Kurzinformation

Rechtliche Grundlagen und Aufgaben des BND bei der Cyberabwehr

Ein **Cyberangriff** ist „eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.“[1] Der Begriff **„Cyberabwehr“** wird üblicherweise als „Bestandteil einer weit gefassten Sicherheitsstrategie für informationstechnische Systeme gegen Angriffe aus Netzwerken“ verstanden.[2]

Nach § 1 Abs. 2 Satz 1 Bundesnachrichtendienstgesetz (BNDG) sammelt der Bundesnachrichtendienst (BND) zur Gewinnung von **Erkenntnissen über das Ausland**, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus. Da Erkenntnisse über das Ausland gesammelt werden, wird der BND auch als „Auslandsnachrichtendienst“ bezeichnet. Der Auftrag des BND ist **Aufklärung**, also die Gewinnung von Erkenntnissen durch Erhebung, Auswertung und Verarbeitung von Informationen. Der BND hat **keine exekutiven Befugnisse**, also auch keine polizeilichen Befugnisse (z. B. Zwangsmaßnahmen) oder Weisungsbefugnisse (§ 2 Abs. 3 Satz 1 BNDG). Maßnahmen der Gefahrenabwehr sind anderen Behörden vorbehalten. Der Auftrag des BND erschöpft sich insoweit in der Informationsübermittlung an Dritte und in Berichtspflichten.[3]

Die Erhebung von Informationen durch den BND erfolgt entweder offen oder – für die Cyberabwehr relevant – heimlich durch nachrichtendienstliche Mittel, zu denen unter den gesetzlichen Voraussetzungen auch die **Überwachung des Fernmeldeverkehrs** gehört. Eine Überwachung des Fernmeldeverkehrs kann entweder nach § 3 Artikel 10-Gesetz (G 10) als Individualmaßnahme gegen eine bestimmte Person oder als strategische Maßnahme nach § 5 G 10 bzw. § 19 BNDG erfolgen.

---

1 Bundesministerium des Innern, für Bau und Heimat, Cybersicherheitsstrategie für Deutschland 2021, S. 133, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=89B907BCF04E673DFDEAA0D7ECA10682.2_cid364?__blob=publicationFile&v=1 (letzter Abruf 22. Februar 2022).

2 Brunst in: Dietrich/Eiffeler, Handbuch des Rechts der Nachrichtendienste, 2017, Teil 5, § 7 Cyberabwehr, Rn. 4.

3 Gusy in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, BNDG Rn. 23.

WD 3 - 3000 - 021/22 (25. Februar 2022)

Im Rahmen der sogenannten **strategischen Überwachung** des Fernmeldeverkehrs (SIGINT) ist der BND befugt, bestimmte Telekommunikationsverbindungen mittels **Suchbegriffen** zu durchsuchen. Es handelt sich dabei nicht um einzelne Telekommunikationsanschlüsse, sondern um die „Transportwege" der Telekommunikation. Unterschieden wird dabei zwischen „internationalen Telekommunikationsbeziehungen", bei denen vom Inland in das Ausland kommuniziert wird, oder umgekehrt, und der „Ausland-Fernmeldeaufklärung", bei der es um Kommunikation von Ausländern im Ausland geht.

Bei **internationalen Kommunikationsbeziehungen** ist der BND nach § 5 Abs. 1 Nr. 8 G 10 zu einer Überwachung des Fernmeldeverkehrs befugt, „zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr […] des internationalen kriminellen, terroristischen oder staatlichen **Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen** in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen." Die so erhobenen Daten dürfen nach § 7 G 10 an andere Sicherheitsbehörden übermittelt werden. § 7 Abs. 4a G 10[4] erlaubt die Übermittlung an das Bundesamt für Sicherheit in der Informationstechnik (BSI)[5], „wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes oder zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken auch für andere Stellen und Dritte." Die zuletzt genannte Variante („Dritte") betrifft insbesondere die Sensibilisierung infrastrukturrelevanter Unternehmen seitens des BSI über eine potenzielle Gefährdung durch Cyberangriffe.[6]

Im Rahmen der **strategischen Ausland-Fernmeldeaufklärung** hat der BND nach § 19 Abs. 1 Nr. 2, Abs. 4 Nr. 1 lit. d BNDG[7] die Befugnis, den Fernmeldeverkehr zu überwachen, „soweit dies erforderlich ist für den Zweck […] der Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung". Im Bereich von Cyberangriffen müssen „tatsächliche Anhaltspunkte dafür vorliegen, dass durch [die strategischen Aufklärungsmaßnahmen] Erkenntnisse gewonnen werden können […] mit Bezug zu den folgenden Gefahrenbereichen: […] zu internationalen kriminellen, terroristischen oder staatlichen Angriffen mittels Schadprogrammen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von informationstechnischen Systemen." Auch diese Daten dürfen unter den in § 29 BNDG genannten Voraussetzungen übermittelt werden.

