

Bejaht man eine Handlung nach Art. 26 Abs. 1 Satz 1 GG, so muss diese jedenfalls auch geeignet sein, eine konkrete Gefahr für den Fortbestand des Friedens mit sich zu bringen, wobei genügt, dass eine Verletzung des Friendens mit hinreichender Sicherheit zu erwarten ist.[18] Ob eine bestimmte Handlung diese Gefahr birgt, bedarf allerdings häufig einer komplexen Prognoseentscheidung, bei der den entscheidenden Staatsorganen ein weiter Beurteilungsspielraum zusteht.[19]

Da Art. 26 Abs. 1 Satz 1 GG nur völkerrechtswidriges Verhalten sanktioniert[20], erfasst er jedoch keine Fälle, in denen die Drohung oder Anwendung von Gewalt zur individuellen oder kollektiven Selbstverteidigung oder Nothilfe (Art. 51 UN-Charta) ausgeübt wird oder anderweitig völkerrechtlich gerechtfertigt ist.[21]

---

14 Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 23; Jarass, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 26 Rn. 2; Herdegen, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 26 Rn. 17.

15 Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 24; ähnlich auch: Streinz/Wiater, in: Sachs, Grundgesetz, 10. Aufl. 2024, Art. 26 Rn. 11; nach Herdegen, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 26 Rn. 17 ginge etwa eine Einbeziehung aller Verletzungen des ius cogens zu weit.

16 Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 24.

17 Streinz/Wiater, in: Sachs, Grundgesetz, 10. Aufl. 2024, Art. 26 Rn. 10 m.w.N.; Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 24.

18 Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 39.

19 BVerfGE 68, 1 (103): „Jenseits dieser rechtlichen Grenzen aber obliegt es der außen- und verteidigungspolitischen Beurteilungs- und Handlungsmacht der Exekutive, solche Lagen, Entwicklungen und Risiken zu beurteilen und Entscheidungen zu treffen"; Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 39, soweit Private handeln, können die Gerichte den Tatbestand der Eignung zur Friedensstörung dagegen in vollem Umfang nachprüfen.

20 Jarass, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 26 Rn. 4, einschränkend wird zudem eine hinreichende Klarheit der Völkerrechtswidrigkeit gefordert.

21 Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 33.

In subjektiver Hinsicht setzt Art. 26 Abs. 1 Satz 1 GG voraus, dass der Angriff in der Absicht vorbenommen wird, das friedliche Zusammenleben der Völker zu stören.[22] Dabei muss die Friedensstörung nicht das bewusst gewollte Ziel der Handlung sein, vielmehr genügt es, wenn sie als unvermeidliches Mittel zur Erreichung anderer Ziele bewusst in Kauf genommen wird.[23]

Zu beachten ist, dass Maßnahmen, die gegen völkerrechtliche Regelungen verstoßen, welche nicht von der Norm erfasst sind (wie z.B. das Interventionsverbot), zwar nicht nach Art. 26 Abs. 1 Satz 1 GG verfassungswidrig, aber dennoch von den staatlichen Stellen zu beachten sind, da sie – je nach betroffener Regelung – den Rang eines einfachen Gesetzes gemäß Art. 59 Abs. 2 GG oder zwischen einfachem Recht und Verfassung haben (Art. 25 GG).[24]

2.2. Maßnahmen der aktiven Cyberabwehr im Lichte von Art. 26 Abs. 1 Satz 1 GG

Staatliche Maßnahmen der aktiven Cyberabwehr dürfen somit im Rahmen von Art. 26 Abs. 1 Satz 1 GG nicht der Vorbereitung oder der Durchführung eines Angriffskriegs dienen oder in anderer Art und Weise ungerechtfertigt gegen die oben genannten Vorgaben des Völkerrechts, insbesondere gegen das Gewaltverbot verstoßen.[25]

Ob ein Verstoß gegen Art. 26 Abs. 1 Satz 1 GG vorliegt, müsste jeweils im Einzelfall bewertet werden. Dabei wäre insbesondere zu prüfen, ob ein Verstoß gegen das Gewaltverbot gemäß Art. 2 Nr. 4 UN-Charta vorliegt, ob sich dieser völkerrechtlich rechtfertigen lässt, und – wenn dies nicht der Fall ist –, ob er in der Absicht vorgenommen wird, das friedliche Zusammenleben der Völker zu stören. Da sich die Voraussetzungen eines Verstoßes gegen das Gewaltverbot und einer entsprechenden Rechtfertigung nach Art. 51 UN-Charta maßgeblich nach dem Völkerrecht richten, wird weitestgehend auf die ausführlichen Darstellungen des Fachbereichs EU 6 verwiesen.[26]

Hingewiesen wird hier nur darauf, dass staatlich verantwortete Cyberoperationen grundsätzlich einen Verstoß gegen das Gewaltverbot darstellen können, jedoch nur dann, wenn sie nach Ausmaß (scale) und Wirkung (effect) mit einer Gewaltanwendung mit konventionellen Mitteln, die auf der Freisetzung kinetischer Energie beruht, gleichzusetzen sind, also physische Zerstörungen

22 Jarass, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 26 Rn. 4.

23 Fink/Langenfeld, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 26 Rn. 42 m.w.N.

24 Zur Rechtfertigung von Maßnahmen unterhalb der Schwelle des Gewaltverbots: Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26.

25 Dazu auch: Bothe, Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsausschuss des Deutschen Bundestages vom 17.02.2016, Ausschuss.-Drs. 18(12)633, S. 2.

