Dr. Niklaus Oberholzer
Rechtsanwalt
Kesselhaldenstrasse 55
9016 St. Gallen

mail@niklausoberholzer.ch

Vorkommnisse im Ressort Cyber des Nachrichtendienstes des Bundes (NDB)

Bericht der Administrativuntersuchung

erstattet im Auftrag des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS)

15. August 2022

Auszug aus den Empfehlungen und der rechtlichen Beurteilung des Schlussberichts

1 Ausgangslage und Berichterstattung zur Administrativuntersuchung

Der Schweizerische Nachrichtendienst (NDB) hatte im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen in den Jahren 2015 bis 2020 auch Informationen über den Netzwerkverkehr potenzieller Angreifer beschafft und bearbeitet. Derartige Informationen zählen zu den sogenannten Randdaten des Fernmeldeverkehrs und stehen unter dem Schutz des Fernmeldegeheimnisses. Sie können rechtmässig nur unter Einhaltung der Bestimmungen des Nachrichtendienstgesetzes (NDG) mittels genehmigungspflichtiger Beschaffungsmassnahmen erhoben werden. Die dazu erforderlichen Genehmigungen durch das Bundesverwaltungsgericht und die politische Freigabe durch die Vorsteherin VBS wurden vom NDB jedoch nicht eingeholt.

Nachdem der Nachrichtendienst wegen dieser Vorkommnisse bereits eine interne Untersuchung durchgeführt hatte, beauftragte das VBS im Januar 2022 Dr. Niklaus Oberholzer, Rechtsanwalt und ehemaliger Richter am Schweizerischen Bundesgericht, mit der Durchführung einer Administrativuntersuchung. Er erstattete dem Departement im August 2022 seinen Schlussbericht.

Eine vollständige Publikation des Schlussberichts kommt nicht in Frage, da dieser einerseits Informationen enthält, die aus geheim klassifizierten Quellen stammen, und andererseits Ausführungen zum Aufbau, den Strukturen, der internen Organisation und den Arbeitsmethoden des Nachrichtendienstes enthält. Eine Offenlegung dieser Informationen könnte den Quellen- oder den Personenschutz oder die Geheimhaltung von operativen Mitteln und Methoden der Nachrichtendienste schwerwiegend gefährden[1].

Das VBS hat sich deshalb entschieden, den Schlussbericht der Administrativuntersuchung als geheim zu klassifizieren, soweit dieser sich zu geheimhaltungsbedürftigen Tatsachen der nachrichtendienstlichen Organisation oder Methoden äussert. Den Informationsbedürfnissen der Öffentlichkeit wird einerseits mit einer zusammenfassenden Präsentation der wesentlichen Erkenntnisse Rechnung getragen. Andererseits erfolgt mit dem vorliegenden Auszug eine weitgehend vollständige Publikation der im Schlussbericht enthaltenen Empfehlungen und der darin vorgenommenen rechtlichen Beurteilungen. Dies betrifft neben einer Einleitung zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken im Wesentlichen die Empfehlungen zu einer organisatorischen Neuausrichtung von Cyber NDB und zu einer Revision der Bestimmungen des Nachrichtendienstgesetzes über die genehmigungspflichtigen Beschaffungsmassnahmen sowie die rechtliche Analyse einer allfälligen strafrechtlichen Relevanz der unrechtmässigen Datenbeschaffung und -bearbeitung durch den Nachrichtendienst.

Soweit aus berechtigten Geheimhaltungsinteressen Auslassungen vorgenommen werden, sind diese mit einer entsprechenden Klammer (...) separat gekennzeichnet. Allfällige Erläuterungen zu den Auslassungen sind kursiv gesetzt.

---

1 Vgl. Art. 5 Abs. 1 lit. f der Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV; SR 510.411).

2 Cyber NDB und Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

Das beim Eidgenössischen Finanzdepartement (EFD) angesiedelte Nationale Zentrum für Cybersicherheit (NCSC) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für Wirtschaft, Verwaltung Bildungseinrichtungen und Bevölkerung. Es ist verantwortlich für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018–2022[2].

Cyber NDB ist in die Nationale Strategie zum Schutz der Schweiz von Cyberrisiken 2018–2022[3] eingebettet und koordiniert seine Aktivitäten mit den anderen staatlichen Organisationseinheiten im Bereich der Cyberabwehr. Das Ressort arbeitet im Bereich der Informationsbeschaffung eng mit "Computer Network Operations" (CNO), einer Abteilung des Zentrums elektronische Operationen (ZEO) der Führungsunterstützungsbasis der Armee (FUB), und dem Militärischen Nachrichtendienst (MND) zusammen; eine institutionalisierte Zusammenarbeit mit der Cybermiliz der Armee[4] ist nicht vorgesehen. Das Schwergewicht der Tätigkeit von Cyber NDB liegt in der Auswertung von Informationen, welche die Früherkennung von Angriffen und deren geografische Zuordnung ermöglichen[5].

