9.4 Internationales Übereinkommen über die Cyberkriminalität

Die Schweiz hat 2011 das Internationale Übereinkommen über die Cyberkriminalität (CCC)[227] der Mitgliedstaaten des Europarats und anderen Staaten ratifiziert. Es beruht auf der Feststellung, dass die modernen Kommunikations- und Datenverarbeitungstechnologien eine Herausforderung für die Bekämpfung der Computer- und Internetkriminalität darstellen. Elektronische Daten werden, unabhängig vom Herkunfts- oder Aufbewahrungsort, innert Sekunden an beliebige Empfänger (Personen und Einrichtungen) auf der ganzen Welt versandt. In Computersystemen gespeicherte Informationen können einem bestimmten oder unbestimmten Personenkreis zugänglich gemacht, gezielt gesucht und entsprechend heruntergeladen werden. Staatsgrenzen bilden für den Informationsfluss im Internetzeitalter keine Hindernisse mehr: Die neuen Technologien führen in steigendem Masse dazu, dass Ausgangspunkte und Ziele von deliktischem Verhalten geographisch weit auseinanderliegen können. Da der Anwendungsbereich der staatlichen Gesetzgebungen demgegenüber vom Territorialitätsgrundsatz begrenzt wird, muss die Strafverfolgung im Bereich des Cybercrime über adäquate Instrumente des internationalen Strafrechts unterstützt werden[228].

Die international vereinheitlichten und spezifizierten Instrumente des Cybercrime-Übereinkommens versuchen insbesondere den Umständen Rechnung zu tragen, dass förmliche Rechtshilfeverfahren sich regelmässig aufwändig, kompliziert und langwierig gestalten und diverse Staaten keine oder nur eine relativ kurze Vorratsdatenspeicherung in Bezug auf die rückwirkende Erhebung von Randdaten des elektronischen Fernmeldeverkehrs kennen. Deshalb droht der Ablauf der gesetzlichen Überwachungsfrist, bevor über ein hängiges Rechtshilfegesuch entschieden werden konnte. Das Übereinkommen sieht diesbezüglich spezifische Instrumente vor, darunter die vorsorgliche umgehende Sicherung gespeicherter Computerdaten im Hinblick auf ein späteres Rechtshilfeersuchen[229], die umgehende Weitergabe von Verkehrsdaten, welche aufgrund eines vorsorglichen Ersuchens gesichert wurden[230] sowie den direkten grenzüberschreitenden Zugriff in jenen Fällen, bei denen ein Berechtigter (etwa ein ausländischer Internetservice-Provider[231]) der Datenerhebung zugestimmt hat[232].

Eine ähnliche Stossrichtung zur Beschleunigung der internationalen Rechtshilfe im Cyberbereich verfolgt Thomas Hansjakob in seinem Standardwerk zum Überwachungsrecht der Schweiz. Er postuliert, dass Erkenntnisse aus Überwachungen des Fernmeldeverkehrs bereits vor Abschluss des entsprechenden Verfahrens aus präventiven Gründen laufend an den ersuchenden Staat weitergegeben werden können, die

---

227 Übereinkommen über die Cyberkriminalität, abgeschlossen in Budapest am 23. November 2011, von der Bundesversammlung genehmigt am 18. März 2011, in Kraft getreten für die Schweiz am 1. Januar 2012 (SR 0.311.32).

228 Vgl. Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, BBl 2010, S. 4700.

229 Art. 29 CCC.

230 Art. 30 CCC.

231 Zustimmungs- und weiterleitungsberechtigt sind namentliche ausländische Internetprovider bzw. Anbieter von sozialen Netzwerken, welche sich in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien ein solche Weiterleitungsrecht an in- und ausländische Strafverfolgungsbehörden gegenüber ihren Kunden ausbedungen haben; vgl. BGE 141 IV 108 E. 5.9 und 5.10.

232 Art. 32 lit. b CCC.

Erkenntnisse im Strafverfahren gegen den Gefährder aber nicht verwendet werden dürfen[233].

Mit der Ratifizierung des Übereinkommens über die Cyberkriminalität hat sich die Schweiz gegenüber ausländischen Staaten u.a. verpflichtet, Computerdaten im Hinblick auf ein späteres Rechtshilfeersuchen – und damit bereits vor dem Vorliegen eines formellen Gesuchs – umgehend zu sichern sowie die gesicherte Randdaten umgehend weiterzugeben, auch wenn das Rechtshilfeverfahren noch nicht abgeschlossen ist[234]. Es erstaunt deshalb, dass die schweizerische Gesetzgebung sich gegenüber ausländischen Staaten zur Einräumung von Erleichterungen verpflichtet hat, diese aber dem eigenen Nachrichtendienst verwehrt. Gewiss; auch für die umgehende Sicherung von Computerdaten und die Weitergabe von Randdaten an einen ausländischen Staat im Rahmen eines Strafverfahrens bedarf es der Genehmigung durch das Zwangsmassnahmengericht, da sich die Beschaffung der Daten nach dem Recht des ersuchten Staats richtet[235]. Während aber die Strafverfolgungsbehörden die Überwachung schon vor der gerichtlichen Genehmigung anordnen können, können die auf das NDG gestützten genehmigungspflichtigen Beschaffungsmassnahmen erst vollzogen werden, wenn gerichtliche Genehmigung und politische Freigabe vorliegen. Dem NDB müsste deshalb zumindest die Möglichkeit eingeräumt werden, Computerdaten umgehend, d.h. vor Abschluss des Genehmigungs- und Freigabeprozesses, sichern zu lassen und zur Erkennung und Abwehr von Bedrohungen auch verwenden zu können (siehe dazu Ziffer 9.6.2, Seite 75).

9.5 Besonderheiten der Informationsbeschaffung durch Cyber NDB

9.5.1 Spezifische Informationsbedürfnisse

Während den Strafverfolgungsbehörden eine grosse Palette unterschiedlicher Personal- und Sachbeweise[236] zur Verfügung steht, konzentrieren sich die Erkenntnisquellen von Cyber NDB weitgehend [redacted]. Wie der Chef NDBI ausführte, hat die Aufklärung des Netzwerkverkehrs mit der eigentlichen nachrichtendienstlichen Tätigkeit nichts zu tun. Hier gehe es darum, modi operandi zu erkennen, Angriffe zu lokalisieren, die verwendete Software zu lesen und Rückschlüsse auf Urheber, Herkunftsland und Ausrichtung des Angriffs zu erkennen[237].

Durchaus vergleichbar mit einem rechtsmedizinischen Institut oder einem kriminaltechnischen Dienst der Polizei interessiert sich Cyber NDB nicht primär für die hinter einem Angriff stehenden Personen, sondern für die technischen Mittel und Methoden, die dabei zum Einsatz gelangen. Dem für den Angriff benutzten Medium Internet entsprechend, greift Cyber NDB nicht auf den (in der Regel verschlüsselten) Inhalt von Meldungen

233 Thomas Hansjakob, Überwachungsrecht der Schweiz, Zürich 2018, Rz. 1343).

234 Erachtet die ausführende Behörde das Ersuchen als ganz oder teilweise erledigt, erlässt sie eine begründete Verfügung über die Gewährung und den Umfang der Rechtshilfe (Art. 80d des BG über die internationale Rechtshilfe in Strafsachen (IRSG), welche den ordentlichen Rechtsmitteln unterliegt (Art. 80e IRSG). Eine vorzeitige Übermittlung von Informationen oder Beweismitteln ist nur ausnahmsweise möglich (Art. 80d[bis] IRSG).

235 Vgl. Art. 18b des BG über die internationale Rechtshilfe in Strafsachen (IRSG).

236 Siehe dazu Art. 139 ff. StPO.

237 Anhörung [redacted], S. 10.

zurück; entscheidend für seine Analysen sind die Modalitäten des Datenverkehrs als solche. Allein aus den Kommunikationswegen, der Art und Weise der Kommunikation, den eingesetzten Mitteln, der Komplexität der Datenstrukturen und aufgrund weiterer Besonderheiten des Datenverkehrs versucht Cyber NDB, Rückschlüsse auf die mögliche Herkunft des Angriffs sowie auf dessen Motive und Ziele zu ziehen, um daraus Abwehrszenarien entwickeln zu können. Die von Cyber NDB benötigten und bearbeiteten Daten des Netzwerkverkehrs sind vorwiegend, wenn nicht ausschliesslich technischer Natur. Sie geben Auskunft über die IP-Adressen der Kommunikationspartner sowie über den Zeitpunkt, die Dauer und die technischen Merkmale der Verbindung. Ein Personenbezug ist im Rahmen der technischen Analyse des Netzwerkverkehrs nicht gegeben und für Cyber NDB auch nicht von Interesse. Dieser kann sich allenfalls bei der späteren operativen Einordnung der technischen Erkenntnisse in den nachrichtendienstlichen Kontext ergeben (siehe dazu Ziffer 6.3, Seite 34).

9.5.2 Zeitliche Dringlichkeit

Bei der Erkennung von Cyberangriffen kommt dem Zeitfaktor eine entscheidende Bedeutung zu. Zu Beginn liegen nur vage Anhaltspunkte, aber noch keine konkreten Hinweise vor, was unter Berücksichtigung der vom Gesetz verlangten Anforderungen für genehmigungspflichtige Beschaffungsmassnahmen, d.h. eine konkrete Bedrohung[238]), zu zusätzlichen Problemen führen kann. Bestehen konkrete Hinweise, ist der Angriff bereits im Gange, sodass es für eine erfolgreiche Abwehr vielfach schon zu spät ist.

Zwischen dem Beginn eines Angriffs und seiner Entdeckung können bis zu mehreren Monaten verstreichen[239]: So geht etwa aus dem von MELANI erstellten Technischen Bericht über den Spionagefall bei der RUAG hervor, dass zwischen den ersten Angriffshandlungen und den ersten Hinweisen auf einen Angriff rund 15 Monate verstrichen waren. Wie die Mitarbeitenden von Cyber NDB erklärten, geht einem Angriff meistens eine längere Vorbereitungszeit voraus, in der das Opfer ausgeforscht wird und der Angreifer nach möglichen Eintrittsvektoren sucht. Diese Vorbereitungshandlungen erfolgen meistens unterhalb der Entdeckungsschwelle. Der Angreifer hat auch alles Interesse, möglichst lange von Schwachstellen profitieren zu können und Informationen abzuschöpfen. Dies ist ihm aber nur möglich, solange der Angriff nicht erkannt wird. Auch Angreifer wissen um den kritischen Faktor Zeit und wechseln deshalb ihre Infrastruktur oder ihre Angriffsmuster, sodass die Abwehr eigentlich immer nur hinterherhinken kann[240].

Der Chef NDBI betonte denn auch, dass – verglichen mit den klassischen Betätigungsfeldern wie etwa unerlaubtem Nachrichtendienst, Nonproliferation, Gewaltextremismus etc. – bei der Cyberabwehr vor allem die zeitliche Komponente entscheidend ist: Cyber sei extrem schnell, d.h. die Informationen seien sehr volatil, sodass man rasch reagieren müsse[241]. [redacted] vertrat gar den Standpunkt, dass eine effiziente Bekämpfung von Cyberangriffen unter dem Regime der genehmigungspflichtigen Beschaffungsmassnahmen nicht mehr möglich sei. Die Wege seien zu lang und zu

238 Art. 27 Abs. 1 lit. a NDG.

239 Technischer Bericht über den Spionagefall bei der RUAG vom 23. Mai 2016 (https://www.govcert.ch/whitepapers/apt-case-ruag-technical-report-govcert-ch/). (https://www.ncs.admin.ch/ncs/de/home/dokumentation/berichte/fachberichte/technical -report_apt_case_ruag.html).