26 Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26, S. 8 ff.

von erheblichem Umfang verursachen.[27] Maßnahmen, die allein im Cyberraum bleiben, dürften dagegen keine Gewalt im Sinne von Art. 2 Nr. 4 UN-Charta darstellen.[28]

Läge eine staatliche Cybermaßnahme vor, die mit einem physischen Angriff gleichzusetzen wäre, so ließe sich diese (abgesehen von einer Mandatierung durch den Sicherheitsrat nach Art. 39, 42 UN-Charta) grundsätzlich nur über das Recht zur individuellen oder kollektiven Selbstverteidigung nach Art. 51 UN-Charta rechtfertigen.[29] Dieser ermöglicht eine Gewaltanwendung jedoch nur als Reaktion auf einen bewaffneten Angriff. Hierzu führt *Barczak* aus:

> „Dieses Tatbestandsmerkmal ist zwar einer dynamischen Auslegung zugänglich und somit nicht auf Angriffsszenarien beschränkt, wie sie der Völkergemeinschaft noch im Jahr 1945 vor Augen gestanden haben mögen. Um eine ausufernde und missbräuchliche Handhabung des Selbstverteidigungsrechts auszuschließen, bedarf es jedoch eines funktionalen Angriffsäquivalents. Ein Cyberangriff muss hiernach – wiederum nach Ausmaß und Wirkung – einem bewaffneten Angriff im konventionellen Sinne gleichkommen, was erhebliche Sach- und Personenschäden sowie die Zerstörung kritischer Infrastruktur erfordert. Dies ist nur in besonders gelagerten Ausnahmefällen vorstellbar: Im Regelfall wird die Schwelle zum bewaffneten Angriff auch bei fortgeschrittenen und nachhaltigen Cyberangriffen (sog. Advanced Persistent Threats, APT) nicht überschritten.“[30]

Soweit ein Verstoß gegen das Gewaltverbot in Rede steht, sind somit die Hürden für eine Rechtfertigung hoch.

Im Zusammenhang mit der aktiven staatlichen Cyberabwehr wird zudem häufig das Problem aufgeworfen, dass sich Cyberangriffe nicht immer zweifelsfrei einem Angreifer zuordnen lassen. So führt etwa *Schmoldt* aus:

> „[…] IP-Adressen und Identitäten können verschleiert und anonymisiert werden, indem beispielsweise Cyberangriffe über Botnetze, kompromittierte oder hintereinander gereihte Rechner ausgeführt werden, so dass die IP-Adresse oder Identität des unbeteiligten Botrechner sichtbar, die des Angreifers allerdings verschleiert ist. Und selbst wenn durch technische Attribution der Ursprungsort oder die Urheber-IP-Adresse identifiziert werden kann, so bleibt unklar, wer der Urheber des Angriffs war oder welche Person in welcher Funktion zum Angriffszeitpunkt dahintersteht.“[31]

---

27 Barczak, Lizenz zum Hacken, NJW 2020, 595 (597); Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26, S. 11.

28 Unterabteilung Europa, Aktive Cyberabwehr, Völkerrechtliche Rahmenbedingungen, Sachstand vom 19.06.2026, EU 6 - 3000 - 079/26, S. 11 m.w.N.

29 Barczak, Lizenz zum Hacken, NJW 2020, 595 (597).

30 Barczak, Lizenz zum Hacken, NJW 2020, 595 (597 m.w.N.).

31 So: Schmoldt, Von der Defensive zur Cyberoffensive? Aktive Cyberabwehr, Hackbacks und der Diskurs der Akteure in der deutschen Sicherheitspolitik, ZFAS 2024, 165 (176).

Ohne zweifelsfreie Attribution bestehe so das Risiko, dass Angreifer falsche Fährten legten und Gegenmaßnahmen Unbeteiligte träfen.[32]

Im Rahmen von Art. 26 Abs. 1 Satz 1 GG wäre dies so lange unproblematisch, wie die Auswirkungen im Cyberraum blieben oder nicht die (hohen) Hürden des Gewaltverbots erreichten. Würden dagegen aufgrund einer falschen Fährte durch staatliche Cybermaßnahmen unbeteiligte Staaten in einem Ausmaß betroffen, das zu physischer Zerstörung von erheblichem Umfang führte, so könnte ein Verstoß gegen das Gewaltverbot vorliegen, der sich auch über Art. 51 UN-Charta nicht rechtfertigen ließe, da sich die Gegenmaßnahme nicht gegen den Angreifer richten würde.[33] Zudem wird darauf hingewiesen, dass es, wenn Ermittlungen angestellt werden, um die zweifelsfreie Zuordnung eines Cyberangriffs zu ermöglichen, wiederum für eine völkerrechtliche Rechtfertigung an einem zeitlichen und sachlichen Zusammenhang zwischen Angriff und Gegenmaßnahme fehlen könne.[34]

Art. 26 Abs. 1 Satz 1 setzt wie erläutert zudem in subjektiver Hinsicht voraus, dass die Friedensstörung als unvermeidliches Mittel zur Erreichung anderer Ziele bewusst in Kauf genommen wird. Ab wann diese Schwelle bei der Durchführung von staatlichen Maßnahmen der aktiven Cybermaßnahmen erreicht wäre, wäre ebenfalls im jeweiligen Einzelfall zu betrachten. Dabei könnte auch von Relevanz sein, inwieweit die dargestellte Problematik berücksichtigt sowie versucht wurde, eine fehlerhafte Attribution im konkreten Falle auszuschließen, und inwieweit eine mögliche Friedensstörung in Kauf genommen oder darauf vertraut wurde, dass es dazu im konkreten Fall nicht kommen würde.

3. Kompetenzverteilung des Grundgesetzes

Weiter wurde gefragt, welche Bundesbehörden nach der Kompetenzverteilung des Grundgesetzes für Maßnahmen der aktiven Cyberabwehr zuständig sein könnten. Auftragsgemäß beschränkt sich die Darstellung nicht auf die im Gesetzentwurf genannten Behörden, sondern gibt einen kursorischen Überblick über die Kompetenzverteilung in diesem Bereich. Dies schließt nicht aus, dass auch weitere Behörden in Betracht kommen können.

