Sachstand

Zur geheimdienstlichen Tätigkeit ausländischer Nachrichtendienste in Deutschland und zur nachrichtendienstlichen Kooperation

WD 3 - 3000 - 165/22, WD 7 - 3000 - 114/22

Zur geheimdienstlichen Tätigkeit ausländischer Nachrichtendienste in Deutschland und zur nachrichtendienstlichen Kooperation

Aktenzeichen:	WD 3 - 3000 - 165/22, WD 7 - 3000 - 114/22
Abschluss der Arbeit:	15.12.2022
Fachbereich:	WD 3: Verfassung und Verwaltung (Teil 1, 2 und 4) WD 7: Zivil-, Straf- und Verfahrensrecht, Bau und Stadtentwicklung (Teil 3)

Inhaltsverzeichnis

1. Überblick 4

2. Verfassungsrechtliche Voraussetzungen und Regelungen des BNDG 4

3. Strafrechtliche Regelungen 6
3.1. Strafbarkeit geheimdienstlicher Tätigkeiten von ausländischen Staaten gegen die Bundesrepublik Deutschland 7
3.2. Strafbarkeiten durch den Einsatz von Software zur Ausspähung von Daten 8

4. Internationale Nachrichtendienstkooperationen 10

1. Überblick

Geheimdienstliche Aktivitäten ausländischer Nachrichtendienste in Deutschland sind als Ausübung fremder Staatsgewalt grundsätzlich unzulässig, sofern die Bundesrepublik sie nicht gestattet. Eine Gestattung oder Duldung entsprechender Überwachungsaktivitäten bedarf wegen ihrer Grundrechtsrelevanz einer Rechtsgrundlage. Dem geltenden Nachrichtendienstrecht lässt sich eine solche nicht entnehmen. Was geregelt ist, ist der Austausch von Informationen zwischen deutschen und ausländischen Nachrichtendiensten. Diese Form der Kooperation zwischen Nachrichtendiensten ist jedoch von Überwachungsaktivitäten ausländischer Nachrichtendienste in Deutschland zu unterscheiden, welche sogar strafbar sein können.

Im Folgenden wird der Regelungsrahmen in Bezug auf Überwachungsaktivitäten ausländischer Nachrichtendienste in Deutschland einschließlich gegebenenfalls einschlägiger Straftatbestände, insbesondere auch mit Blick auf den Einsatz von Spähsoftware, vorgestellt (unter 2. und 3.). Abschließend werden einige in der Praxis etablierte Kooperationsformate zwischen Nachrichtendiensten verschiedener Staaten dargestellt (unter 4.).

2. Verfassungsrechtliche Voraussetzungen und Regelungen des BNDG

Werden ausländische Nachrichtendienste informationserhebend in Deutschland tätig, so üben diese ausländische Staatsgewalt auf dem Hoheitsgebiet des deutschen Staates aus.[1] Ein solches Vorgehen eines fremden Staates ohne Einwilligung der Bundesrepublik ist grundsätzlich unzulässig.[2] Diese ist kraft grundrechtlicher Schutzpflichten verpflichtet, unzulässige Beeinträchtigungen der Grundrechte in Deutschland durch andere Staaten zu verhindern bzw., wenn sie fremden Staaten die Ausübung von Hoheitsgewalt in Deutschland gestattet, für ein grundrechtskonformes Handeln Sorge zu tragen.[3] So ist der deutsche Staat etwa mit Blick auf Art. 10 Abs. 1 GG verpflichtet, die Integrität des laufenden Telekommunikationsverkehrs zu schützen, und zwar sowohl vor Beeinträchtigungen durch Private also auch durch ausländische Staaten.[4] Darüber hinaus wird der deutsche Staat durch das in Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG verbürgte Recht auf informationelle Selbstbestimmung als Ausgestaltung des allgemeinen Persönlichkeitsrechts verpflichtet, auch personenbezogene Daten außerhalb des laufenden Telekommunikationsvorgangs zu schützen.[5] Diese Schutzpflichten bestehen gleichermaßen gegenüber deutschen Staatsangehörigen sowie Staatsangehörigen der Europäischen Union oder von Drittstaaten. Denn die in Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG und Art. 10 Abs. 1 GG verbürgten Grundrechte sind sog. „Jedermann-

---

1 Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 1 Rn. 62.