240 Anhörung [redacted] S. 4;

241 Anhörung [redacted], S. 3.

kompliziert: [redacted] Die Erfahrung zeige zudem, dass die Akteure die Command and Control Server (C2-Server) in zwei, maximal vier Wochen auswechseln, um nicht entdeckt zu werden. Bis also nur schon der Antrag für eine Operation stehe, dürfte der Server längst gewechselt und meistens auch gelöscht sein[242]. In die gleiche Richtung argumentierte [redacted] und erachtete eine Anpassung der gesetzlichen Grundlagen für die Beschaffung von Netzwerkverkehrsdaten als unerlässlich. Die heutigen Bestimmungen über die genehmigungspflichtigen Beschaffungsmassnahmen seien nicht zielführend, weil deren Anforderungen am Anfang der Aufklärungstätigkeit praktisch nie erfüllt werden könnten[243].

[redacted]

9.5.3 Relevanz der technischen Analyse Cyber NDB für die Strafverfolgung

Aus der präventiven Ausrichtung des Nachrichtendienstes ergibt sich, dass seine Befugnisse auf die frühzeitige Erkennung und Verhinderung von Bedrohungen der inneren oder äusseren Sicherheit beschränkt sind. Die von ihm zur Erfüllung seiner Aufgabe beschafften Informationen sind primär auf dieses Ziel ausgerichtet, auch wenn sie allenfalls sekundär noch für andere Behörden in anderen Verfahren von Bedeutung sein können. So sieht das Gesetz vor, dass der NDB andere Dienststellen des Bundes und der Kantone unter Wahrung des Quellenschutzes über Vorgänge und Erkenntnisse informiert, welche die gesetzlichen Aufgaben dieser Stellen bei der Wahrung der inneren oder äusseren Sicherheit betreffen[244]. Ergeben sich Anhaltspunkte auf ein möglicherweise strafbares Verhalten, zählt zu diesen anderen Dienststellen insbesondere die Bundesanwaltschaft (BA) in ihrer Eigenschaft als Strafverfolgungsbehörde des Bundes[245], soweit für die Verfolgung der entsprechenden Delikte die Bundesgerichtsbarkeit[246] gegeben ist. Dies ist insbesondere bei unerlaubtem Nachrichtendienst, dem Hauptbetätigungsfeld von Cyber NDB, der Fall.

Cyber NDB befasst sich weitgehend, wenn nicht ausschliesslich mit Angriffen, die auf Spionage ausgerichtet sind und von staatlichen Akteuren ausgehen. Für nichtstaatliche

---

242 Anhörung [redacted] S. 8.
243 Anhörung [redacted], S. 11.
244 Art. 6 Abs. 3 NDG.
245 Art. 2 Abs. 1 des Strafbehördenorganisationsgesetzes (StBOG).
246 Art. 23f. StPO.

Akteure, etwa Cyberkriminelle, bei denen primär die Identifizierung des individuellen Angreifers im Vordergrund steht, sind das NCSC zusammen mit MELANI oder die Kantone zuständig; dort kommen auch die Strafverfolgungsbehörden ins Spiel[247]. Soweit in diesen Fällen im Rahmen einer eröffneten Strafuntersuchung die Daten des Netzwerkverkehrs erhoben werden, ist deren Analyse auf die Verfolgung des mutmasslichen Täters ausgerichtet. Sie führt in der Regel nicht nur zu einem Eingriff in die Persönlichkeitsrechte des mutmasslichen Täters, sondern zieht für diesen – falls ihm die Tat nachgewiesen werden kann – auch strafrechtliche Folgen nach sich. Dies ist mitzuberücksichtigen, wenn sich die Frage nach der sachlichen Rechtfertigung für eine von den strafprozessualen Normen abweichende Regelung des Beizugs von Randdaten durch Cyber NDB stellt. Die Administrativuntersuchung ging deshalb auch der Frage nach, ob und wie weit die Analyseergebnisse von Cyber NDB Eingang in spätere Strafverfahren gefunden haben.

[redacted][250].

Im Rahmen der Administrativuntersuchung wurde bei der Bundesanwaltschaft eine schriftliche Auskunft zu den vom NDB im Zusammenhang mit Cyberspionage erstellten Amtsberichten eingeholt. Laut ihrem Bericht[251] hatte der NDB in den Jahren 2015 bis 2020 im Zusammenhang mit unerlaubtem Nachrichtendienst und Cyber insgesamt [redacted] Amtsberichte zuhanden der BA erstellt. Zum Teil wurden sie auf Ersuchen der BA verfasst. Ob die Berichte u.a. auf der Auswertung von Netzwerkverkehrsdaten beruhten, war für die BA nicht ersichtlich. [redacted]

[redacted][252].

247 Anhörung [redacted], S. 31.
248 Anhörung [redacted], S. 15.
249 Anhörung [redacted], S. 13.
250 Anhörung [redacted] S. 7.
251 Antwort der BA auf das Auskunftsersuchen in der Administrativuntersuchung 30.06.2022.
252 Das Verfahren wird namentlich dann sistiert, wenn die Täterschaft oder ihr Aufenthaltsort unbekannt ist oder andere vorübergehende Verfahrenshindernisse bestehen (Art. 314 Abs. 1 StPO). Es wird u.a. dann eingestellt, wenn: kein Tatverdacht erhärtet ist, der eine Anklage rechtfertigt (Art. 319 Abs. 1 StPO.

[redacted]

Die Tätigkeit von Cyber NDB ist zwar für die international koordinierte Erkennung und Abwehr von Cyberangriffen von hoher Bedeutung, aber für die Strafverfolgung von weitgehend fehlender Relevanz: In keinem der von Cyber NDB in den Jahren 2015 bis 2020 mittels der Analyse von Daten des Netzwerkverkehrs aufgedeckten Fälle kam es zu einer strafrechtlichen Anklage oder zu einem Strafbefehl, geschweige denn zu einer Verurteilung des oder der Täter. Es zeigt sich somit auch hier, dass eine möglichst weitgehende Übereinstimmung präventiver und repressiver Informationsbeschaffungsmassnahmen im Hinblick darauf, dass deren Ergebnisse beiden Zwecken dienen können, nicht zwingend erforderlich ist. Auch unter diesem Gesichtspunkt liesse es sich ohne weiteres rechtfertigen, das Verfahren zur Erlangung von Netzwerkverkehrsdaten – jedenfalls sowie diese für die Erkennung und Abwehr von Cyberangriffen verwendet werden sollen – wesentlich zu vereinfachen und im Gegenzug in Kauf zu nehmen, dass sie in einem späteren Strafverfahren nicht verwendet werden können.

9.5.4 Schweiz-Bezug und internationale Dimension der Cyberabwehr

Der Zuständigkeitsbereich des NDB – und damit auch von Cyber NDB – beschränkt sich nach geltendem Recht grundsätzlich auf den Schutz wichtiger Landeinstessen i.S.v. Art. 2 NDG. Nachdem die Informationsbeschaffung und -bearbeitung des NDB im Wesentlichen dem frühzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz i.S.v. Art. 6 Abs. 1 NDG dient, kann Cyber NDB nur aktiv werden, wenn ein hinreichender Bezug der Bedrohung zur Schweiz oder zu Schweizer Interessen gegeben ist. Dies ist – so weit im vorliegenden Zusammenhang relevant – immer dann der Fall, wenn der Angriff von staatlichen Akteuren zum Zweck des politischen Nachrichtendienstes zum Nachteil der Schweiz erfolgt oder sich gegen kritische Infrastrukturen der Schweiz richtet.

Liegen erste Hinweise auf einen Angriff vor, ist in der Regel wenig über den Angreifer und die Zielrichtung des Angriffs bekannt. Dementsprechend schwer fällt es zu diesem Zeitpunkt, konkrete Anhaltspunkte für den geforderten Schweiz-Bezug zu nennen. Erst die weiteren Abklärungen können zeigen, wer Urheber des Angriffs sein könnte und auf welche Ziele er gerichtet ist. Hinzu kommt, dass Cyberangriffe sich nicht an Landesgrenzen orientieren und der geografische Standort der dafür eingesetzten Infrastruktur vielfach zufällig ist. Meistens laufen die Angriffe über verschiedene Stationen in unterschiedlichen Ländern ab. Die von den Angriffen ausgehende Bedrohung kann zwar gezielt auf die Interessen eines einzelnen Landes gerichtet sein; in aller Regel stellen aber insbesondere die auf Spionage zielenden Angriffe eine Bedrohung für ganze geopolitische Regionen dar.

---

253 Nach Art. 66 Abs. 1 StBOG bedarf die Verfolgung politischer Straftaten einer Ermächtigung durch den Bundesrat. Dieser kann sie zur Wahrung der Interessen des Landes verweigern.

Erfolgen Cyberangriffe auf ausländische Staaten oder Organisationen über in der Schweiz gelegene Server oder Zwischen-Server, sind einstweilen nur ausländische Interessen unmittelbar betroffen. Trotzdem hat die Schweiz ein existentielles Interesse daran, an der internationalen Abwehr von Cyberangriffen mitzuwirken, selbst wenn diese nicht unmittelbar die Schweiz betreffen, aber unter (Mit-)Benutzung schweizerischer Infrastrukturen erfolgen. Die bisherige Gesetzgebung und die darauf beruhende Rechtsprechung des Bundesverwaltungsgerichts zur Genehmigung geheimer Beschaffungsmassnahmen verlangen aber für ein Tätigwerden des Nachrichtendienstes eine unmittelbare Bedrohung der inneren oder äusseren Sicherheit der Schweiz und werden damit der spezifischen internationalen Natur von Cyberangriffen nur beschränkt gerecht.

Es ist deshalb sehr zu begrüssen, dass mit der laufenden Revision des Nachrichtendienstgesetzes der Rechtswirklichkeit Rechnung getragen wird und die Feststellung, Beobachtung und Beurteilung von sicherheitspolitisch bedeutsamen Vorgängen auf das Ausland und auf den gesamten Cyberraum ausgedehnt werden soll[254]. Folgerichtig soll auch bei den genehmigungspflichtigen Überwachungsmassnahmen der strikte Bezug zu einer konkreten und unmittelbaren Bedrohung der Sicherheitsinteressen der Schweiz gelockert werden.

Der Vorentwurf sieht vor, dass der NDB genehmigungspflichtige Überwachungsmassnahmen auch dann anordnen kann, wenn eine konkrete Bedrohung wichtiger internationaler Sicherheitsinteressen gegeben ist und zudem internationales Handeln unerlässlich ist, wenn die Nichtaufklärung zu negativen Reaktionen der betroffenen Staaten gegenüber der Schweiz führen oder eine schwere Bedrohung der Sicherheit der Schweiz selbst zur Folge haben könnte[255]. Damit soll sichergestellt werden, dass Kommunikationsvorgänge zwischen Personen, die die internationale Sicherheit schwer bedrohen und aus technischen Gründen (etwa bedingt durch den Standort des Servers) über die Schweiz kommunizieren, abgeklärt werden können. Nur nebenbei wird im erläuternden Bericht zum Vorentwurf erwähnt, dass eine Kooperationsfähigkeit der Schweiz in einer umgekehrten Konstellation auch die internationale Kooperationsbereitschaft zu Gunsten der Sicherheit der Schweiz fördern kann.

Mit der vorgeschlagenen Ausdehnung des Zuständigkeitsbereichs des NDB auf die Datenbeschaffung und -bearbeitung zu sicherheitspolitischen Vorgängen im Ausland und im Cyberraum dürfte ein Teil der von Cyber NDB gegen die Tauglichkeit des Einsatzes genehmigungspflichtiger Beschaffungsmassnahmen vorgebrachten Bedenken (siehe dazu Ziffer 9.5.2, Seite 68) ausgeräumt sein. Gelöst sind damit aber keineswegs sämtliche Probleme, die sich im Zusammenhang mit der Genehmigungspflicht bzw. mit dem Genehmigungsverfahren stellen können.