Es wird auch darauf hingewiesen, dass im Hinblick auf die Zuständigkeitsverteilung im Bereich der aktiven Cyberabwehr bislang noch vieles rechtlich offen erscheint. So weist etwa *Kipker* darauf hin, dass die Zuständigkeitsabgrenzungen bei der aktiven Cyberabwehr aufgrund der grenzüberschreitenden Natur und der Vielzahl von Interessen und Akteuren bei Cyberangriffen ver-

---

32 Schmoldt, Von der Defensive zur Cyberoffensive? Aktive Cyberabwehr, Hackbacks und der Diskurs der Akteure in der deutschen Sicherheitspolitik, ZFAS 2024, 165 (177); so auch u.a.: Cyberintelligence.Institute GmbH, Schriftliche Stellungnahme zum Referentenentwurf der Bundesregierung für ein Gesetz zur Stärkung der Cybersicheriet, 15.03.2026, S. 7; Verband der Internetwirtschaft e.V., Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Stärkung der Cybersicherheit, 17.03.2026, S. 3; Bundesverband IT-Sicherheit e.V., Stellungnahme zum BMI-Referentenentwurf eines Gesetzes zur Stärkung der Cyber-Sicherheit, 16.03.2026, S. 4.

33 Schmoldt, Von der Defensive zur Cyberoffensive? Aktive Cyberabwehr, Hackbacks und der Diskurs der Akteure in der deutschen Sicherheitspolitik, ZFAS 2024, 165 (177).

34 Verband der Internetwirtschaft e.V., Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Stärkung der Cybersicherheit, 17.03.2026, S. 3.

schwämmen und sich die Frage stelle, ob es sich bei aktiven Maßnahmen der Cyberabwehr überhaupt um Prävention, Gefahrenabwehr oder repressive Handlungen handle oder nicht[35] – wobei er dies zu vereinen scheint und aus diesem Grund auf die Bundeswehr verweist. Andere Stimmen halten aktive Cybermaßnahmen auch im zivilen Bereich für zulässig und bejahen jedenfalls die grundsätzliche Möglichkeit einer Wahrnehmung auch durch andere Sicherheitsbehörden.[36]

Im Folgenden soll daher grob zwischen Cyberverteidigung und Cyberabwehr unterschieden werden.[37] Cyberverteidigung wird insofern als Cybergegenwehr durch die militärischen Fähigkeiten der Streitkräfte verstanden, deren rechtlicher Rahmen derjenige ist, der für den Einsatz der Streitkräfte gilt und deren Adressaten in der Logik des Völkerrechts grundsätzlich andere Staaten als Zurechnungsobjekte von Cyberoperationen sind.[38] Als Cyberabwehr werden dagegen zivile Reaktionen auf rechtswidrige Beeinträchtigungen bezeichnet, welche die Verfügbarkeit, Integrität und Vertraulichkeit von informationstechnischen Systemen durch informationstechnische Mittel manipulieren, beeinflussen oder stören. Diese sind am Rechtsrahmen für Sicherheitsbehörden zu messen und haben „in der Logik des Gefahrenabwehrrechts“ vor allem nicht-staatliche Akteure „als gefahrenabwehrrechtliche Störer“ als Adressaten.[39]

3.1. Cyberverteidigung

Die Bundeswehr operiert im Cyberraum auf Grundlage der allgemeinen verfassungsrechtlichen Vorschriften für Bundeswehreinsätze. Einen Überblick zu den kompetenzrechtlichen Grundlagen für Cybermaßnahmen der Bundeswehr sowie die Erfordernisse der parlamentarischen Beteiligung gibt die Dokumentation der Wissenschaftlichen Dienste des Deutschen Bundestages „Cyberoperationen der Bundeswehr“, auf die insoweit verwiesen wird.[40]

---

35 Kipker, Hackback in Deutschland: Wer, was, wie und warum?, GSZ 2020, 26 (27).

36 Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GSZ 2020, 251; für die grundsätzliche Möglichkeit einer Zuständigkeit anderer Sicherheitsbehörden unterhalb der Schwelle des Verteidigungsfalles wohl auch: Barczak, Lizenz zum Hacken, NJW 2020, 595 (599).

37 Zur Differenzierung siehe: Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GZS 2020, 251 mit Verweis auf die Cybersicherheitsstrategie für Deutschland des BMI aus dem Jahr 2016 und die ständige parlamentarische Antwortpraxis.

38 Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GZS 2020, 251 mit Verweis auf Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP (BT-Drs. 19/5076) vom 05.11.2018, BT-Drs. 19/5472, S. 5, 7.

39 Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GZS 2020, 251 mit Verweis auf Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jimmy Schulz, Manuel Höferlin, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP (BT-Drs. 19/2032) vom 11.06.2018, BT-Drs. 19/2645, S. 2; Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Agnieszka Brugger, Dr. Konstantin von Notz, Dr. Tobias Lindner, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN (BT-Drs. 19/2618) vom 17.07.2018, BT-Drs. 19/3420, S. 2, 6.

40 Wissenschaftliche Dienste des Deutschen Bundestages, Cyberoperationen der Bundeswehr, Dokumentation vom 25.02.2022, WD 2 - 3000 - 012/22.

3.2. Cyberabwehr

Soweit es unterhalb der Schwelle der Cyberverteidigung um die Abwehr von Gefahren im Cyberraum geht, ergibt sich Folgendes im Hinblick auf die Zuständigkeitsverteilung: Nach der Systematik des Grundgesetzes ist die Gefahrenabwehr grundsätzlich Sache der Länder und wird entsprechend durch die Landesbehörden, insbesondere die Landespolizeien wahrgenommen (Art. 30, 70 Abs. 1 GG).[41] Damit dürfte auch die Abwehr von zivilen Cyberangriffen in erster Linie in die Kompetenz der Länder fallen.