2 Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 1 Rn. 62; vgl. auch Wissenschaftliche Dienste des Bundestages, WD 2, Ausarbeitung mit dem Titel „Gewinnung von Telekommunikationsinformationen durch ausländische Nachrichtendienste aus völkerrechtlicher Sicht“, S. 6, auf Deutsch abrufbar unter: https://www.bundestag.de/resource/blob/412670/c420dddbab7e3af7c35e40e62582fc06/WD-2-083-13-pdf-data.pdf

3 Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 1 Rn. 62.

4 Ewer/Thienel, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30 (34).

5 Lachenmann, DÖV 2016, 501 (504 f.).

Grundrechte“[6]: Ihr Schutzbereich ist anders als z.B. bei der Berufsfreiheit, die in Art. 12 Abs. 1 GG nur Deutschen Rechte zuspricht, nicht an eine bestimme Nationalität gebunden.

Im Zuge seiner Rechtsprechung zur Ausland-Ausland-Fernmeldeaufklärung[7] nach dem Bundesnachrichtendienstgesetz hat das Bundesverfassungsgericht den rechtlichen Rahmen für die Zusammenarbeit mit ausländischen Nachrichtendiensten sowie zum Tätigwerden ausländischer Nachrichtendienste im Inland formuliert, der der Dimension staatlicher Schutzpflichten gerecht wird:

> Ein funktionierender Informationsaustausch kann im Interesse des verfassungsrechtlich gebotenen Schutzes der Menschen eine Übermittlung von ihm Inland erhobenen Erkenntnissen voraussetzen und im Gegenzug auf Unterrichtungen durch ausländische Stellen angewiesen sein […].
>
> Eine **Zusammenarbeit bei der Telekommunikationsüberwachung** muss allerdings so gestaltet sein, dass der **grundrechtliche Schutz gegenüber heimlichen Überwachungsmaßnahmen** und die diesbezüglichen Anforderungen an die Datenerhebung, -verarbeitung und -übermittlung **nicht unterlaufen** werden. Das gilt insbesondere für den Schutz vor Inlandsüberwachung, der nicht durch einen freien Austausch mit Erkenntnissen aus auf Deutschland bezogenen Überwachungsmaßnahmen ausländischer Dienste um seine Wirkung gebracht werden darf. Ein solcher „**Ringtausch**“ ist insoweit verfassungsrechtlich nicht zulässig. Entsprechendes gilt aber auch für die grundrechtlichen Anforderungen an den Bundesnachrichtendienst hinsichtlich der Fernmeldeaufklärung im Ausland.
>
> Danach darf **ausländischen Diensten** selbst die **Befugnis zu Überwachungsmaßnahmen** vom Inland aus allenfalls dann eingeräumt oder diesbezüglich eine Duldungszusage erteilt werden, wenn hierzu ein **bestimmter Anlass** besteht und durch **detaillierte Rechtsgrundlagen** die **uneingeschränkte Geltung des Grundrechtsschutzes** materiell-rechtlich und prozedural gesichert ist.[8]

In der Folge hat der deutsche Gesetzgeber zwar das Gesetz über den Bundesnachrichtendienst novelliert, hierin aber im Abschnitt 4, Unterabschnitt 3 nur die Kooperation mit ausländischen öffentlichen Stellen im Rahmen der strategischen Ausland-Fernmeldeaufklärung geregelt. Schon nach der Unterabschnittsüberschrift „Ausland-Fernmeldeaufklärung“ ist damit gerade nicht die Informationsgewinnung ausländischer Dienste im deutschen Inland erfasst. Dafür spricht auch § 31 Abs. 1 Satz 2 BNDG, der erklärt, dass die Kooperation sich nicht auf die Erhebung von Daten deutscher Staatsangehöriger, inländischer juristischer Personen und sich im Bundesgebiet aufhaltender Personen erstreckt.