---

254 Art. 6 Abs. 1 lit. b Vorentwurf zur Revision des Nachrichtendienstgesetzes vom 18. Mai 2022 (VE-NDG); siehe auch Art. 19 Abs. 2 lit. f und Art. 20 Abs. 1 lit. i VE-NDG (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-88899.html).

255 Art. 27 Abs. 1 lit. a VE-NDG (siehe dazu auch die Hinweise zur bisherigen Rechtsprechung des BVGer im erläuternden Bericht des Bundesrates zur Revision des Nachrichtendienstgesetzes (Fn. 51), S. 11).

9.6 Revision der genehmigungspflichtigen Beschaffungsmassnahmen

9.6.1 Verzicht auf das Genehmigungserfordernis für Randdaten

Das NDG sieht einheitliche Voraussetzungen und ein einheitlich geregeltes Verfahren für genehmigungspflichtige Beschaffungsmassnahmen vor. Es unterscheidet – im Unterschied zur Strafprozessordnung – nicht zwischen der eigentlichen Überwachung des Inhalts der Kommunikation und dem Beizug der Verbindungsdaten (Randdaten) des Fernmelde- oder Netzwerkverkehrs[256]. Das Bundesgericht anerkennt zwar, dass auch die Speicherung und Aufbewahrung sowie die Beschaffung und Auswertung der Verkehrsdaten einen Eingriff in die Grundrechte des Betroffenen darstellen. Es relativiert aber die Schwere des Grundrechtseingriffs, da die Daten nicht den Inhalt der Kommunikation betreffen, sondern nur die Kommunikationswege zum Gegenstand haben[257]. Der damit verbundene Eingriff in das Fernmeldegeheimnis wiegt deshalb bei Randdaten "deutlich weniger schwer" als in den Fällen der inhaltlichen Kommunikationsüberwachung[258]. Bildet aber die Schwere des Eingriffs das entscheidende Kriterium für besondere Schutzmassnahmen, ist nicht nachvollziehbar, weshalb – jedenfalls im Strafverfahren – Eingriffe in das Fernmeldegeheimnis einer gerichtlichen Genehmigung bedürfen, Eingriffe in das ebenfalls verfassungsrechtlich geschützte Hausrecht (etwa mit einer Hausdurchsuchung) aber einfach verfügt werden können. An der Heimlichkeit der Massnahme allein kann es nicht liegen, da auch andere Ermittlungen ohne Kenntnis des Betroffenen erfolgen[259].

Die Rechtsprechung tendiert auch anderweitig zu einer Relativierung des absoluten Schutzes von Randdatenerhebungen. So verzichtet das Bundesgericht auf die Einhaltung des Genehmigungserfordernisses, falls "nur" die auf dem Speicher des jeweiligen Kommunikationsgeräts bereits angefallenen und gespeicherten Daten ausgewertet werden sollen[260]. Dies ist selbst dann nicht genehmigungspflichtig, wenn die Staatsanwaltschaft zu diesem Zweck beim Dienst ÜPF die Herausgabe des PUK-Codes verlangt[261]. In einem anderen Entscheid hat das Bundesgericht die Frage offengelassen, ob für Zwecke des Strafverfahrens Verkehrsdaten des Fernmeldeverkehrs nur unter Einhaltung der für genehmigungspflichtige Beschaffungsmassnahmen geltenden Vorschriften eingeholt werden dürfen. Es hat die Verwertbarkeit der von der Staatsanwaltschaft direkt beim Betreiber der hausinternen Vermittlungsanlage beigezogenen Daten allein unter dem Gesichtspunkt des öffentlichen Interesses und der Verhältnismässigkeit, nicht aber auch unter demjenigen der geheimen Beschaffungsmassnahmen geprüft und deren Verwertbarkeit im konkreten Einzelfall mangels dringendem Tatverdacht und fehlender Verhältnismässigkeit verneint[262].

---

256 Während die inhaltliche Überwachung des Post- und Fernmeldeverkehrs nur bei Vorliegen eines dringenden Tatverdachts auf einer der in Art. 269 Abs. 2 StPO im Einzelnen aufgelisteten Straftatbestände (Katalogtaten) zulässig ist, genügt für die Erhebung der blossen Randdaten der dringende Verdacht auf irgendein Verbrechen oder Vergehen (Art. 273 Abs. 1 StPO). In beiden Fällen bedarf jedoch die Anordnung des Staatsanwaltes der Genehmigung durch das Zwangsmassnahmengericht.

257 BGE 144 I 126 E. 4 und 5; BGE 142 IV 34 E. 4.3.2.

258 BGE 139 IV 98 E. 4.2.

259 Vgl. etwa Art. 95 Abs. 2 StPO für die Beschaffung von Personendaten.

260 BGE 143 IV 270 E.4.6; vgl. auch BGE 140 IV 181 E. 2.

261 BGE 141 IV 423 E. 1.

262 BGer 1B_26/2016 E.4.2-4.4.

Angesichts des hohen Schadenspotentials eines Angriffs und der geringen Eingriffsintensität der Beschaffung und Auswertung von Netzwerkverkehrsdaten, der vorwiegend technischen und nicht personenbezogenen Analyse der beigezogenen Daten, der zeitlichen Dringlichkeit und der weitgehend fehlenden Relevanz der auf diesem Weg gewonnenen Erkenntnisse für ein allfälliges Strafverfahren sowie in Berücksichtigung der präventiven Ausrichtung des Nachrichtendienstes und in Abstimmung mit dem aktuellen Stand der Gesetzbebung zur internationalen Zusammenarbeit auf dem Gebiet der Cyberabwehr, erscheint es gerechtfertigt und zugleich erforderlich, die Beschaffung von Netzwerkverkehrsdaten durch Cyber NDB – jedenfalls soweit diese allein der Erkennung und Abwehr von Cyberangriffen dient – wesentlich zu vereinfachen.

Letztlich wird die Politik entscheiden müssen, welche Prioritäten sie im Bereich der Cyberabwehr setzen will: Strebt sie eine effiziente Früherkennung und Abwehr von Angriffen an oder bevorzugt sie eine spätere, wenn auch keineswegs sichere Strafverfolgung der Täterschaft im Rahmen eines den Grundsätzen der Strafprozessordnung entsprechenden Strafverfahrens?

Eine erste Alternative könnte darin bestehen, die bisherige Praxis von Cyber NDB zu "legalisieren" und die Bestimmungen des NDG über die genehmigungspflichtigen Beschaffungsmassnahmen dahingehend abzuändern, dass der bestehende Art. 25 NDG (besondere Auskunftspflichten von Privaten) um einen neuen Absatz 3 ergänzt und dem NDB die Befugnis eingeräumt wird, bei Betreiberinnen und Betreibern von Infrastrukturen, die den Zugang zum Internet ermöglichen, Aufzeichnungen über den Netzwerkverkehr direkt und ohne Einhaltung der Bestimmungen über die genehmigungspflichtigen Beschaffungsmassnahmen zu beziehen. Dies liesse sich ohne weiteres rechtfertigen, nachdem Art. 25 NDG ohnehin schon Beschaffungsmassnahmen vorsieht, welche in die Persönlichkeitsrechte der Betroffenen (insbesondere in Bezug auf Aufzeichnungen von Bildübertragungs- und Bildaufzeichnungsgeräten) eingreifen. Rechtsstaatlichen Bedenken könnte Rechnung getragen werden, indem die auf diesem Weg gewonnenen Erkenntnisse in einem allfälligen späteren Strafverfahren als Beweismittel nicht verwendet werden dürfen. Ein neuer Art. 25 Abs. 3 NDG könnt in etwa wie folgt lauten:

> Bestehen hinreichende Anhaltspunkte, dass eine Bedrohung der inneren oder äusseren Sicherheit über das Internet begangen wird oder worden ist, kann der NDB die Anbieterinnen von Fernmeldediensten verpflichten, alle Angabe, insbesondere Aufzeichnungen des Netzwerkverkehrs, zu liefern, welche die Identifikation der Urheberschaft oder Herkunft ermöglichen[263]. Das Verfahren der genehmigungspflichtigen Beschaffungsmassnahmen (Art. 26 ff. NDG) ist nicht anwendbar. Die aus der Analyse des Netzwerkverkehrs gewonnenen Erkenntnisse können in einem späteren Strafverfahren nicht verwertet werden.

Zugleich müsste in Art. 26 Abs. 1 lit. a NDG ein entsprechender Vorbehalt angebracht werden:

> [1]Die folgenden Beschaffungsmassnahmen sind genehmigungspflichtig:
> a. Überwachungen des Postverkehrs und des Fernmeldeverkehrs und Verlangen von Randdaten des Postverkehrs und des Fernmeldeverkehrs gemäss BÜPF;

263 Vgl. Art. 22 BÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet und zur Identifikation von Personen bei Bedrohungen der inneren oder äusseren Sicherheit).

vorbehalten bleibt die Beschaffung von Randdaten aufgrund besonderer Auskunftspflichten Privater nach Art. 25 dieses Gesetzes.

9.6.2 Beschleunigung des Genehmigungs- und Freigabeverfahrens

Wird die skizzierte Lösung als zu weitgehend erachtet, drängen sich zumindest Korrekturen im Hinblick auf eine Beschleunigung des Anordnungs- und Genehmigungsverfahrens auf. Insbesondere muss dem NDB ermöglicht werden, eine Randdatenerhebung unverzüglich anzuordnen und den gerichtlichen Genehmigungs- und den politischen Freigabeprozess erst im Nachhinein in die Wege zu leiten. Dieses Vorgehen ist schon deshalb erforderlich, damit die Daten – auch im Sinne des Übereinkommens über die Cyberkriminalität – umgehend gesichert werden können und nicht in der Zeitspanne zwischen dem Antrag auf Anordnung der Massnahme und dem Abschluss des Genehmigungsverfahrens "verloren" gehen.

Nach geltendem Recht kann die vom NDB angeordnete geheime Beschaffungsmassnahme erst vollzogen werden, nachdem der gerichtlichen Genehmigungs- und der politische Freigabeentscheid vorliegen[264] (siehe dazu Ziffer 9.2, Seite 62). Zwischen den ersten Anzeichen auf einen Cyberangriff und der Beschaffung der für eine Analyse unerlässlichen Netzwerkverkehrsdaten können somit Tage und Wochen, wenn nicht – falls die Genehmigungsinstanz eine Ergänzung der Akten oder weitere Abklärungen verlangt[265] – Monate verstreichen (siehe dazu Ziffer 9.5.2, Seite 68).