Daneben ermöglichen jedoch auch einige Gesetzgebungs- und Verwaltungskompetenzen dem Bund, in begrenztem Ausmaß eigene Polizeibehörden zu unterhalten, die Aufgaben der Gefahrenabwehr wahrnehmen.[42] Nur soweit dem Bund insoweit bereichsspezifische Kompetenzen zukommen, darf er Eingriffsmaßnahmen – wie solche der aktiven Cyberabwehr – regeln und durchführen.[43]

Soweit in der Debatte um die aktive Cyberabwehr über eine allgemeine Bundeszuständigkeit für Cyberangriffe aus einer ungeschriebenen Kompetenz kraft Natur der Sache nachgedacht wird, wird dies soweit ersichtlich überwiegend mit der Begründung abgelehnt, dass die Kompetenz eng auszulegen und auf Sachgebiete beschränkt sei, die strukturell nur bundeseinheitlich geregelt werden könnten – was für die aktive Cyberabwehr verneint wird.[44]

3.2.1. Bundeskriminalamt

Ein denkbarer Akteur im Bereich der Cyberabwehr könnte das Bundeskriminalamt (BKA) sein. Gemäß Art. 73 Abs. 1 Nr. 9a GG hat der Bund die Kompetenz für „die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht“. Unter Terrorismus wird die Verbreitung von Angst und Schrecken durch Androhung bzw. Anwendung von Gewalt und deren Instrumentalisierung als Druckmittel verstanden.[45] International ist dieser, wenn er länderübergreifend organisiert ist, länderübergreifend agiert oder länderübergreifende Ziele verfolgt.[46]

---

41 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 190.

42 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 190.

43 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 193.

44 So jedenfalls: Arbeitsgruppe Kritische Infrastrukturen, Stellungnahme zum Ref-E des Bundesministeriums des Innern (BMI) für ein Gesetz zur Stärkung der Cybersicherheit im Rahmen der Verbändebeteiligung, 12.03.2026, S. 11; siehe auch: Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GSZ 2020, 251 (252).

45 So: Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 212; ähnlich: Heintzen, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 73 Rn. 101: „Gewaltaktionen gegen eine politische Ordnung, um einen politischen Wandel herbeizuführen.“

46 Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 213 m.w.N.

Der Begriff der „Gefahrenabwehr“ ist im Kontext von Art. 73 Abs. 1 Nr. 9a GG weit zu verstehen und umfasst neben der Abwehr konkreter Gefahren auch die Verhütung terroristischer Straftaten im Vorfeld konkreter Gefahren.[47] Entsprechend verfügt der Bund in diesem Bereich über die Zuständigkeit zur Schaffung der aus dem Polizei- und Sicherheitsrecht bekannten Eingriffsbefugnisse.[48] Die Abwehr von Gefahren des internationalen Terrorismus muss nach Art. 73 Abs. 1 Nr. 9a GG „durch das Bundeskriminalpolizeiamt“ (d.h. das BKA) erfolgen.[49] Die Verwaltungskompetenz hierzu wird teils Art. 73 Abs. 1 Nr. 9a GG, teils Art. 87 Abs. 3 Satz 1 GG entnommen.[50]

Vor diesem Hintergrund erscheint es jedenfalls nicht ausgeschlossen, dass dem Bundeskriminalamt für Phänomene des „Cyberterrorismus“, die eine länderübergreifende Gefahr darstellen, auch Befugnisse der aktiven Cyberabwehr übertragen werden könnten.[51] Geht es um Cyberangriffe unterhalb dieser Schwelle, dürfte eine Zuständigkeit des BKA nach Art. 73 Abs. 1 Nr. 9a GG, Art. 87 Abs. 3 Satz 1 GG dagegen ausscheiden.

Darüber hinaus nimmt das BKA jedoch als Zentralstelle Aufgaben der innerstaatlichen und kriminalpolizeilichen Zusammenarbeit wahr: Art. 73 Abs. 1 Nr. 10 GG verleiht dem Bund die ausschließliche Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei, die Errichtung eines Bundeskriminalpolizeiamtes und die internationale Verbrechensbekämpfung. Nach Art. 87 Abs. 1 Satz 2 GG darf der Bund durch Bundesgesetz Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei errichten.[52]

Nach der herrschenden Ansicht darf das Bundeskriminalamt nur als Zentralstelle Aufgaben in den Bereichen der kriminalpolizeilichen Zusammenarbeit sowie der internationalen Verbrechensbekämpfung wahrnehmen.[53] Inwieweit dies die Kompetenzen des Bundes beschränkt, ist umstritten, insbesondere im Hinblick auf die Frage, ob das BKA auch die Aufgabe erhalten darf, schwere Kriminalität unabhängig von den Landespolizeibehörden mit originären Eingriffsbefugnissen zu bekämpfen.[54] Während teilweise eine restriktive Handhabung gefordert wird, nach der

---

47 Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 214 m.w.N.; Heintzen, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 73 Rn. 102.

48 Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 215 m.w.N.; über die materielle Verfassungskonformität derartiger Befugnisse sagt der Kompetenztitel dagegen nichts aus.

49 Heintzen, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 73 Rn. 104.

50 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 233 m.w.N.

51 So auch Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GSZ 2020, 251 (253).

52 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 220.

53 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 221 m.w.N.