Etwas anderes ergibt sich auch nicht aus § 31 Abs. 1 Satz 3 i. V. m. § 19 Abs. 7 Satz 6 BNDG. Danach dürfen bei Kooperationen des Bundesnachrichtendiensts mit ausländischen öffentlichen Stellen personenbezogene Daten deutscher Staatsangehöriger, inländischer juristischer Personen

---

6 Starck, in: v. Mangoldt/Klein/Starck, GG, 7. Auflage 2018, Art. 1 Rn. 205.

7 BVerfGE 154, 152.

8 BVerfGE 154, 152 (279 f. Rn. 246 f.) – Hervorhebungen nur hier.

und sich im Bundesgebiet aufhaltender Personen nur verarbeitet werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Verarbeitung der Daten eine erhebliche Gefahr für Leib, Leben oder Freiheit einer Person, die Sicherheit des Bundes oder eines Landes oder die Sicherheit anderer Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages abgewendet werden können. Dies setzt zwar eine faktische Erhebung von personenbezogenen Daten deutscher Staatsangehöriger, inländischer juristischer Personen und sich im Bundesgebiet aufhaltender Personen durch eine ausländische öffentliche Stelle voraus. Daraus lässt sich jedoch gerade nicht auf das informationserhebende Tätigwerden einer ausländischen öffentlichen Stelle auf deutschem Territorium schließen. In § 31 Abs. 1 Satz 3 i. V. m. § 19 Abs. 7 Satz 6 BNDG ist daher auch keine dies gestattende Rechtsgrundlage zu sehen.

Zwar erfordert § 28 Abs. 1 BNDG, der dem Bundesnachrichtendienst gestattet, ausländische öffentliche Stellen zur Durchführung strategischer Aufklärungsmaßnahmen zu ersuchen, ein tatsächliches Tätigwerden ausländischer Nachrichtendienste im Rahmen der Durchführung strategischer Aufklärungsmaßnahmen auf Ersuchen des Bundesnachrichtendienstes. Selbst wenn aber hierunter auch das Tätigwerden im Inland erfasst wäre – wogegen die Überschrift des Unterabschnitts 1 „Verarbeitung von personenbezogenen Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung“ spricht –, stellt § 28 Abs. 1 BNDG jedenfalls keine Rechtsgrundlage für das selbstständige, d.h. durch fremde Staaten initiierte, informationsbeschaffende Tätigwerden ausländischer Nachrichtendienste dar.

Eine Rechtsgrundlage für die Tätigkeit ausländischer Nachrichtendienste in Deutschland findet sich damit nicht.

3. Strafrechtliche Regelungen

Die Strafbarkeit einer ausländischen, gegen die Bundesrepublik Deutschland gerichteten geheimdienstlichen Tätigkeit, die unter Einsatz von informationstechnischen Mitteln wie einer Spähsoftware erfolgt, hängt maßgeblich von den **Umständen des Einzelfalles** ab. Im Folgenden sollen daher lediglich allgemeine strafrechtliche Implikationen aufgezeigt werden, die für eine Strafbarkeit im Einzelfall gelten könnten.

Grundsätzlich sieht das Strafgesetzbuch (StGB)[9] in den §§ 93-101a StGB Straftatbestände zum Landesverrat und der Gefährdung der äußeren Sicherheit vor, die auch die geheimdienstliche Tätigkeit ausländischer Staaten unter Einsatz informationstechnischer Systeme erfassen können. Daneben können wegen des Einsatzes von Software zum Ausspähen von Daten insbesondere Strafbarkeiten nach den §§ 202a, 202b, 202c und 303a StGB vorliegen.