Im Unterschied zum NDB kann die Staatsanwaltschaft im Strafverfahren, welches auf die Verfolgung eines mutmasslichen Täters und nicht auf die Abwehr eines Angriffs ausgerichtet ist und damit in der Regel zeitlich weniger dringlich ist, geheime Überwachungsmassnahmen in eigener Kompetenz anordnen und über den Dienst ÜPF sofort vollziehen lassen. Ernst nach ihrer Anordnung reicht sie diese samt Begründung und den wesentlichen Verfahrensakten innert 24 Stunden dem für die Genehmigung zuständigen Zwangsmassnahmengericht ein[266]. Das NDG sieht zwar bei Dringlichkeit vor, dass die Direktorin oder der Direktor NDB den sofortigen Einsatz von genehmigungspflichtigen Beschaffungsmassnahmen anordnen kann und erst nach erfolgter Anordnung das Bundesverwaltungsgericht und die Vorsteherin oder den Vorsteher des VBS orientiert[267]. Diese Regelung ist jedoch auf Ausnahmefälle zugeschnitten[268] und soll nicht zum Normalfall werden

Weil bei den auf Randdaten beschränkten genehmigungspflichtigen Beschaffungsmassnahmen zur Erkennung oder Abwehr eines Cyberangriffs immer eine zeitliche Dringlichkeit gegeben ist, drängt sich auf, das Verfahren für die Beschaffung von Netzwerkaufzeichnungen analog zu den im Strafprozess geltenden Grundzügen zu regeln, jedenfalls wenn es ausschliesslich um die technische Analyse eines Cyberangriffs geht. Dies scheint umso eher gerechtfertigt, als bei dieser Art von Beschaffungsmassnahmen nicht der Kommunikationsinhalt überwacht, sondern lediglich Verkehrsdaten beigezogen

---

264 Art. 27 Abs. 2 NDG.
265 Vgl. Art. 29 Abs. 5 NDG.
266 Vgl. Art. 274 Abs. 1 StPO.
267 Art. 31 Abs. 1 NDG.
268 Botschaft zum Nachrichtendienstgesetz (Fn. 201), BBl 2014, 2163.

werden und sich demzufolge der Eingriff nach der Praxis des Bundesgerichts als "deutlich weniger einschneidend" erweist[269]. Unter diesem Aspekt liesse es sich gar überlegen, dem NDB generell (und nicht nur beschränkt auf die Erkennung und Abwehr von Cyberangriffen) die Möglichkeit einzuräumen, Randdatenerhebungen selbstständig anzuordnen und die erforderlichen Genehmigungen erst nachträglich einzuholen.

In diesem Sinn könnte ein neuer Abs. 31bis NDG eingeführt werden:

> Beschränkt sich die geheime Beschaffungsmassnahme auf Randdaten (und dienen diese allein der technischen Analyse eines Cyberangriffs), kann der NDB den sofortigen Vollzug anordnen. Im Übrigen richtet sich das Verfahren zur nachträglichen Einholung der gerichtlichen Genehmigung und der politischen Freigabe nach Art. 31 dieses Gesetzes.

269 BGE 142 IV 34 E. 4.3.2; BGE 139 IV 98 E. 4.2.

10 Strafrechtliche Relevanz der Vorkommnisse im Ressort Cyber NDB

10.1 Beurteilung durch die interne Untersuchung des NDB

In der internen Untersuchung des NDB wurde der externen Anwaltskanzlei nicht nur der Auftrag erteilt, eine allgemeine Auslegeordnung zur Rechtmässigkeit der Vorkommnisse bei Cyber NDB vorzunehmen, sondern auch eine Antwort zur allfälligen strafrechtlichen Relevanz dieser Vorgänge erwartet[270]. Der Bericht der Anwaltskanzlei äussert sich auf mehr als zehn Seiten zu Straftatbeständen, die möglicherweise – sei es durch Mitarbeitende der Internet-Service-Provider, welche auf freiwilliger Basis Netzwerkverkehrsdaten aufgezeichnet und an den NDB herausgegeben haben, sei es durch Mitarbeitende des NDB, welche die Provider um die Herausgabe von Netzwerkverkehrsdaten ersucht, diese erhalten und bearbeitet haben – erfüllt sein könnten[271]. Zugleich betonen die Verfasserinnen und Verfasser aber auch, dass sie sich mangels Expertise auf dem Gebiet des Strafrechts auf summarische Aussagen beschränken müssen[272].

Im Einzelnen werden im Bericht folgende Straftatbestände als möglicherweise erfüllt erachtet:

- unerlaubte Datenbeschaffung (Art. 143 StGB);
- unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB;
- Verletzung des Fernmeldegeheimnisses (Art. 321ter StGB);
- weitere Delikte gegen die Privatsphäre bzw. den Geheim- und Privatbereich (Art. 179 ff. StGB);
- Teilnahme durch Anstiftung

Die Ausführungen zur strafrechtlichen Relevanz sind sehr abstrakt gehalten. Die Verfasserinnen und Verfasser des Berichts beschränken sich vorwiegend darauf, die gesetzlichen Straftatbestände im Wortlaut wiederzugeben und anschliessend den aktuellen Stand von Lehre und Rechtsprechung darzustellen. Gestützt auf eine vorwiegend theoretische Analyse der Rechtslage gelangen sie zum Ergebnis, dass die von ihnen genannten Straftatbestände erfüllt sein oder jedenfalls nicht ausgeschlossen werden könnten. Die Tathandlung erblicken sie darin, dass die Provider Daten des Netzwerkverkehrs, welche dem Fernmeldegeheimnis unterliegen, ohne Einhaltung der Vorschriften über die geheimen Beschaffungsmassnahmen und damit ohne Vorliegen eines Rechtfertigungsgrundes[273] beschafft und an Cyber NDB herausgegeben haben. Die Mitarbeitenden von Cyber NDB ihrerseits sollen sich mit ihren Anfragen an die Provider möglicherweise der Anstiftung, wenn nicht gar der Mittäterschaft zu den genannten Delikten schuldig gemacht haben.

---

270 Rechtsgutachten (Fn. 17), RZ 11, S. 7 f. Ziffer 2.1.2, Position 5 und Position 11c.

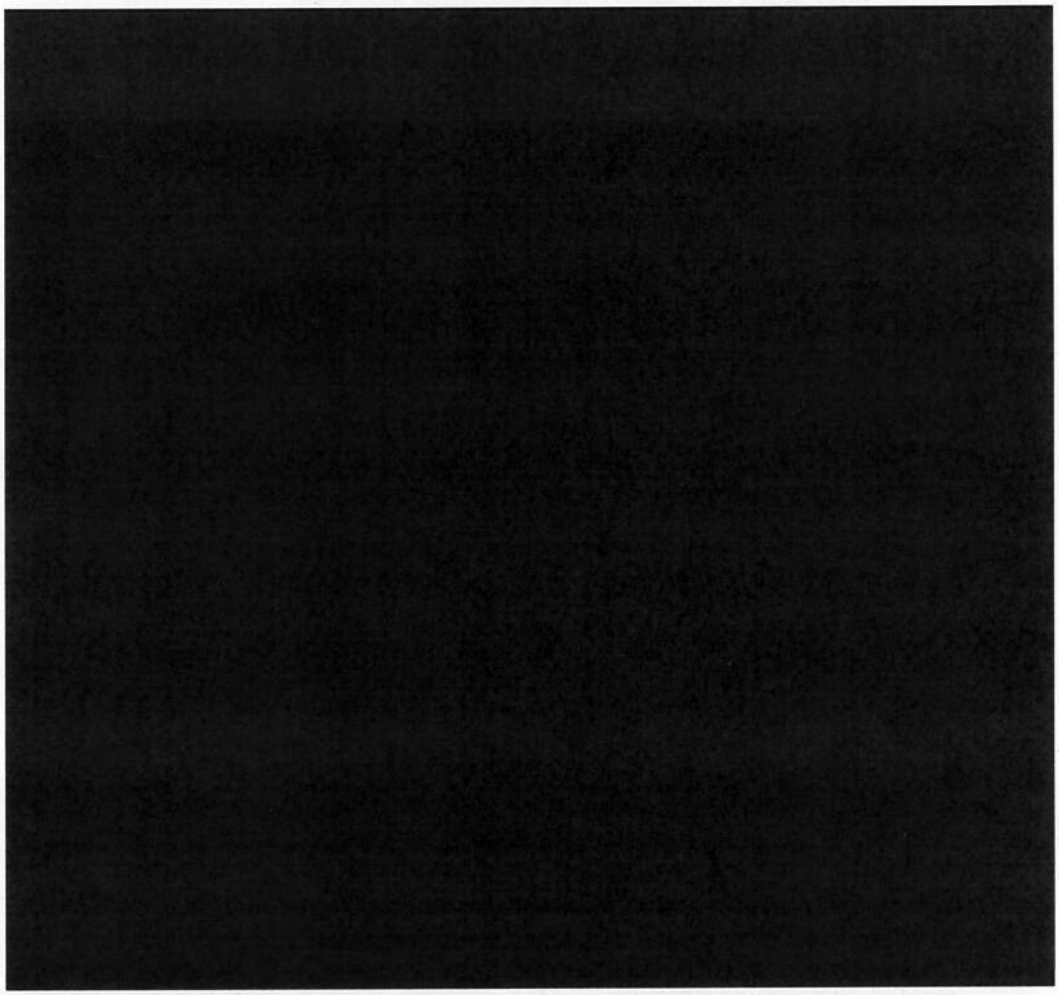
271 Rechtsgutachten (Fn. 17), Rz. 141-148, S. 49-53 und Rz. 260-303, S. 86-96.

272 Rechtsgutachten (Fn. 17), Rz. 141, S. 49.

273 Art. 14 StGB: Wer handelt, wie es das Gesetz gebietet oder erlaubt, verhält sich rechtmässig, auch wenn die Tat nach diesem oder einem anderen Gesetz mit Strafe bedroht ist.

Art. 179^{octies} StGB: Wer in Ausübung ausdrücklicher, gesetzlicher Befugnisse die Überwachung des Post- und Fernmeldeverkehrs einer Person anordnet oder durchführt oder technische Überwachungsgeräte (Art. 179bis StGB) einsetzt ist nicht strafbar, wenn unverzüglich die Genehmigung des zuständigen Richters eingeholt wird.

Im Bericht werden die Erkenntnisse zur möglichen strafrechtlichen Relevanz wie folgt zusammengefasst[274]:



10.2 Allgemeine Vorbemerkungen zur strafrechtlichen Relevanz

Es kann nicht Aufgabe einer Administrativuntersuchung sein, das Verhalten von Privatpersonen, die ausserhalb der Bundesverwaltung stehen, unter strafrechtlichen Gesichtspunkten zu beurteilen. Dies ist allein den Strafverfolgungsbehörden und Gerichten vorbehalten. Die nachfolgenden Bemerkungen beschränken sich deshalb auf mögliche Straftatbestände, die Mitarbeitenden des NDB zur Last gelegt werden könnten, und äussern sich nicht zu allfälligen strafrechtlichen Konsequenzen, die sich für die Mitarbeitenden der Internet-Service-Provider ergeben könnten. Nachdem aber hinsichtlich der Mitarbeitenden des NDB vorwiegend, wenn nicht ausschliesslich eine strafbare Beteiligung (Mittäterschaft, Anstiftung oder Gehilfenschaft[275]) zur Diskussion steht, wird es trotzdem unumgänglich sein, auch zu den einzelnen Straftatbeständen Stellung zu nehmen.

---

274 Rechtsgutachten (Fn. 17), Rz. 300 ff., S. 95 f.

275 Art. 24 f. StGB.

Die Ausführungen zur strafrechtlichen Relevanz im Bericht der externen Anwaltskanzlei bewegen sich auf einer sehr hohen Abstraktionsebene. Es wird – anders als in einem konkreten Strafverfahren – nicht auf tatsächliche Vorkommnisse im Sinne realer Lebenssachverhalte abgestellt. Ausgangslage der Beurteilung bilden die vom NDB vorgegebenen hypothetischen Fallbeispiele und abstrakten Fragestellungen. Die Verfasserinnen und Verfasser arbeiten deshalb vorwiegend mit Hypothesen. Ihre theoretischen Ausführungen zu einer möglichen Strafbarkeit geben zwar den aktuellen Stand von Lehre und Rechtsprechung zu den einzelnen Straftatbeständen korrekt wieder. Sie beziehen sich aber von vornherein nur auf die objektiven Tatbestandselemente und lassen im Übrigen – den Vorgaben entsprechend – sowohl die Besonderheiten eines realen Lebenssachverhalts wie auch die sich im Zusammenhang mit dem subjektiven Tatbestand ergebenden Fragestellungen (Vorsatz und Irrtum) weg. Die Frage nach einer allfälligen strafrechtlichen Haftung der Vorgesetzten (Begehen durch pflichtwidriges Untätigbleiben[276]) wird schon gar nicht aufgeworfen. Bezeichnenderweise äussert sich der Bericht denn auch nicht dazu, wer mit welcher Handlung oder Unterlassung konkret welchen Straftatbestand erfüllt haben könnte; die Verfasserinnen und Verfasser lassen es auch diesbezüglich bei der pauschalen Aussage „die Internet-Service-Provider" bzw. „der NDB" bewenden.