54 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 222 ff.

nur Regelungen geschaffen werden können, die spezifisch die Zusammenarbeit von Bund und Ländern oder im Hinblick auf die internationale Verbrechensbekämpfung zum Gegenstand haben, verstehen andere Stimmen die Begriffe der Zentralstellen und der Zusammenarbeit weit und halten es für verfassungsrechtlich zulässig, das BKA mit originären Befugnissen zu außenwirksamen Maßnahmen, insbesondere zu eigenen Ermittlungen und zur repressiven Strafverfolgung und präventiven Straftatenverhütung auszustatten.[55] Die Rechtsprechung des BVerfG erscheint insoweit bislang uneindeutig, betont aber, dass das BKA als Zentralstelle „im Wesentlichen auf die Wahrnehmung von Koordinationsaufgaben“ beschränkt ist.[56] Jedenfalls im Hinblick auf die aktive Cyberabwehr wird eine Übertragung „neuer eigener gefahrenabwehrrechtlicher Eingriffsbefugnisse des Bundes" auf Grundlage von Art. 73 Abs. 1 Nr. 10, Art. 87 Abs. 1 Satz 1 GG abgelehnt.[57] Der Bund Deutscher Kriminalbeamter (BDK) hat hierzu ausgeführt:

> „Wenn die bisherige Kooperationskompetenz des Bundes nach Art. 73 Abs. 1 Nr. 10 GG ausreichen würde, hätte es die Grundgesetzänderung von 2006 zur Terrorismusabwehr nicht gebraucht. Der Verfassungsgeber hat damals bewusst Art. 73 Abs. 1 Nr. 9a GG eingefügt, um dem Bund eine präventive Zuständigkeit zur Abwehr von Gefahren des internationalen Terrorismus zu geben – also genau für Fälle, in denen eine Bundesbehörde in die klassische Gefahrenabwehr der Länder eingreifen soll.“[58]

Ob sich Befugnisse für die aktive Cyberabwehr des BKA darüber hinaus auf Art. 73 Abs. 1 Nr. 1 GG stützen ließen, erscheint offen. Bisher wurden v.a. die nachrichtendienstlichen Befugnisse des BND auf die Kompetenz des Bundes für „auswärtige Angelegenheiten“ gestützt. Hinsichtlich dieser betonte das BVerfG, dass Art. 73 Abs. 1 Nr. 1 GG nur Aufgaben und Befugnisse mit internationaler Dimension umfasse. Dagegen sei der Bundesgesetzgeber im Hinblick auf die Kompetenzverteilung des GG, insbesondere hinsichtlich der Zuständigkeit der Länder für die Gefahrenabwehr, nicht dazu berechtigt, den BND allgemein mit der Gewährleistung der inneren Sicherheit zu betrauen (dazu auch noch unter 3.2.3.).[59] Dies wäre auch bei einer Aufgabenübertragung an das BKA zu beachten.

Das BKA nimmt zudem Strafverfolgungssachen in Staatsschutzsachen wahr (Art. 96 Abs. 5 GG).[60] Ob dem BKA in diesen Bereichen auch gefahrenabwehrrechtliche Eingriffsbefugnisse eingeräumt

---

55 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 224 f. m.w.N.

56 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 223 m.w.N.; BVerfGE 110, 33 (51).

57 Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GSZ 2020, 251 (253).

58 Bund Deutscher Kriminalbeamter, BDK fordert klare verfassungsrechtliche Grundlage für Cyberabwehr auf Bundesebene, 27.10.2025.

59 BVerfGE 154, 152 (233).

60 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 231.

werden könnten, ist unklar, scheint jedoch aufgrund der grundsätzlichen Zuständigkeit der Länder für die Gefahrenabwehr zu weitgehend.

Zudem können dem BKA als Annex zu seinen sonstigen Aufgaben präventive Schutzaufgaben zugewiesen werden, die das BKA mit eigenen Ermittlungs- und Zwangsbefugnissen erfüllt.[61] Zu nennen sind insbesondere der Zeugenschutz sowie darüber hinaus – gestützt auf eine Kompetenz kraft Natur der Sache – der Schutz von Mitgliedern der Verfassungsorgane des Bundes und ihrer ausländischen Gäste. Ob sich hieraus auch eine bereichsspezifische Kompetenz des Bundes für aktive Cybermaßnahmen entnehmen lässt, etwa bei Angriff auf Systeme, die dem Zeugenschutz dienen, erscheint offen, könnte jedoch in Anbetracht der grundsätzlichen Verortung der Gefahrenabwehr bei den Ländern zu weit gehen. Jedenfalls lässt sich den Kompetenzen keine umfassende Zuständigkeit für die aktive Cyberabwehr entnehmen.

3.2.2. Bundespolizei

Ein weiterer möglicher Akteur könnte die Bundespolizei sein. Diese nimmt (als früherer Bundesgrenzschutz, umbenannt im Jahr 2005) über seine ursprüngliche Kernaufgabe, die Außengrenzen der Bundesrepublik zu schützen, hinaus inzwischen auch diverse weitere Aufgaben wahr, die in die Vollzugszuständigkeit des Bundes fallen.[62]

Zuständig ist die Bundespolizei nach Art. 73 Abs. 1 Nr. 5 GG, 87 Abs. 1 Satz 1 GG zunächst für die polizeiliche Überwachung der Bundesgrenzen, insbesondere die Abwehr von Gefahren für die Grenzen und die Kontrolle des grenzüberschreitenden Verkehrs.[63] Erfasst sind auch Kontrollen im anliegenden Hinterland sowie Kontrollen des grenzüberschreitenden Verkehrs auf Flughäfen und Bahnhöfen.[64] Regelungen zur Gefahrenabwehr, „die zwar an die Offenheit der Grenzen und damit einhergehende Gefahren anknüpfen“[65], nicht jedoch unmittelbar dem Schutz der Bundesgrenze dienen (wie Regelungen zur Bekämpfung von grenzüberschreitender Kriminalität), unterfallen dagegen nicht dem Grenzschutz.[66]

---

61 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 245.

62 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 246.