9 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), das zuletzt durch Artikel 4 des Gesetzes vom 04.12.2022 (BGBl. I S. 2146) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/stgb/StGB.pdf (Stand dieser sowie sämtlicher nachfolgender Internetquellen: 13.12.2022).

3.1. Strafbarkeit geheimdienstlicher Tätigkeiten von ausländischen Staaten gegen die Bundesrepublik Deutschland

Die Straftatbestände der §§ 94-97 StGB knüpfen an ein **Staatsgeheimnis** als Tatobjekt an. Staatsgeheimnisse sind gemäß § 93 Abs. 1 StGB Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden. Betrifft die Tätigkeit eines fremden Geheimdienstes ein solches Staatsgeheimnis, könnte im Einzelfall eine Strafbarkeit wegen des **Auskundschaftens von Staatsgeheimnissen gemäß § 96 Abs. 1 StGB** in Betracht kommen. Danach wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft, wer sich ein Staatsgeheimnis verschafft, um es zu verraten. Als Verschaffen im tatbestandlichen Sinne gelten neben dem Erwerb, Diebstahl und dem Anfertigen von fotografischen oder handschriftlichen Kopien auch sämtliche Formen der Cyberkriminalität.[10] Der Täter muss dabei in der Absicht eines Verrats gemäß § 94 StGB handeln. Ein solcher Verrat kann gemäß § 94 Abs. 1 Nr. 1 StGB insbesondere in der Mitteilung eines Staatsgeheimnisses an eine fremde Macht bestehen, wenn dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland begründet wird. Dabei ist jedoch zu beachten, dass die bloße Entgegennahme eines Staatsgeheimnisses durch die Mitarbeiter eines fremden Geheimdienstes den Anforderungen eines Verrats nach § 94 StGB nicht genügt.[11] Vielmehr muss ihr Verhalten über eine bloße Entgegennahme hinausgehen; erst dann kann im Einzelfall ein Verrat nach § 94 StGB vorliegen, den der Täter des § 96 StGB beabsichtigen muss.[12] Ohne Einfluss auf eine Strafbarkeit wegen des Auskundschaftens und Mitteilens von Staatsgeheimnissen ist hingegen der Tatort, denn gemäß § 5 Nr. 4 StGB erstreckt sich die Deutsche Strafgewalt auch auf Delikte, deren Tatort im Ausland liegt.

Betrifft die geheimdienstliche Tätigkeit hingegen **kein Staatsgeheimnis**[13], kann im Einzelfall eine Strafbarkeit wegen einer **geheimdienstlichen Agententätigkeit nach § 99 StGB** in Betracht kommen. Nach § 99 Abs. 1 Nr. 1 StGB wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wer für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit gegen die Bundesrepublik Deutschland ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist. Der Straftatbestand ist weit gefasst, um die vielfältig denkbaren Tätigkeiten fremder Geheimdienste erfassen zu können und die Interessen der Bundesrepublik Deutschland umfassend zu schützen.[14] Den Tatbestand erfüllen dabei nur solche geheimdienstlichen Tätigkeiten, die sich gegen die Bundesrepublik Deutschland richten, denn

---

10 Ellbogen, in: Heintschel/Heinegg (Hrsg.), Beck'scher Onlinekommentar zum StGB, 55. Edition, Stand: 01.11.2022.

11 Hegmann/Stuppi, in: Münchener Kommentar zum StGB, 4. Auflage 2021, § 94 StGB, Rn. 6.

12 Ebenda.

13 Die Strafbarkeit des § 99 Abs. 1 StGB wird nach ihrem ausdrücklichen Wortlaut im Wege der gesetzlich angeordneten Konkurrenz durch Strafbarkeiten nach den §§ 94, 96 Abs. 1, 97a, 97b StGB verdrängt.