Aussagen zu prozessualen Fragestellungen, etwa zum hinreichenden Tatverdacht als Voraussetzung für die Eröffnung eines Strafverfahrens, finden sich nicht. Aus den Ausführungen muss geschlossen werden, dass die Verfasserinnen und Verfasser den Standpunkt vertreten, dass Anhaltspunkte für die Erfüllung des objektiven Tatbestands der im einzelnen aufgeführten Strafbestimmungen gegeben sein könnten, weshalb ein strafbares Verhalten nicht ausgeschlossen werden kann. Für die Eröffnung eines konkreten Strafverfahrens genügt es jedoch nicht, dass ein strafbares Verhalten nicht ausgeschlossen werden kann. Vielmehr wird verlangt, dass ein hinreichender Tatverdacht besteht[277]. Ein solcher liegt vor, wenn nicht bloss eine unbestimmte Möglichkeit für ein strafbares Verhalten gegeben ist, sondern konkrete Anhaltspunkte vorhanden sind. Die zur Eröffnung einer Strafuntersuchung erforderlichen Hinweise auf eine strafbare Handlung müssen erheblich und konkreter Natur sein. Blosse Gerüchte oder Vermutungen genügen nicht. Der Anfangsverdacht soll eine plausible Tatsachengrundlage haben, aus der sich die konkrete Möglichkeit der Begehung einer Straftat ergibt[278].

10.3 Bemerkungen zu den einzelnen Straftatbeständen

10.3.1 Unbefugte Datenbeschaffung (Art. 143 StGB)

Bei sämtlichen im Bericht der externen Anwaltskanzlei aufgelisteten Straftatbestände handelt es sich um Vorsatzdelikte. Bei der unbefugten Datenbeschaffung wird zusätzlich eine Bereicherungsabsicht des Täters verlangt. Selbst wenn der NDB für die Erstellung von Netzwerkaufzeichnungen oder Serverabbildern an einzelne Provider offene oder verdeckte Zahlungen geleistet haben sollte – was jedoch auch in der Administrativuntersuchung nicht nachgewiesen werden konnte (siehe dazu Ziffer 8.4, Seite 43) – ist eine

276 Art. 11 StGB.

277 Nach Art. 309 Abs. 1 der Schweizerischen Strafprozessordnung (StPO; SR 312) eröffnet die Staatsanwaltschaft u.a. eine Untersuchung, "wenn sich aus den Informationen und Berichten der Polizei, aus der Strafanzeige oder aus ihren eigenen Feststellungen ein hinreichender Tatverdacht ergibt".

278 BGer 6B_833/2019 E. 2.4.2.

Bereicherungsabsicht nicht ersichtlich. Die fraglichen Zahlungen – sollten sie denn je nachgewiesen werden können – dienten nach dem heutigen Stand des Wissens allein dazu, den auf Veranlassung des NDB bei den Providern angefallen Zusatzaufwand zu decken. Anhaltspunkte dafür, dass die angeblichen Zahlungen über eine blosse Aufwandsentschädigung hinausgingen, liegen nicht vor – auch wenn man von den Zahlen ausgeht, die der ehemalige Chef Cyber NDB in seiner Aktennotiz festgehalten hat. Eine Bereicherungsabsicht dürfte somit ausgeschlossen werden können. Theoretisch verbliebe die Möglichkeit, dass Zahlungen an eine beim Provider angestellte Kontaktperson geleistet wurden und diese den Betrag nicht zur Abgeltung der dem Provider entstandenen Aufwendungen, sondern im eigenen Interesse verwendet hat. Konkrete Anhaltspunkte dafür liegen aber nicht vor.

10.3.2 Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB)

Unbefugtes Eindringen in ein Datenverarbeitungssystem wird nur auf Antrag bestraft. Das Antragsrecht steht nur der durch die Straftat verletzten Person zu[279]. Es erlischt nach Ablauf von drei Monaten, nachdem der antragsberechtigten Person der Täter bekannt wird[280]. Ein Strafantrag liegt nicht vor, und es ist auch nicht ersichtlich, welche Person ihn realistischerweise stellen könnte[281].

10.3.3 Verletzung des Post- und Fernmeldegeheimnisses (Art. 321ter StGB)

Die Verletzung des Post- und Fernmeldegeheimnisses zählt zu den echten Sonderdelikten. Täter kann nur sein, wer als Beamter, Angestellter oder Hilfsperson einer Organisation, die Post- oder Fernmeldedienstleistungen erbringt, einer Drittperson Angaben über den Post-, Zahlungs- oder den Fernmeldeverkehr der Kundschaft macht, eine verschlossene Sendung öffnet oder ihrem Inhalt nachforscht, oder einem Dritten Gelegenheit gibt, eine solche Handlung zu begehen. Der gleichen Strafandrohung untersteht nach Absatz 2, wer eine nach Absatz 1 zur Geheimhaltung verpflichtete Person durch Täuschung veranlasst, die Geheimhaltungspflicht zu verletzen.

Die Mitarbeitenden des NDB zählen nicht zu dem von Art. 321ter Abs. 1 StGB erfassten Täterkreis. Sie könnten sich deshalb im Sinne von Absatz 2 nur strafbar gemacht haben, wenn sie die Provider durch Täuschung veranlasst hätten, allfällige (eigene) Geheimhaltungspflichten zu verletzten. Ein täuschendes Vorgehen ist nie zur Diskussion gestanden.

Neben der in Art. 321ter Abs. 2 StGB geregelten mittelbaren Täterschaft, bleibt eine Teilnahme am Sonderdelikt in Form der Anstiftung oder Gehilfenschaft möglich, auch wenn dem Anstifter oder Gehilfen die besondere Tätereigenschaft nicht zukommt: er wird aber milder bestraft[282].

---

279 Art. 30 Abs. 1 StGB.

280 Art. 31 StGB.

281 Zur Komplexität des Strafantragsrechts bei Datendelikten vgl. Christine Möhrke-Sobolewski, Gehackte Fahrzeuge, Strafantragsrecht bei Datendelikten in der Schweiz und in Deutschland, Zürich 2021.

282 Art. 26 StGB.

Der Bericht der externen Anwaltskanzlei legt im Zusammenhang mit einer Anstiftung zur Verletzung des Post- und Fernmeldegeheimnisses entscheidendes Gewicht auf einen Entscheid des Bundesgerichts von 2001 in einem Fall von Anstiftung zur Verletzung des Amtsgeheimnisses[283]. Das Bundesgericht entschied, dass zur Verletzung des Amtsgeheimnisses anstiftet, wer wissend, dass der zuständige Bezirksanwalt Angaben über die Vorstrafen von festgenommenen Personen verweigerte, eine Verwaltungsassistentin der Staatsanwaltschaft um entsprechende Auskünfte ersucht, ihr per Fax eine Liste dieser Personen mit der Bitte übermittelt, ihm die entsprechenden Angaben auf Grund der Eintragungen im EDV-Register zu machen, zu dem sie mittels eines Passwortes Zugang hatte, und sie dadurch veranlasst, ihm die geheimen Angaben zukommen zu lassen[284].

Der fragliche Entscheid ist nicht nur in der Lehre auf massive Kritik gestossen[285], sondern führte auch zu einer Verurteilung der Schweiz durch den Europäischen Gerichtshof für Menschenrechte wegen Verletzung der Meinungsäusserungsfreiheit[286]. Auch wenn der Meinungsäusserungsfreiheit im Zusammenhang mit den Aktivitäten von Cyber NDB keine Bedeutung zukommen dürfte, bleibt zu beachten, dass das Bundesgericht bei seinem Entscheid zur strafbaren Anstiftung den Eventualvorsatz[287] sehr sorgfältig geprüft und dabei namentlich berücksichtigt hatte, dass der Anstifter über eine langjährige Erfahrung als Polizei- und Gerichtsberichterstatter verfügte und der zuständige Bezirksanwalt die fraglichen Informationen ihm zuvor ausdrücklich verweigert hatte[288]. Entscheidend war somit weniger die Anfrage als solche, als vielmehr die Tatsache, dass der Täter eine gewisse Raffinesse an den Tag gelegt hatte.

Dieses Kriterium dürfte bei den Anfragen von Cyber NDB an die Provider kaum gegeben sein. [redacted] (siehe dazu Ziffer 7.2, Seite 42), handelte es sich um eine reine Anfrage um freiwillige Herausgabe von Daten. Diese Anfrage beruhte zudem auf der irrtümlichen Annahme, Art. 23 NDG bilde dafür eine genügende gesetzliche Grundlage, und enthielt erst noch den Hinweis, dass nur um die Herausgabe von Daten gebeten werde, die nicht unter das Fernmeldegeheimnis fallen oder zu deren Übermittlung der Kunde ausdrücklich sein Einverständnis zugesichert habe. Die hier zur Diskussion stehende Konstellation unterscheidet sich damit wesentlich vom Sachverhalt, der die Grundlage des erwähnten Bundesgerichtsentscheids gebildet hatte. Von einer vorsätzlichen Bestimmung zur Verletzung des Fernmelde- und Postgeheimnisses, wie sie für eine Anstiftung[289] verlangt würde, kann keine Rede sein.

10.3.4 Delikte gegen den Geheim- oder Privatbereich (Art. 179 ff. StGB)

Die Delikte gegen den Geheim- oder Privatbereich gewähren nicht – wozu auf den ersten Blick der Randtitel allenfalls verleiten könnte – einen umfassenden Schutz der

---

283 Rechtsgutachten (Fn. 17), S. 93 ff.

284 BGE 127 IV 122 E. 2; der Entscheid betraf einen Journalisten des "Blick" und erging im Zusammenhang mit dem seinerzeitigen Fraumünster-Postdiebstahl.

285 Vgl. etwa Felix Bommer, Anstiftung und Selbstverantwortung, plädoyer 03/2002, S. 34 ff.; Franz Riklin, Amtsgeheimnisverletzung durch Journalisten, medialex 2001, S. 160 ff.

286 EGMR 24.04.2006; Requête n° 77551/01.

287 Vorsätzlich handelt bereits, wer die Verwirklichung der Tat für möglich hält und in Kauf nimmt (Art. 12 Abs. 2 StGB.

288 Marc Forster, BSK Strafrecht II, 4. Aufl., Basel 2019, N. 16a zu Art. 24 StGB.

289 Art. 24 Abs. 1 StGB.

Persönlichkeitsrechte der Betroffenen gegen Beeinträchtigungen irgendwelcher Art. Sie erfassen nur einzelne Aspekte des Persönlichkeitsschutzes, insbesondere die Verletzung des Schriftgeheimnisses (Art. 179 StGB), das Abhören und Aufnehmen fremder Gespräche (Art. 179bis StGB), das unbefugte Aufnehmen von Gesprächen (Art. 179ter StGB), die Verletzung des Geheim- oder Privatbereichs durch (Bild-)Aufnahmegeräte (Art. 179^{quater} StGB), das Inverkehrbringen und Anpreisen von Abhör-, Ton- und Bildaufnahmegeräten (Art. 179^{sexties} StGB), den Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB) sowie das unbefugte Beschaffen von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen (Art.179^{novies} StGB). Zugleich sehen sie einen Rechtfertigungsgrund für amtliche Überwachungen vor (Art. 179^{octies} StGB).