Voraussetzung für die Anordnung einer **Individualmaßnahme** ist das Vorliegen tatsächlicher Anhaltspunkte für den Verdacht, dass jemand im einzelnen bezeichnete Straftaten aus dem Bereich Cyber-Kriminalität[8] plant, begeht oder begangen hat, soweit sich die Straftat gegen die innere oder

---

4 Absatz 4a wurde durch Gesetz vom 17.12.2015 in das G 10 eingefügt; BGBl. 2015 I S. 1938.

5 Vgl. hierzu Wissenschaftliche Dienste des Deutschen Bundestags, Möglichkeit der Einstufung des BSI als Nachrichtendienst, WD 3 - 3000 - 200/21, https://www.bundestag.de/resource/blob/880180/615910e191c77469747837be54a42dfb/WD-3-200-21-pdf-data.pdf (Letzter Abruf 23. Februar 2022).

6 Huber in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, G 10 § 7 Rn. 17.

7 § 19 BNDG wurde durch Gesetz vom 19. April 2021 BGBl. 2021 I S. 771 neu eingeführt mit Geltung ab 1. Januar 2022.

8 Straftaten nach den §§ 202a, 202b und 303a, 303b des Strafgesetzbuches.

äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet (§ 3 Abs. 1 Satz 1 Nr. 8 G 10[9]). Die Voraussetzungen für eine Übermittlung der erhobenen Daten regeln § 4 Abs. 4 bis 6 G 10. Daten aus einer Individualmaßnahme dürfen nur zur Verhinderung oder Aufklärung von Straftaten übermittelt werden. Da das BSI keine Strafverfolgungskompetenz hat, ist gegenwärtig einer Übermittlung von Erkenntnissen aus einer individuellen Maßnahme an das BSI nicht zulässig.[10]

Sämtliche Maßnahmen beziehen sich auf den Zuständigkeitsbereich des BND, also vor allem auf das **Ausland** und nur in Ausnahmefällen auf das Inland.

Ein Austausch von Informationen mit anderen Sicherheitsbehörden gemäß einschlägiger gesetzlicher Übermittlungsregeln erfolgt unter anderem im Nationalen **Cyber-Abwehrzentrum** (Cyber-AZ), einer Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-) Behörden.[11]

Mit der **Übermittlung der Daten** endet die Zuständigkeit des BND und liegt dann bei den Inlandsbehörden (z. B. Bundesamt für Verfassungsschutz, BSI, Bundeskriminalamt etc.) oder gegebenenfalls bei der Bundeswehr. Diese Vorgehensweise wird als „SIGINT Support to Cyber Defense“ bezeichnet. Die Aufgabe des BND im Rahmen der Cyberabwehr ist daher die einer **Früherkennung solcher Angriffe**. Aktive Cyberabwehr durch Angriffe auf ausländische Server, die nicht zur Informationsgewinnung erfolgen, sondern die Zerstörung von Servern zum Ziel haben (sogenannte „Hackbacks“ oder Computer Network Intervention) sind dem BND nach derzeitiger Rechtslage verboten, da ihm hierzu die Befugnisse fehlen.[12]

In der **Praxis** ist der Anteil des BND bei der Telekommunikationsüberwachung im Bereich Cyber – jedenfalls bei Maßnahmen nach dem G 10 – eher **marginal**. So wurden im Jahr 2019 vom BND keine Maßnahmen nach § 3 Abs. 1 Satz 1 Nr. 8 G 10 durchgeführt. Bei strategischen Maßnahmen nach § 5 G 10 wurden im Gefahrenbereich Cyber im ersten Halbjahr 2019 130 Suchbegriffe und im zweiten Halbjahr 2019 keine Suchbegriffe angeordnet (im Vorjahr 133 bzw. 130). Am 16. März 2019 wurde die den Suchbegriffen zugrundeliegende Beschränkungsmaßnahme vollständig ausgesetzt. Der auswertende Fachbereich stufte keinen Telekommunikationsverkehr als nachrichtendienstlich relevant ein.[13] Für Maßnahmen nach § 19 Abs. 1 Nr. 2, Abs. 4 Nr. 1 lit. d BNDG, der erst kürzlich in Kraft getreten ist, liegen noch keine Berichte vor.

* * *

9 Nr. 8 wurde durch Gesetz vom 17. Dezember 2015 in das G 10 eingefügt; BGBl. 2015 I S. 1938.

10 Brunst in: Dietrich/Eiffeler, Handbuch des Rechts der Nachrichtendienste, 2017, Teil 5, § 7 Cyberabwehr, Rn. 95.

11 https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz.html (letzter Abruf 23. Februar 2022).

12 Wissenschaftliche Dienste des Deutschen Bundestags, Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland, WD 3 - 3000 - 159/18, S. 5, https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf (letzter Abruf 23. Februar 2022).

13 Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post-und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2019) vom 10. September 2021, BT-Drs. 19/32398, S. 6 f.