63 Heintzen, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 73 Rn. 53; Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 123.

64 Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 123; Bäcker, in: Listken/Denninger/Bäcker, Handbuch des Polizei- und Sicherheitsrechts, 8. Aufl. 2026, Kap. 2 Rn. 249; BVerfGE 97, 198 (214).

65 BVerfGE 150, 244 (271).

66 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch des Polizei- und Sicherheitsrechts, 8. Aufl. 2026, Kap. 2 Rn. 249.

Darüber hinaus ist die Bundespolizei gemäß Art. 73 Abs. 1 Nr. 6a[67], Art. 87e Abs. 1 Satz 1 GG für die Bahnpolizei zuständig, da die Norm auch „Regelungen über die traditionell dem Bund zukommende Aufgabe der Abwehr von konkreten Gefahren für die Sicherheit und Ordnung auf den Bahnanlagen der Eisenbahnen des Bundes“ umfasst.[68] Gleiches gilt für die Kompetenz des Bundes für den Luftverkehr gemäß Art. 73 Abs. 1 Nr. 6, Art. 87d Abs. 1 Satz 1 GG hinsichtlich der Abwehr von Gefahren, die auf den Luftverkehr einzuwirken drohen.[69] Räumlich beschränkt sich die Kompetenz auf Luftfahrzeuge und Anlagen für den Luftverkehr und sachlich auf luftverkehrstypische Gefahren (z.B. Flugzeugentführungen und Sabotageakte[70]).[71]

Soweit der Bundespolizei eine präventivpolizeiliche Aufgabe zugewiesen werden darf, darf sie zudem als Annex mit der Verfolgung von Straftaten betraut werden, die im Sachzusammenhang mit dieser Schutzaufgabe stehen.[72]

Auf eine ungeschriebene Kompetenz des Bundes kraft Natur der Sache werden zudem Aufgaben der Bundespolizei gestützt, die mit dem Objektschutz von Verfassungsorganen des Bundes verbunden sind.[73] Ferner kann die Bundespolizei nach überwiegender Ansicht, gestützt auf Art. 73 Abs. 1 Nr. 1 GG bzw. Art. 24 Abs. 2 GG sowie Art. 32 Abs. 1 GG zudem im Ausland – für internationale polizeiliche Maßnahmen, aber auch eigenständig durchgeführte Interventionen im Einzelfall – eingesetzt werden, soweit sich dies auf den Einsatz polizeilicher Mittel beschränkt (und nicht in eine quasi-militärische Aktion umschlägt).[74]

Bei einer Übertragung von Kompetenzen auf die Bundespolizei ist nach der Rechtsprechung des BVerfG jedoch zu beachten, dass sie nicht zu einer allgemeinen, mit den Landespolizeien konkurrierenden Bundespolizei ausgebaut werden und damit ihr Gepräge als Polizei mit begrenzten Aufgaben verlieren darf. Angesichts der grundsätzlichen Zuordnung der Polizeigewalt bei den Ländern müsse der Charakter der Bundespolizei als Sonderpolizei zur Sicherung der Grenzen

---

67 Soweit es materiell um Grenzschutz geht, ist aber Art. 73 Abs. 1 Nr. 5 GG einschlägig, dazu: Heintzen, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 73 Rn. 52, Rn. 63; BVerfGE 97, 198 (219); BVerfGE 155, 119 (174).

68 BVerfGE 97, 198 (221 f.).

69 Heintzen, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 73 Rn. 57; Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 137; zur Übertragung der Aufgabe des Schutzes vor Angriffen auf die Sicherheit des Luftverkehrs auf den Bundesgrenzschutz BVerfGE 97, 198 (225 f.).

70 BVerfGE 97, 198 (226).

71 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch des Polizei- und Sicherheitsrechts, 8. Aufl. 2026, Kap. 2 Rn. 262.

72 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 265.

73 Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 125.

74 Bäcker, in: Lisken/Denninger/Bäcker, Handbuch des Polizei- und Sicherheitsrechts, 8. Aufl. 2026, Kap. 2 Rn. 264.

und zur Abwehr bestimmter, das Gebiet oder die Kräfte eines Landes überschreitender Gefahrenlagen, gewahrt werden.[75]

Ob der Auftrag der Bundespolizei zur Gefahrenabwehr auch Maßnahmen der aktiven Cyberabwehr umfassen könnte, erscheint bislang offen. Teilweise wird dies abgelehnt, da die Bundeskompetenzen insoweit „höchstens eine Kompetenz für ein sachspezifisches potentielles Eindringen in ein angreifendes IT-System, nicht aber für ein Manipulieren oder IT-basiertes Zerstören“[76] bereithielten.

Sähe man dies anders, so müssten sich die Kompetenzen zur aktiven Cyberabwehr aber auf die verfassungsrechtlich begrenzten Kompetenzen der Bundespolizei beschränkten. Es erscheint jedenfalls nicht von Vorneherein ausgeschlossen, dass Cyberangriffe, die einen Bundesbezug aufweisen, sich also etwa gegen die Systeme des Grenzschutzes oder des Bahn- und Luftverkehrs wenden und damit eine Gefahr für diese begründen, nicht auch durch die Bundespolizei abgewehrt werden dürften. Eine Ausdehnung des Begriffs des Grenzschutzes auf die „Grenzen“ des Cyberraums und damit über die physischen Außengrenzen hinaus, dürfte dagegen zu weit gehen, da dies letztlich zu einer generellen Aufgabe der Bundespolizei für die Cyberabwehr führen könnte, die so von der Kompetenzordnung nicht vorgesehen ist. Auch muss bei der Übertragung von Kompetenzen beachtet werden, dass die Bundespolizei ihr Gepräge als Sonderpolizei zur Sicherung der Grenzen und zur Abwehr bestimmter Gefahrenlagen behalten muss.