Während sich die Verletzung des Schriftgeheimnisses bereits in der ursprünglichen Fassung des StGB von 1937 findet[290], wurden die übrigen Tatbestände 1968 in das Strafgesetzbuch eingefügt und in der Folge teilweise ergänzt. Schutzobjekt von Art. 179 ff. StGB ist nicht der elektronische Datenaustausch, sondern im Wesentlichen allein die Vertraulichkeit des geschriebenen und gesprochenen Wortes sowie das Recht des Einzelnen, sich in seinem Geheim- oder Privatbereich unbehelligt von fremder Beobachtung frei bewegen zu können.

Auch aus den vom internen Untersuchungsteam NDB zuhanden der externen Anwaltskanzlei erstellten hypothetischen Sachverhaltsschilderungen geht nicht hervor, dass Cyber NDB je Abhör-, Ton- oder Bildaufnahmegeräte eingesetzt hatte oder dass es sich bei von Providern bezogenen und bearbeiteten Daten um besonders schützenswerte Personendaten oder Persönlichkeitsprofile gehandelt haben könnte. Ein grosser Teil der Delikte gegen den Geheim- oder Privatbereich fällt deshalb bereits aus diesem Grund ausser Betracht.

Am ehesten liesse sich über eine Verletzung des Schriftgeheimnisses diskutieren. Nach Art. 179 StGB wird bestraft, wer ohne Berechtigung eine verschlossene Schrift oder Sendung öffnet, um von ihrem Inhalt Kenntnis zu nehmen. Elektronisch übermittelte E-Mails, andere Textnachrichten oder gar Datensätze können bereits aufgrund der ursprünglichen gesetzgeberischen Konzeption nicht "Sendung" im Sinne der Strafbestimmung sein[291]. Wer sich unbefugt Zugang zu einem Informatiksystem verschafft, um von (unverschlüsselten) Nachrichten Kenntnis zu erhalten, fällt allein unter den Anwendungsbereich von Art. 143 bzw. Art. 143bis StGB, nicht aber unter denjenigen von Art. 179 StGB. Selbst wenn die gegenteilige Ansicht vertreten werden sollte, bleibt zu beachten, dass vom Schriftgeheimnis nur der gedankliche Inhalt verschlossener Schriften oder Sendungen geschützt ist. Werden Textnachrichten im Klartext übermittelt, sind sie mit einer Postkarte zu vergleichen, und es fehlt von vornherein das Erfordernis des Verschlusses. Werden Textnachrichten mit einem kryptographischen Verfahren verschlüsselt, ist nur strafbar, wer Kenntnis vom Inhalt nimmt. Anhaltspunkte dafür, dass Cyber NDB je Kenntnis von verschlüsselt übermittelten Nachrichten erlangt hat, haben sich weder in er internen Untersuchung noch in der Administrativuntersuchung ergeben. Dementsprechend fallen auch die Delikte gegen den Geheim- oder Privatbereich weg.

---

290 Raffael Ramel/André Vogelsang, BSK Strafrecht II, 4. Aufl., Basel 2019, N. 27f. zu Art. 179 StGB.

291 Die Bestimmung ist bis heute nicht geändert worden (vgl. BBl 1937 III 677).

10.4 Fehlender Vorsatz bzw. Irrtum über die Rechtswidrigkeit

10.4.1 Vorsatz und Irrtum

Letztlich kann es dahingestellt bleiben, ob allenfalls der objektive Tatbestand irgendeiner Strafbestimmung erfüllt sein könnte. Sämtliche im Zusammenhang mit der Datenbeschaffung- oder -bearbeitung durch Cyber in Betracht kommende Straftaten sind als Vorsatzdelikte ausgestaltet. Neben der Erfüllung des objektiven Tatbestands müssten deshalb auch Anhaltspunkte dafür gegeben sein, dass die Mitarbeitenden des NDB vorsätzlich und schuldhaft gehandelt haben.

Bestimmt es das Gesetz nicht ausdrücklich anders, ist nur strafbar, wer ein Verbrechen oder Vergehen vorsätzlich begeht. Vorsätzlich begeht ein Verbrechen oder Vergehen, wer die Tat mit Wissen und Willen ausführt. Vorsätzlich handelt bereits, wer die Verwirklichung der Tat für möglich hält und in Kauf nimmt[292]. Dem Täter müssen somit zum Zeitpunkt der Tat einerseits die Tatumstände bekannt sein; nicht erforderlich ist, dass er sich auch der rechtlichen Qualifikation seines Verhaltens bewusst ist. Andererseits muss er die Tatverwirklichung auch wollen oder sie zumindest in Kauf nehmen.

Handelt der Täter in einer irrigen Vorstellung über den Sachverhalt, liegt ein vorsatzausschliessender Sachverhaltsirrtum vor[293]. In diesem Fall beurteilt das Gericht die Tat zu Gunsten des Täters nach dem demjenigen Sachverhalt, den er sich vorgestellt hat. Weiss der Täter bei Begehung der Tat nicht und kann er nicht wissen, dass er sich rechtswidrig verhält, ist ein Irrtum über die Rechtswidrigkeit gegeben[294]. Dieser schliesst zwar nicht den Vorsatz, aber wegen fehlendem Unrechtsbewusstsein die Schuld aus. Wie bei fehlendem Vorsatz bleibt der Täter auch in diesem Fall straflos.

Verlangt wird, dass der Irrtum über die Rechtswidrigkeit unvermeidbar war. Hätte der Irrtum vermieden werden können, mildert das Gericht die Strafe.

10.4.2 Irrtum über die Rechtswidrigkeit

Ein Irrtum über die Rechtswidrigkeit kann in zwei Varianten gegeben sein. Während der Täter beim direkten Verbotsirrtum die übertretene Verbotsnorm nicht kennt, nimmt er beim indirekten Verbotsirrtum irrig die Existenz eines Rechtfertigungsgrunds an[295]. Ein Irrtum über die Rechtswidrigkeit gilt in der Regel als vermeidbar, wenn der Täter selbst an der Rechtmässigkeit seines Handelns zweifelte oder hätte zweifeln müssen, oder wenn er weiss, dass eine rechtliche Regelung besteht, über deren Inhalt und Reichweite er sich aber nicht genügend informiert. Unvermeidbar ist der Verbotsirrtum, wenn der Täter nicht weiss und nicht wissen kann, dass er rechtswidrig handelt, oder wenn der Irrtum auf Tatsachen beruht, durch die sich auch ein gewissenhafter Mensch hätte in die Irre führen lassen[296]. Diese Regelung beruht auf dem Gedanken, dass sich der dem

---

292 Art. 12 Abs. 1 und 2 StGB.
293 Art. 13 StGB.
294 Art. 21 StGB.
295 Stefan Trechsel/Bijan Fateh-Moghadam, Schweizerisches Strafgesetzbuch Praxiskommentar, 4. Aufl., Zürich 2021, N. 1 zu Art. 21 StGB.
296 BGE 104 IV 217 E. 3a.

Recht Unterworfene um die Kenntnis der Rechtslage zu bemühen hat und deren Unkenntnis nur in besonderen Fällen vor Strafe schützt[297].

Obschon Rechtsunkenntnis in der Regel kein zureichender Grund für Straflosigkeit ist, anerkennt die Rechtsprechung ausnahmsweise einen unvermeidbaren Irrtum über die Rechtswidrigkeit, etwa wenn eine Rechtsfrage zu lösen war, die der Täter wegen ihrer besonderen Natur und erhöhten Komplexität nicht erkennen konnte und deshalb auf die Auskünfte eines eigens dafür beigezogenen Rechtsberaters abstellte[298].

Eine irreführende Auskunft oder Anweisung der zuständigen Behörde bildet regelmässig eine ausreichende Grundlage für einen unvermeidbaren Verbotsirrtum[299]. So ist insbesondere im Verwaltungsrecht anerkannt, dass sich aus dem in Art. 9 BV verankerten Grundsatz von Treu und Glauben eine unrichtige Auskunft einer Behörde an einen Bürger unter gewissen Umständen Rechtswirkungen entfaltet. Voraussetzung dafür ist, dass: a) es sich um eine vorbehaltlose Auskunft der Behörden handelt; b) die Auskunft sich auf eine konkrete, den Bürger berührende Angelegenheit bezieht; c) die Amtsstelle, welche die Auskunft gegeben hat, dafür zuständig war oder der Bürger sie aus zureichenden Gründen als zuständig betrachten durfte; d) der Bürger die Unrichtigkeit der Auskunft nicht ohne Weiteres hat erkennen können; e) der Bürger im Vertrauen hierauf nicht ohne Nachteil rückgängig zu machende Dispositionen getroffen hat; f) die Rechtslage zur Zeit der Verwirklichung noch die gleiche ist wie im Zeitpunkt der Auskunftserteilung; g) das Interesse an der richtigen Durchsetzung des objektiven Rechts dasjenige am Vertrauensschutz nicht überwiegt. Vertrauensschutz setzt also nicht zwingend eine unrichtige Auskunft voraus und lässt sich auch aus einer blossen behördlichen Zusicherung und sonstigem, bestimmte Erwartungen begründendem Verhalten der Behörde herleiten[300].

Die Rechtsprechung zum Vertrauensschutz ist zwar im Verwaltungsrecht entwickelt worden und berührt grundsätzlich nur das Verhältnis zwischen staatlichen Behörden und Individuen. Die darin zum Ausdruck gelangende Interessenabwägung bei der Auslegung des verfassungsrechtlichen Gebots von Treu und Glauben[301] muss aber auch dann Beachtung finden, wenn es um die Frage nach der Vermeidbarkeit bzw. Unvermeidbarkeit eines strafrechtlichen Irrtums geht. Der blosse Umstand, dass in der verwaltungsrechtlichen Rechtsprechung das Verhältnis von Individuum und Staat im Vordergrund steht, und es im vorliegenden Zusammenhang um den Vertrauensschutz von Beamten bzw. öffentlich-rechtlichen Angestellten geht, steht einer analogen Anwendung nichts entgegen. Denn auch im Strafverfahren tritt die beschuldigte Person – unabhängig davon, ob es sich um einen Beamten oder eine Privatperson handelt – den staatlichen Strafbehörden als Individuum gegenüber, sodass sie sich vollumfänglich auf ihre verfassungsmässigen Rechte, insbesondere auch den Vertrauensschutz, berufen kann. Sollte sich im Folgenden zeigen, dass die Mitarbeitenden des NDB in einem Irrtum über die Rechtswidrigkeit gehandelt haben, muss unter dem Aspekt der Vermeidbarkeit dieses Irrtums

297 BGE 129 IV 238 E. 3.1.

298 BGE 98 IV 293 E. 4a.

299 Stefan Trechsel/Bijan Fateh-Moghadam (Fn. 295), N. 11 zu Art. 21 StGB.

300 BGE 143 V 95 E.3.6.2; vgl. dazu Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich 2020, N. 667 ff.; Giovanni Biaggini/Thomas Gächter/Regina Kiener, Staatsrecht, 3. Aufl., Zürich 2021, S. 613f.

301 Der Grundsatz findet sich ausdrücklich auch im Strafprozessrecht (Art. 3 Abs. 2 lit. b StPO).

auch das Verhalten ihrer Vorgesetzten und insbesondere dasjenige ihrer Aufsichtsbehörde in die Überlegungen miteinbezogen werden.