14 Safferling/Rückert, Schutz vor Dissidenten und Abwehr von Cyberspionage – die neue Bedeutung des § 99 StGB, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2020, 367 (369).

der Schutz der Interessen fremder Staaten wird nicht bezweckt.[15] Täter des § 99 StGB kann jedermann sein, auch ein Mitarbeiter eines fremden Geheimdienstes.[16] Für deren Strafbarkeit ist es wiederum ohne Belang, ob sie ihre geheimdienstliche Tätigkeit aus dem Ausland verfolgen (§ 5 Nr. 4 StGB). Das Ausüben einer geheimdienstlichen Tätigkeit setzt eine aktive Tätigkeit und die Bereitschaft, sich funktionell in die Spionageaktivitäten eines fremden Geheimdienstes einzugliedern, voraus.[17] Dadurch soll grundsätzlich jedes Verhalten erfasst werden, das die Aktivitäten eines fremden Geheimdienstes fördert.[18] Folglich kann die geheimdienstliche Tätigkeit insbesondere auch in dem heimlichen Eindringen in Informationssysteme jeglicher Art bestehen.[19] Der Tatbestand setzt nicht voraus, dass die Tätigkeit von längerer Dauer oder auf Dauer angelegt sein muss.[20] Denn gerade im Bereich der Cyberspionage können bereits durch kurzfristige Tätigkeiten größere Datenmengen erlangt werden.[21] Jedoch muss die Tätigkeit zielgerichtet zugunsten des Geheimdienstes einer fremden Macht erfolgen. Geheimdienste sind dabei Einrichtungen, die aus fremden Machtbereichen Informationen beschaffen, sammeln und auswerten und regelmäßig konspirative Methoden einsetzen.[22] Die Struktur und Organisation dieser Dienste sind unerheblich, entscheidend ist, dass sie staatlichen Zwecken dienen.[23] Begünstigte fremde Mächte können neben sämtlichen ausländischen Staaten auch zwischen- und überstaatliche Einrichtungen sowie Machtgebilde sein, die staatliche Aufgaben wahrnehmen oder wahrnehmen wollen.[24]

3.2. Strafbarkeiten durch den Einsatz von Software zur Ausspähung von Daten

Ungeachtet geheimdienstspezifischer Strafbarkeiten kann auch der Einsatz von Mitteln zur Ausforschung informationstechnischer Systeme als solcher strafbar sein. Dies gilt insbesondere dann, wenn die Täter zugunsten fremder Geheimdienste **Spähsoftware** einsetzen.

Der Einsatz von Software, die zur Ausforschung fremder informationstechnischer Systeme bestimmt ist, kann im Einzelfall eine Strafbarkeit wegen des **Ausspähens von Daten gemäß § 202a StGB** begründen. Danach wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft,

---

15 Ebenda, 371.

16 Ebenda, 379.

17 Barthe/Schmidt, in: Leipziger Kommentar StGB, Band 7 §§ 90-121, 13. Auflage 2020, § 99 StGB, Rn. 3; Safferling/Rückert, a.a.O., 382.