3.2.3. Nachrichtendienste

Weiter stellt sich die Frage, ob den Nachrichtendiensten, konkret dem Bundesnachrichtendienst (BND) und dem Bundesamt für Verfassungsschutz (BfV) (die Kompetenzen des MAD ergeben sich aus den Regelungen für die Streitkräfte) aus kompetenzrechtlicher Sicht Befugnisse für die aktive Cyberabwehr übertragen werden könnten.

Die Gesetzgebungskompetenz des Bundes ergibt sich für die Aufgaben des BfV aus Art. 73 Abs. 1 Nr. 10 lit. b, lit. c GG. Dieser sieht die Zusammenarbeit von Bund und Ländern auf dem Gebiet des Verfassungsschutzes vor. Zwar bezieht sich die Norm ihrem Wortlaut nach nur auf die Behördenkooperation. „In gewissem Umfang“ ist jedoch auch eine Regelung des implizit vorausgesetzten Bundeshandelns vorgesehen.[77] Insofern ermöglicht der Kompetenztitel dem Bund auch, dem auf Grundlage von Art. 87 Abs. 1 Satz 2 GG eingerichteten BfV die für seine Aufgaben erforderlichen Befugnisse einzuräumen.[78] Art. 87 Abs. 1 Satz 2 GG sieht insoweit vor, dass durch Bundesgesetz Zentralstellen „für Zwecke des Verfassungsschutzes und des Schutzes gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorberei-

---

75 BVerfGE 97, 198 (218); Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 124.

76 Amthor, Aktive sicherheitsbehördliche Gefahrenabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GSZ 2020, 251 (253).

77 Seiler, in: Epping/Hillgruber, BeckOK Grundgesetz, 65. Edition Stand: 01.03.2026, Art. 73 Rn. 48.1.

78 Seiler, in: Epping/Hillgruber, BeckOK Grundgesetz, 65. Edition Stand: 01.03.2026, Art. 73 Rn. 48.1; BVerfGE 155, 119 (174); 163, 43 (79).

tungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden“, eingerichtet werden können. Im Hinblick auf die Umstrittenheit des Zentralstellenbegriffs wird auf die Ausführungen unter 3.2.1. verwiesen. Inwieweit dieser die Kompetenzen des BfV einschränkt, ist auch hier fraglich.

Die Kompetenzen des Bundes im Hinblick auf den BND ergibt sich wie bereits erwähnt für die Gesetzgebung aus Art. 73 Abs. 1 Nr. 1 GG (auswärtige Angelegenheiten).[79] Dieser erfasst auch die Auslandsaufklärung des BND, weil für die „auswärtigen Angelegenheiten“ auch Vorgänge im Ausland, deren Urheber nicht ausländische Staaten sind, Bedeutung haben können. Daher sind sowohl die Einrichtung einer Stelle zur umfassenden Auslandsaufklärung als auch deren Tätigkeit von Art. 73 Abs. 1 Nr. 1 Alt. 1 GG umfasst.[80] Die Verwaltungskompetenz des Bundes stützt sich nach überwiegender Ansicht auf Art. 87 Abs. 3 Satz 1 GG.[81] Im Hinblick auf die Früherkennung von aus dem Ausland drohenden Gefahren hat das BVerfG wie bereits erläutert klargestellt, dass sich aus der Kompetenzverteilung des Grundgesetzes (Art. 73 Abs. 1 Nr. 9a GG, 73 Abs. 1 Nr. 10 GG und der grundsätzlichen Zuständigkeit der Länder für die Gefahrenabwehr) ergibt, dass der Bund den Bundesnachrichtendienst nicht allgemein zum Zweck der Gewährleistung der inneren Sicherheit betrauen kann. Art. 73 Abs. 1 Nr. 1 GG berechtige den Bundesgesetzgeber nicht dazu, Befugnisse einzuräumen, die auf die Verhütung, Verhinderung oder Verfolgung von Straftaten als solche gerichtet seien. Dem BND könnten nur Aufgaben und Befugnisse übertragen werden, die eine außen- und sicherheitspolitische Bedeutung haben und damit eine internationale Dimension aufweisen.[82]

Zudem sind sowohl die Aufgaben des BfV als auch die des BND bislang – jedenfalls nach der einfachgesetzlichen Rechtslage – auf die Beschaffung und Auswertung von Informationen beschränkt. Ob sich dieser Aufgabenzuschnitt zwingend aus der verfassungsrechtlichen Kompetenzverteilung ergibt, oder ob den Behörden darüber hinaus auch exekutive Befugnisse übertragen werden könnten, wird unter dem Stichwort des „Trennungsgebotes“ zwischen Nachrichtendiensten und Polizeibehörden diskutiert und ist bislang nicht abschließend geklärt.

Einen Überblick über die Diskussion gibt die Arbeit „Übertragung ‚operativer‘ Befugnisse an den BND“, auf die insoweit verwiesen wird.[83] Das BVerfG jedenfalls hat bislang offen gelassen, ob

---

79 BVerfGE 100, 313 (368).

80 Uhle, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL Januar 2026, Art. 73 Rn. 41; BVerfGE 100, 313 (369); BVerfGE 154, 152 (234).

81 Ibler, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 109. EL August 2026, Art. 87 Rn. 157; Burgi, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 87 Rn. 49; Kment, in: Jarass/Pieroth, Grundgesetz, 19. Aufl. 2026, Art. 87 Rn. 7; Suerbaum, in: Epping/Hillgruber, BeckOK Grundgesetz, 65. Edition, Stand 01.03.2026, Art. 87 Rn. 26.