10.4.3 Kontroversen über die Rechtmässigkeit staatlichen Handelns

Sämtliche Beteiligten des NDB, die in irgendeiner Weise an der auf freiwilliger Basis erfolgten Herausgabe von Netzwerkaufzeichnungen und Serverabbildern involviert waren, handelten in der – wenn auch irrigen – Annahme, dass ihr Vorgehen in rechtlicher Hinsicht durch Art. 23 NDG (bzw. damals durch Art. 14 Abs. 2 BWIS) gedeckt ist. Die irrtümliche Annahme, ein tatbestandsmässiges Verhalten sei im konkreten Fall rechtmässig, weil ein Rechtfertigungsgrund[302] das Vorgehen erlaube, stellt einen Irrtum über die Rechtswidrigkeit dar. Wie fast jeder Irrtum über die Rechtmässigkeit wäre dieser Irrtum bei entsprechenden Abklärungen zwar zu vermeiden gewesen. Diese theoretische Möglichkeit der richtigen Erkenntnis der Rechtslage schliesst aber – wie das Bundesgericht ausdrücklich festgehalten hat – die Anwendbarkeit von Art. 21 StGB nicht aus. Entscheidend ist allein, ob dem Täter das Fehlen der richtigen Erkenntnis zum Vorwurf gemacht werden kann[303].

Innerhalb des NDB gab es zwar – jedenfalls seit 2018/2019 – Stimmen, welche die Rechtmässigkeit des Vorgehens in Frage stellten. Definitive Klarheit, dass Netzwerkaufzeichnungen und Serverabbilder nur auf dem Weg genehmigungspflichtiger Beschaffungsmassnahmen beigezogen werden können, bestand indessen erst mit der Eröffnung der internen Untersuchung bzw. dem Vorliegen der in jener Untersuchung in Auftrag gegebenen rechtlichen Beurteilung durch eine externe Anwaltskanzlei. Anhaltspunkte dafür, dass Cyber NDB auch danach Daten beigezogen hatte, die nur mittels geheimer Beschaffungsmassnahmen hätten erlangt werden können, liegen nicht vor.

In diesem Zusammenhang ist insbesondere zu berücksichtigen, dass Meinungsverschiedenheiten über die korrekte Auslegung von Verfahrensbestimmungen bzw. die Rechtmässigkeit oder Unrechtmässigkeit staatlichen Handelns zum Alltag jeder Behörde und jedes Beamten zählen. Dies zeigt sich besonders deutlich in Bereichen, in denen Behörden – etwa der Polizei oder der Staatsanwaltschaft – gesetzliche Zwangsmassnahmenbefugnisse zukommen und damit berechtigt sind, in (vielfach auch strafrechtlich geschützte) Grundrechte einzugreifen. Dieser Eingriff ist unter Berücksichtigung aller konkreten Umstände sorgfältig abzuwägen; es sind somit tatsächliche Annahmen zu treffen, Gesetzesauslegungen zu prüfen, Interessenabwägungen vorzunehmen und Verhältnismässigkeitsüberlegungen anzustellen. Dieser Prozess verläuft nicht entlang einer scharfen Grenzlinie zwischen eindeutiger Rechtmässigkeit und klarer Rechtswidrigkeit, sondern weist zahlreiche Graubereiche auf.

Dass der Prozess zur Wahl des richtigen Vorgehens (auch) zu unterschiedlichen Beurteilungen führen kann, ist vorgegeben. Das Gesetz antizipiert die Relativität der einmal getroffenen Entscheidung und sieht zahlreiche Beschwerdemöglichkeiten und Rechtsmittelwege vor, um Kontroversen über tatsächliche Feststellungen oder Annahmen und rechtliche Auslegungsfragen zu klären und gegebenenfalls falsche Entscheide zu

---

302 Hier Art. 14 StGB: „Wer handelt, wie es das Gesetz gebiet oder erlaubt, verhält sich rechtmässig, auch wenn die Tat nach diesem oder einem anderen Gesetz mit Strafe bedroht ist."

303 BGE 116 IV 56 E. II 3a.

korrigieren. Dabei dürfte es sich von selbst verstehen, dass nicht jede geschützte Haftbeschwerde oder jeder Freispruch nach erstandener Untersuchungshaft zugleich auch zur Eröffnung eines Strafverfahrens wegen Freiheitsberaubung führen muss. Im Gegenteil; der überwiegende Teil umstrittener Verfahrensfragen im polizeilichen und strafprozessualen Verfahrensrecht wurde erst geklärt, nachdem staatliche Behörden in verfassungsmässige (und vielfach auch strafrechtlich geschützte) Rechte Betroffener eingegriffen hatten und in der Folge vom Bundesgericht eines Besseren belehrt werden mussten[304]. Zu erinnern ist in diesem Zusammenhang etwa an die Entscheide zur verdeckten Ermittlung in Chat-Räumen[305], zu Alkoholtestkäufen bei Jugendlichen[306], zu Scheinkäufen bei Drogendelikten[307] oder auch zu den Sozialdetektiven[308]. Das sind alles Entscheide, die – wie hier – Beschaffungsmassnahmen ohne Einholung der erforderlichen Genehmigungen zum Gegenstand hatten.

10.4.4 Rechtsstandpunkt der Aufsichtsbehörde über den Nachrichtendienst

Unter dem Aspekt der Vermeidbarkeit des Irrtums über die Rechtswidrigkeit ist nicht zuletzt von Bedeutung, dass die eigene Aufsichtsbehörde detaillierte Kenntnisse von den Vorgängen bei Cyber NDB hatte und dagegen nicht eingeschritten war. Zu den Aufgaben der AB-ND gehört bekanntlich, die nachrichtendienstliche Tätigkeit des NDB auf ihre Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit zu überprüfen[309]. Ihren Stellungnahmen kommt somit erhebliches Gewicht zu. Die AB-ND hat im August 2021 einen Prüfbericht i.S. [redacted] verfasst und ist (noch nach der Eröffnung der internen Untersuchung) zur Beurteilung gelangt, es bestehe das Risiko, dass der NDB mit den Netzwerkaufzeichnungen und Serverabbildern in einem rechtlichen Graubereich handle, was durchaus nachvollziehbar sei, da es das Ressort Cyber NDB in dieser Form erst seit relativ kurzer Zeit gebe und noch nicht alle Fragen beantwortet sein könnten. Es bedürfe deshalb einer Analyse, in welchen Fällen das Vorgehen des NDB bei der Ansprache von Providern hinsichtlich der Einsichtnahme in Randdaten des Datenverkehrs als rechtskonform gelten dürfe bzw. welche Voraussetzungen dazu erfüllt sein müssten (siehe dazu Ziffer 4, Seite 23). Diese Empfehlung hat der NDB unverzüglich umgesetzt, die bisherige Praxis der Datenbeschaffung sofort eingestellt[310] und bei der Anwaltskanzlei [redacted] eine rechtliche Beurteilung der Informationsbeschaffung und -bearbeitung in Auftrag gegeben.

Es zeigt sich somit, dass selbst die eigene Aufsichtsbehörde noch im August 2021 die Problematik einer unrechtmässigen, möglicherweise gar strafbaren Datenbeschaffung nicht in ihrem vollen Ausmass erkannt, ja erst noch ein gewisses Verständnis für die direkte Ansprache von Providern gezeigt hatte. Sie verlangte nicht die sofortige Beendigung der Aktionen, sondern gab allein die Empfehlung ab, die Vorgänge im Hinblick auf deren Rechtmässigkeit einer vertieften rechtlichen Analyse zu unterziehen. Unter diesen

---

304 Dies zeigte sich besonders deutlich in der Rechtsprechung des Bundesgerichts zur staatsrechtlichen Beschwerde unter der Geltung des früheren Bundesrechtspflegegesetzes, als dessen Kognition im Bereich des kantonalen Prozessrechts noch auf die Verletzung verfassungsmäßiger Rechte beschränkt war.

305 BGE 134 IV 266.

306 BGer 6B_272/2009.

307 BGer 6B_743/2009.

308 BGE 143 I 377.

309 Art. 78 NDG.

310 Siehe dazu interner Bericht (Fn. 39), S. 6

Umständen muss sämtlichen Mitarbeitenden des Nachrichtendienstes unter strafrechtlichen Gesichtspunkten zugestanden werden, dass sie nicht wussten und nicht wissen konnten, dass ihr Handeln bzw. Unterlassen rechtswidrig war. Es kann ihnen folglich auch nicht zur Last gelegt werden, dass ihr Irrtum über die Tragweite von Art. 23 NDG vermeidbar gewesen wäre. Eine Strafbarkeit wegen vorsätzlicher Anstiftung zu einem strafbaren Verhalten scheidet somit wegen fehlendem Unrechtsbewusstsein und damit mangels schuldhaftem Verhalten aus, selbst wenn der objektive Tatbestand eines Daten- oder Persönlichkeitsdelikts allenfalls noch erfüllt sein könnte.

10.4.5 Opportunität einer Strafanzeige

Gewiss, definitive Klarheit bei der Subsumierung eines konkreten Verhaltens unter einen bestimmten Straftatbestand können nur Staatsanwaltschaft und Strafgerichte schaffen. Trotzdem scheint aufgrund des heutigen Erkenntnisstands die rechtliche Ausgangslage genügend klar zu sein, um mit guten Gründen auf die formelle Einreichung einer Strafanzeige durch das VBS zu verzichten. Diese könnte sich ohnehin wohl nur gegen Mitarbeitende des NDB richten. Das VBS hat primär öffentliche Interessen zu wahren und trägt die Verantwortung für das Handeln seiner Mitarbeitenden. Es trägt aber keine Verantwortung für das Verhalten von Drittpersonen (Providern), die möglicherweise Rechte anderer Drittpersonen (Datenberechtigte) verletzt haben könnten, zumal diesbezüglich eine strafbare Anstiftung durch Mitarbeitende des NDB klar verneint werden kann. Abgesehen davon, erschiene es wenig opportun, wenn das VBS aus eigener Initiative Strafanzeige gegen Drittpersonen (Provider) erheben würde, die keineswegs zum Schaden des Departements, sondern – im Gegenteil – im Interesse des Nachrichtendienstes gehandelt haben.

Sollte das VBS eine Strafanzeige gegen Mitarbeitende des NDB dennoch in Erwägung ziehen[311], erscheint zum einen die Wahrscheinlichkeit einer Verurteilung ausgesprochen gering. Sämtliche in Frage kommenden potenziell Beschuldigten könnten sich – abgesehen von allen übrigen Einwendungen – darauf berufen, dass sie sich in einem unvermeidbaren Irrtum über die Rechtswidrigkeit befunden und deshalb nicht schuldhaft gehandelt hatten. Zum andern bleibt zu berücksichtigen, dass der Sachverhalt und die Rechtslage – wie auch die GPDel mit ihrem Verzicht auf eigenständige Abklärungen einstweilen zum Ausdruck gebracht hat – mit der internen Untersuchung, der vom NDB eingeholten rechtlichen Beurteilung und der vorliegenden Administrativuntersuchung weitgehend geklärt ist. Es besteht deshalb kein öffentliches Interesse daran, eine weitere, zumal noch strafrechtliche Untersuchung in die Wege zu leiten. Auch ist nicht anzunehmen, dass sich im Rahmen eines Strafverfahrens neue Gesichtspunkte ergeben könnten, welche bis anhin nicht bekannt waren. Vielmehr wird – nicht zuletzt wegen der mangelnden Dokumentation bei Cyber NDB – weiterhin einiges an konkreten Geschehnissen im Dunkeln bleiben.