18 Barthe/Schmidt, a.a.O.; Rn . 3.

19 Safferling/Rückert, a.a.O., 383, 384.

20 Barthe/Schmidt, a.a.O.; Rn . 3; Safferling/Rückert, a.a.O., 381.

21 Safferling/Rückert, a.a.O., 381, 382.

22 Barthe/Schmidt, a.a.O., Rn. 5a; Safferling/Rückert, a.a.O., 380.

23 Ebenda.

24 Safferling/Rückert, a.a.O., 380.

wer unbefugt sich oder anderen Zugang zu Daten, die nicht für ihn bestimmt und gegen die unbefugte Verwendung besonders gesichert sind, unter Umgehung ebendieser Zugangssicherung verschafft. Daten im tatbestandlichen Sinne sind nur solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind (§ 202a Abs. 2 StGB). Ein Verschaffen solcher Daten ist grundsätzlich anzunehmen, wenn der Täter tatsächliche Herrschaft über den Ursprungsdatenträger erlangt, die Daten zur Kenntnis nimmt, Kopien der Daten anfertigt oder sie anderweitig aufzeichnet.[25] Dabei muss der Täter besondere Sicherungen gegen eine unberechtigte Verwendung der Daten umgehen. Eine besondere Sicherung gegen eine unbefugte Verwendung liegt vor, wenn der Verfügungsberechtigte sein Interesse an einer Geheimhaltung der Daten durch Sicherungen dokumentiert hat, etwa indem Passwörter oder besondere Schutzprogramme einen unberechtigten Zugriff erschweren.[26] Werden Daten aus informationstechnischen Systemen beschafft, ist eine tatbestandliche Umgehung etwa anzunehmen, wenn sogenannte Trojaner-Programme installiert werden oder bestehende Sicherheitslücken ausgenutzt werden.[27]

Werden durch den Einsatz einer Spähsoftware hingegen Daten abgefangen, die nicht durch besondere Sicherungen vor einem fremden Zugang geschützt sind, kommt eine Strafbarkeit wegen des **Abfangens von Daten gemäß § 202b StGB** in Betracht. Danach wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe unter anderem bestraft, wer unbefugt sich oder einem anderen unter Anwendung technischer Mittel nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung verschafft, soweit die Tat nicht bereits durch andere Straftatbestände mit schwererer Strafe bedroht ist. Das Verschaffen der Daten kann während jeder Datenübermittlung über Telefon, E-Mail, Kommunikationsprogramme oder während der Nutzung von Zwischenspeichern im Internet geschehen.[28] Voraussetzung ist jedoch, dass der Übertragungsvorgang nichtöffentlich ist.[29] Technische Mittel zur Verschaffung der Daten können sowohl Vorrichtungen zur Erfassung und Aufzeichnung als auch spezielle Softwares zum Abfangen von Daten sein.[30]

§ 202c Abs. 1 StGB stellt darüber hinaus bereits die **Vorbereitung** von Straftaten nach den §§ 202a, 202b StGB unter Strafe. Danach wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer eine Straftat nach den §§ 202a, 202b StGB vorbereitet, indem er entweder Passwörter und sonstige Sicherungscodes für Daten oder Computerprogramme zur Begehung von Taten nach den §§ 202a, 202b StGB herstellt, sich oder anderen verschafft, verkauft, überlässt, verbreitet oder sonst zugänglich macht.

---

25 Graf, in: Münchener Kommentar zum StGB, a.a.O., § 202a StGB, Rn. 56.

26 Bundesgerichtshof (BGH), Beschluss vom 27.07.2017, Az.: 1 StR 412/16, Neue Zeitschrift für Strafrecht (NStZ) 2018, 401 (403); Eisele, in: Schönke/Schröder (Hrsg.), Strafgesetzbuch, 30. Auflage 2019, § 202a StGB, Rn. 14; Graf, a.a.O., §202a StGB Rn. 35.

27 Eisele, a.a.O., Rn. 20.

28 Graf, a.a.O., § 202b StGB, Rn. 9.

29 Ebenda, Rn. 10.

30 Ebenda, Rn. 18.

Im Einzelfall kann schließlich eine Strafbarkeit wegen einer **Datenveränderung gemäß § 303a Abs. 1 StGB** vorliegen. Danach wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Geschützt ist die unversehrte Verwendbarkeit der Daten.[31] Demnach setzen alle Tathandlungen eine Einwirkung auf die Daten voraus; das bloße unerlaubte Kopieren von Daten ist hingegen nicht tatbestandsmäßig.[32]

4. Internationale Nachrichtendienstkooperationen

Unter den Nachrichtendiensten verschiedener Staaten haben sich einige Kooperationsformate herausgebildet, die laut Presseberichten unter folgenden Bezeichnungen bekannt sind: „5 Eyes“, „Five Eyes Plus“ „Nine Eyes“, „14 Eyes“, „Maximator“ und der „Berner Club“.