82 BVerfGE 154, 152 (233).

83 Wissenschaftliche Dienste des Deutschen Bundestages, Übertragung „operativer“ Befugnisse an den BND, Sachstand vom 12.12.2025, WD 3 - 3000 - 089/25, S. 6 ff.

und inwieweit sich der Kompetenzordnung des Grundgesetzes ein Trennungsgebot zwischen Nachrichtendiensten und Polizeibehörden entnehmen lässt.[84]

Aus den Grundrechten, genauer aus dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), hat das BVerfG jedoch ein informationelles Trennungsprinzip hergeleitet hat, nach dem der Datenaustausch zwischen Nachrichtendiensten und Polizeibehörden nur ausnahmsweise unter bestimmten, hohen Voraussetzungen zulässig sein soll. Dies soll hier in Anbetracht des unter 1. dargestellten Prüfumfangs nicht vertieft werden.[85]

Da das BfV nach der Kompetenzverteilung des GG grundsätzlich für das Inland (Art. 87 Abs. 1 Satz 2 GG „Bestrebungen im Bundesgebiet“) und der BND für das Ausland (Art. 73 Abs. 1 Nr. 1 GG) zuständig ist, könnte es in der Praxis für die Zuständigkeitsabgrenzung zwischen BfV und BND zudem problematisch sein, dass sich die Frage, ob ein Cyberangriff aus dem In- oder Ausland herrührt, nicht immer eindeutig beantworten lässt.

3.2.4. Bundesamt für Sicherheit in der Informationstechnik

Fraglich ist, ob das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständige Behörde für die aktive Cyberabwehr in Betracht kommen könnte. Grundsätzlich wird im Hinblick auf Regelungen, die unmittelbar die Sicherung der Informationstechnik in der Bundesverwaltung betreffen – und damit auch für die Errichtung des BSI – eine ungeschriebene Gesetzgebungskompetenz kraft Natur der Sache sowie aus Art. 86 Satz 2 GG angenommen[86] – wobei darauf hingewiesen wird, dass aus Art. 86 Satz 2 GG keine Verwaltungskompetenz des Bundes folgt, sondern dieser eine solche voraussetzt, sodass sich die Verwaltungskompetenz wohl eher aus Art. 87 Abs. 3 Satz 1 GG oder aus einer ungeschriebenen Verwaltungskompetenz ergeben dürfte. Zudem können sich Regelungen zum Schutz der Informationstechnik kritischer Infrastrukturen auf Art. 74 Abs. 1 Nr. 11 GG und auf weitere spezielle Kompetenztitel sowie die gefahrenabwehrrechtlichen Annexkompetenzen stützen.[87] Letztere erlauben es dem Bundesgesetzgeber, neben der ausdrücklich zugewiesenen Materie weitere Materien mitzuregeln, wenn diese in einem untrennbaren, sachlichen Zusammenhang mit der Hauptmaterie stehen und ihrer Vorbereitung oder Durchführung dienen.[88] Allerdings kann dies nur punktuelle Regelungen tragen.[89] Bei rein defensiven Befugnissen dürfte dies vertretbar sein, eine Kompetenz für aktive Gegenmaßnahen scheint jedoch

---

84 BVerfGE 97, 198 (217).

85 Siehe dazu aber: Wissenschaftliche Dienste des Deutschen Bundestages, Übertragung „operativer“ Befugnisse an den BND, Sachstand vom 12.12.2025, WD 3 - 3000 - 089/25, S. 9 ff.

86 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 16.02.2009, BT-Drs. 16/11967, S. 10.

87 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 25.02.2015, BT-Drs. 18/4096, S. 19; Gesetzentwurf der Bundesregierung, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 25.01.2021, BT-Drs. 19/26106, S. 31.

88 Degenhart, in: Sachs, Grundgesetz, 10. Aufl. 2024, Art. 70 Rn. 36.

89 Degenhart, in: Sachs, Grundgesetz, 10. Aufl. 2024, Art. 70 Rn. 37 m.w.N.

insbesondere im Hinblick auf die oben dargestellte Residualkompetenz der Länder im Bereich der Gefahrenabwehr zu weit zu gehen.[90]

3.3. Anforderungen an die parlamentarische Beteiligung und Kontrolle

Gefragt wurde darüber hinaus, ob sich unterschiedliche Anforderungen für die parlamentarische Beteiligung und Kontrolle ergeben würden, je nachdem welche Behörde für aktive Cybermaßnahmen zuständig wäre. Bei einer Übernahme durch die Streitkräfte ist zu beachten, dass diese der Kontrolle durch den Bundestag als Ganzem, durch den Verteidigungsausschuss und durch die Wehrbeauftragte des Deutschen Bundestages unterliegen und unter Umständen für einen Einsatz eine Zustimmung des Bundestages benötigen.[91] Bei einer Übertragung an die Nachrichtendienste unterlägen entsprechende Maßnahmen zudem den Besonderheiten der parlamentarischen Kontrolle der Nachrichtendienste. Insoweit wird auf die Ausarbeitung „Parlamentarische Kontrolle der Nachrichtendienste in ausgewählten Staaten“ verwiesen.[92] Eine Übertragung an andere Bundesbehörden dürfte dagegen nicht zu Besonderheiten im Hinblick auf die parlamentarische Kontrolle führen.

***

90 Amthor, Aktive sicherheitsbehördliche Cyberabwehr: Dogmatische Defizite und verfassungsrechtlicher Reformbedarf, GSZ 2020, 251 (252).

91 Wissenschaftliche Dienste des Deutschen Bundestages, Cyberoperationen der Bundeswehr, Dokumentation vom 25.02.2022, WD 2 - 3000 - 012/22.

92 Wissenschaftliche Dienste des Deutschen Bundestages, Parlamentarische Kontrolle der Nachrichtendienste in ausgewählten Staaten, Ausarbeitung vom 14.10.2022, WD 3 - 3000 - 095/22, S. 8 - 11.