Es würde zwar zu gewissen Tendenzen passen, Meinungsverschiedenheiten über die Rechtmässigkeit staatlichen Handelns und die Korrektheit des Vorgehens staatlicher Angestellter durch die Strafjustiz klären zu lassen. Die Erfahrung zeigt aber, dass individuelle Strafverfahren gegen einzelne Beamte oder öffentliche Angestellte –

311 Eine Strafanzeige könnte auch gegen "Unbekannt" erhoben werden, womit es dann Aufgabe der Strafverfolgungsbehörden wäre, die verantwortlichen Personen zu eruieren.

selbstverständlich abgesehen von klarem individuellem Fehlverhalten – nicht viel weiterhelfen. Dabei bleibt mitzuberücksichtigen, dass zwar die Bestimmungen des Nachrichtendienstgesetzes über die genehmigungspflichtigen Beschaffungsmassnahmen nicht eingehalten und damit unrechtmässig Daten beschafft wurden[312]. Betroffen waren aber keine besonders schützenswerte Personendaten, sondern im Wesentlichen technische Daten des Netzwerkverkehrs. Daraus entstandene Nachteile für die Betroffenen – in der Regel mutmassliche staatliche Akteure von Spionageangriffen – sind nicht bekannt. Mit den vom Nachrichtendienst in der Zwischenzeit getroffenen Massnahmen ist sichergestellt, dass sich gleichartige Vorkommnisse nicht wiederholen können, sodass auch aus diesem Grund kein Bedarf nach einem zusätzlichen Miteinbezug der Strafbehörden besteht.

Hinzu kommt schliesslich, dass es sich bei den zur Diskussion stehenden Straftatbeständen[313] um Offizialdelikte handelt. Die Bundesanwaltschaft wäre deshalb als Strafverfolgungsbehörde des Bundes – sollte sie Anhaltspunkte für einen hinreichenden Tatverdacht erkennen – auch ohne Strafanzeige verpflichtet, von Amtes wegen ein Strafverfahren einzuleiten[314]. Die für den Entscheid über die Einleitung oder Nichteinleitung eines Strafverfahrens erforderlichen Informationen liegen der Bundesanwaltschaft bereits heute in den wesentlichen Grundzügen vor. Der damalige Direktor NDB hatte im Mai 2021 [redacted] sowie [redacted] über die ersten Erkenntnisse der internen Untersuchung orientiert. Die Bundesanwaltschaft verneinte damals eine strafrechtliche Dimension der Vorkommnisse bei Cyber NDB[315] und sah sich nicht veranlasst, eine Strafuntersuchung zu eröffnen[316]. Aus der Medienmitteilung des Bundesrates vom Januar 2022 ging überdies klar hervor, dass der Nachrichtendienst in den Jahren 2015 bis 2020 im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen ohne Einholung der erforderlichen Genehmigungen auch Daten beschafft hatte, welche dem Fernmeldegeheimnis unterstehen. Auch die Offenlegung dieser Fakten bildete für die Bundesanwaltschaft offenbar keinen hinreichenden Grund für die Einleitung eines Strafverfahrens.

Aus Sicht des Untersuchungsbeauftragten liegt somit kein sachlicher Grund für die formelle Einreichung einer Strafanzeige vor. Auch für allfällige Überlegungen, der Bundesanwaltschaft den Bericht der Administrativuntersuchung – soweit er die unrechtmässige Datenbeschaffung zum Gegenstand hat – zur Kenntnis zu bringen, besteht keine Veranlassung.

St. Gallen, 15. August 2022 Der Untersuchungsbeauftragte

U. Oleth Obrz

312 Diese Bestimmungen sollten nach der hier vertretenen Auffassung im Sinne einer "Legalisierung" der bisherigen Praxis oder zumindest in Form einer wesentlichen Vereinfachung der Verfahrensabläufe ohnehin revidiert werden (siehe dazu Ziffer 9.6 (Seite 73).

313 Mit Ausnahme des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB).

314 Art. 7 Abs. 1 StPO.

315 Die Besprechung mit der BA fand am [redacted] statt; eine Aktennotiz wurde nicht erstellt. Der damalige Direktor NDB informierte aber am folgenden Tag die Vorsteherin des VBS über das Ergebnis der Besprechung (Dokumente 610 und 614 der internen Untersuchung).

316 Interner Bericht (Fn. 39), S. 18.

Abkürzungsverzeichnis

AB-ND	Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten
BA	Bundesanwaltschaft
BBL	Bundesblatt
BG	Bundesgesetz
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BGer	Bundesgerichtsentscheid (nicht in der amtlichen Sammlung publiziert)
BPG	Bundespersonalgesetz vom 24. März 2000 (SR 172.220.1)
BSD	Bundessicherheitsdienst
BStGer	Bundesstrafgericht
BÜPF	BG betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (SR 780.1)
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101)
BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (SR 120)
CCC	Convention on Cybercrime; Übereinkommen über die Cyberkriminalität, abgeschlossen in Budapest am 23. November 2001; in Kraft getreten für die Schweiz am 1. Januar 2012 (SR 0.311.43)
CNO	Computer Network Operations des Zentrums für Elektronische Operationen der Führungsunterstützungsbasis der Armee (künftig voraussichtlich Cyber-Kommando)
COMINT	Communications Intelligence (Funk- und Kabelaufklärung)
[redacted]	[redacted]
CyRV	VO über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020 (Cyberrisikenverordnung; SR 120.73)
Dienst ÜPF	Dienst Überwachung Post- und Fernmeldeverkehr; administrativ dem ISC-EJPD zugewiesen
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (SR 0.101)
FUB	Führungsunterstützungsbasis der Armee
GarG	Bundesgesetz über die politischen und polizeilichen Garantien zugunsten der Eidgenossenschaft (Garantiegesetz) vom 26. März 1934 (SR 170.21)
GEBM	Genehmigungspflichtige Beschaffungsmassnahme
GEVER	elektronische Geschäftsverwaltung NDB
GPDel	Geschäftsprüfungsdelegation der Eidgenössischen Räte
GPK	Geschäftsprüfungskommission
HUMINT	Human Intelligence (menschliche Quellen)
IASA	Informations- und Analysesystem Allsource des NDB
IKT	Informations- und Kommunikationstechnologien
IMINT	Imagery Intelligence (Bildaufklärung)
IRSG	BG über die internationale Rechtshilfe in Strafsachen VOM 20. März 1981 (SR 351.1)
ISB	Informatiksteuerungsorgan des Bundes
ISC-EJPD	Informatik Service Center des EJPD
ISDS	Informationssicherheit und Datenschutz
ISMS	Informationssicherheitsmanagementsystem
KND	Kantonaler Nachrichtendienst

MELANI	Melde- und Analysestelle Informationssicherung
MND	Militärischer Nachrichtendienst
NDB	Nachrichtendienst des Bundes
[redacted]	Direktionsbereich [redacted]
[redacted]	Direktionsbereich [redacted]
NDBI	Direktionsbereich Informationsmanagement/Cyber NDB
[redacted]	Direktionsbereich [redacted]
[redacted]	Direktionsbereich [redacted]
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
NCSC	Nationales Zentrum für Cybersicherheit
NDG	BG über den Nachrichtendienst vom 25. September 2015 (Nachrichtendienstgesetz; SR 121)
NDV	VO über den Nachrichtendienst vom 16. August 2017 (Nachrichtendienstverordnung; SR 121.1)
OIC MELANI	Operation Information Center der Melde- und Analysestelle Informationssicherung
[redacted]	[redacted]
OSINT	Open Source Intelligence (öffentliche Quellen)
ParlG	BG übe die Bundesversammlung vom 13. Dezember 2002 (Parlamentsgesetz; SR 171.10)
PD	Partnerdienst
PPP	Public Private Partnership
PVK	Parlamentarische Verwaltungskontrolle
RVOG	Regierungs- und Verwaltungsorganisationsgesetz (SR 172.010)
RVOV	Regierungs- und Verwaltungsorganisationsverordnung (SR 172.010.1)
Sensor	Gesamtheit der Quellen des ND
StBOG	BG über die Organisation der Strafbehörden des Bundes vom 19. Mai 2010 (Strafbehördenorganisationsgesetz; SR 173,71)
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung (SR 312.0).
TRAVINT	Travel Intelligence (Information zu Aufenthalt und Reisen
VA	Verteidigungsattaché
VAND	VO über die Aufsicht über die nachrichtendienstlichen Tätigkeiten vom 16. August 2017 (SR 121.3)
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE-NDG	Entwurf zu einer Revision des BG über den Nachrichtendienst
VES	Verordnung über den Einsatz von privaten Sicherheitsunternehmen für Schutzaufgaben durch Bundesbehörden (Verordnung über den Einsatz privater Sicherheitsfirmen durch den Bund; SR 124)
VIS-ND	Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bund vom 16. August 2017 (SR 121.2)
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten (Verantwortlichkeitsgesetz; SR 170.32
VO	Verordnung
VPR	Verwaltungspraxis der Bundesbehörden
VStrR	Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (SR 313.0)
VÜPF	VO über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 (SR 780.11)
VwVG	Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968
ZEO	Zentrum elektronische Operationen der Führungsunterstützungsbasis der Armee
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (SR 272)

Technisches Glossar

APT	Advanced Persistent Threats: Angreifer verwendet fortgeschrittene Angriffstechniken, um sich einen dauerhaften Zugriff zu einem Netzwerk zu verschaffen und sich auf weitere Systeme auszubreiten; fixes Ziel vor Augen, hartnäckig.
C2-Server	Command and Control Server: Server im Internet, den ein Angreifer zur Ausführung von Befehlen auf infizierten Computern verwendet. Nachdem ein Schadprogramm ein System infiziert hat, nimmt es Kontakt mit dem C2 auf, um von dort weitere Schadcode nachzuladen, Instruktionen zu empfangen oder auf dem infizierten System ausgespähte Informationen an den Server zu übermitteln.
CTI	Cyber Threat Intelligence: Evidenzbasierte Informationen über Cyberangriffe, die von Experten geordnet und analysiert werden und von auf Cybersicherheit spezialisierten Unternehmen weiteren Abnehmern kommerziell zur Verfügung gestellt werden.
DDoS	Distributed Denial of Service: DDoS Attacken verfolgen das Ziel, Systeme oder ganze Infrastrukturen derart zu belasten, dass sie ihre Funktionsfähigkeit verlieren.
IOC	Indicators of Compromise: Technische Informationen, die zur Detektion einer Infektion in einem System oder Netzwerk oder zur Kennzeichnung einer Malware verwendet werden können.
IP-Adresse	Internet Protocol Adress: Netzwerkadresse, die nur einmal vergeben werden darf und im Hinblick auf die Adressierung von Datenpaketen als eindeutiges Identifikationsmerkmal eines Computers dient, um seinen Standort im Internet zu definieren.
ISP	Internet Service Provider: Stellt Dienste, Inhalte oder technische Leistungen bereit, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind.
Log-Daten	In einem Protokoll festgehaltene Daten aller oder bestimmter Aktionen von Prozess auf einem Computer.
[redacted]	[redacted].
Provider	Stellt als Mobilfunkprovider, Internet Service Provider oder Telefonnetzprovider die Infrastruktur für den Daten- und Sprachtransport bereit.
Server	Rechner, der seine Hardware- und Softwareressourcen in einem Netz anderen Rechnern Clients zugänglich macht.
Spanning	Kopieren der Serverdaten während einem simulierten Wartungsmodus.
Tapping	Vorgänge bei privaten Schweizer Unternehmen, die Opfer von Cyberangriffen wurden, und ihre Einwilligung zur Untersuchung deren Netzwerke auf Cyberaktivitäten erteilt haben.