Das „Five Eyes“- Abkommen besteht hiernach seit 1946 und baut auf der Zusammenarbeit seiner Mitglieder Australien, Kanada, Neuseeland, dem Vereinigten Königreich und den Vereinigten Staaten während des Zweiten Weltkrieges auf.[33] Das Abkommen ist bei „Five Eyes Plus“ erweitert um Frankreich, Deutschland und Japan bei der Abwehr von Bedrohungen durch China oder Russland, während Frankreich, Japan und Südkorea zum Informationsaustausch über militärische Aktivitäten Nordkoreas kooperieren.[34] Das „Nine Eyes“-Abkommen wiederum stellt eine Vergrößerung der „5 Eyes“-Partnerschaft dar, und zwar um Dänemark, Frankreich, die Niederlande und Norwegen.[35] Das „14 Eyes“-Abkommen umfasst neben den „9 Eyes“-Partnern auch Belgien, Deutschland, Italien, Spanien und Schweden.[36]

Als „Maximator“ wird eine nachrichtendienstliche Zusammenarbeit zwischen Dänemark, Deutschland, Frankreich, den Niederlanden und Schweden, der seit 1976 besteht.[37] Der „Berner Club“ hingegen ist ein informeller Zusammenschluss aller Direktoren der Inlandsgeheimdienste

---

31 Wieck-Noodt, in: Münchener Kommentar zum StGB, a.a.O., § 303a StGB, Rn. 2.

32 Hecker, in: Schönke/Schröder (Hrsg.), a.a.O., § 303a StGB, Rn. 8.

33 „Geheimbund "Five Eyes": Der exklusive Club der Geheimdienste“, in: Tagesspiegel vom 5. Juli 2013, auf Deutsch abrufbar unter: https://www.tagesspiegel.de/politik/der-exklusive-club-der-geheimdienste-6361585.html.

34 “Five Eyes intel group ties up with Japan, Germany, France to counter China in cyberspace”, in: the Mainichi vom 4. Februar 2019, auf Englisch abrufbar unter: https://mainichi.jp/english/articles/20190204/p2a/00m/0na/001000c, “Five Eyes’ Countries Eye Expanded Cooperation Amid North Korea Challenges“, in: The Diplomat vom 28. Januar 2020, auf Englisch abrufbar unter: https://thediplomat.com/2020/01/five-eyes-countries-eye-expanded-cooperation-amid-north-korea-challenges/.

35 „NSA-GCHQ Snowden leaks: A glossary of the key terms“, in: BBC News Technology vom 28. Januar 2014, auf Englisch abrufbar unter: https://www.bbc.co.uk/news/technology-25085592.

36 „NSA-GCHQ Snowden leaks: A glossary of the key terms“, in: BBC News Technology vom 28. Januar 2014, auf Englisch abrufbar unter: https://www.bbc.co.uk/news/technology-25085592.

37 „Maximator: European signals intelligence cooperation, from a Dutch perspective“, in: Taylor & Francis Online 35/2020, auf Englisch abrufbar unter: https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538.

der EU-Mitgliedstaaten sowie von Großbritannien, Norwegen und der Schweiz, der 1969 initiiert wurde.[38]

Soweit sich deutsche Nachrichtendienste an diesen Kooperationen beteiligen, muss sich dies im Rahmen der oben geschilderten verfassungs- und einfachrechtlichen Anforderungen halten.

***

38 „So spionierte die Schweiz mit Israel Araber aus“, in Tages-Anzeiger vom 07.02.2016, auf Deutsch abrufbar unter https://www.tagesanzeiger.ch/so-spionierte-die-schweiz-mit-israel-araber-aus-137721698366.