Soweit es bei der Beschaffung und Auswertung von Information um die Einschätzung der Cyberbedrohungslage geht, ist die vom Informatiksteuerungsorgan des Bundes (ISB) und vom NDB gemeinsam betriebene Melde- und Analysestelle Informationssicherung (MELANI) federführend[6]. Diese unterstützt im Rahmen eines Public Private Partnership (PPP) subsidiär den Informationssicherungsprozess innerhalb der kritischen Infrastrukturen.

Cyber NDB stellt die von ihm beschafften und ausgewerteten Informationen zur Erkennung von Cyberangriffen (sogenannte Indicators of Compromise; IOC) dem Nationalen Cyber-Sicherheitszentrum und weiteren Partnern im Bereich der Cyberabwehr zur Verfügung. Seine Informationen fliessen in die allgemeinen Lagebeurteilungen ein und dienen der Bewältigung oder zumindest Minimierung von Risiken durch die dafür zuständigen Organisationseinheiten des Bundes und der Kantone.

Das Ressort Cyber NDB, die Melde- und Analysestelle Informationssicherung (MELANI) und Teile der Armee sind die massgeblichen Akteure, die Cyberbedrohungen begegnen. Sie sind in einer interdepartementalen, komplexen Organisationsstruktur zum Schutz kritischer Infrastrukturen und zur Cyberabwehr eingebettet. Hauptaufgabe des NDB ist es, mit nachrichtendienstlichen Mitteln Cyberangriffe zu identifizieren und zuzuordnen. Darüber hinaus unterstützt er die Betreiber kritischer Infrastrukturen mit der Darstellung der aktuellen Cyberlage. Operative und technische Analyse sind im NDB im Ressort Cyber zusammengefasst. Parallel dazu verfügt auch das ZEO im Bereich Cyber Network Operations (CNO) über eine Einheit Cyber Threat Intelligence (CTI), die sich mit der Cyberbedrohungsanalyse beschäftigt. Das Ressort Cyber im NDB sieht sich im Handlungsfeld Cyber dann gefordert, wenn es um sicherheitspolitisch relevante Vorfälle geht,

---

2 Website des NCSC (http://www.admin.ch/ncs/de/home/ueber -ncsc/das-ncs.html).

3 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018-2022 (NCS) (https://www.ncsc.admin.ch/ncsc/de/home/strategie/strategie-ncsc-2018-2022.html).

4 Cyber-Kompanie, in der elektronischen Abteilung der Führungsunterstützungsbrigade angesiedelt (http://www.vtg.admin.ch/de/aktuell/themen/cyberdefence/syber-miliz.html).

5 NCS, S. 24.

6 Aktennotiz NDB zuhanden der Administrativuntersuchung 20.04.2022.

die einem anderen Staat zuordenbar sind. Reine Aktivitäten von Cyberkriminellen zählen nicht zu seinem Aufgabenbereich[7].

Die bisherigen Bemerkungen zu den von Bundesrat und Departement verabschiedeten Strategien zum Schutz vor Cyberrisiken erscheinen angezeigt, um die Bedeutung hervorzustreichen, welche diesem Thema von der Politik beigemessen wird. Die verschiedenen Strategiepapiere verdeutlichen, dass vom Nachrichtendienst erwartet wird, mittels einer systematischen Beschaffung und Auswertung von Informationen neue Angriffsmuster möglichst frühzeitig zu entdecken und diesen deren Urheberschaft zuzuordnen.

Damit der NDB diese Zielvorgaben, insbesondere ein möglichst rasches Vorgehen, erreichen kann, müssen die erforderlichen gesetzlichen Grundlagen geschaffen und die nötigen Mittel zur Verfügung gestellt werden. Wie die vorliegende Untersuchung zeigt, scheint dies nicht immer der Fall gewesen zu sein: Kann Cyber NDB die zur Entdeckung eine Cyberangriffs erforderlichen Informationen nur auf dem Weg der genehmigungspflichtigen Beschaffungsmassnahmen erlangen, verstreichen Tage, wenn nicht gar Wochen, bevor das Ressort mit einer systematischen Auswertung der Daten und damit mit einer Analyse der Angriffsmuster beginnen kann. Die von der Politik verlangte Früherkennung dürfte damit illusorisch werden. Insofern mag es zwar nicht gerechtfertigt, aber doch nachvollziehbar sein, dass Cyber NDB in der vermeintlichen Überzeugung, Art. 23 NDB biete für eine freiwillige Datenherausgabe eine hinreichende Grundlage, eigenständig neue Mittel und Wege zur Informationsbeschaffung gesucht hat, um seine Aufgaben erfüllen zu können.

Bei einer Würdigung der nationalen Cyberstrategie fällt weiter auf, dass nicht nur die Bedeutung eines gemeinsamen und koordinierten Vorgehens zwischen staatlichen Behörden und Privaten betont, sondern auch auf die Unerlässlichkeit einer engen internationalen Zusammenarbeit hingewiesen wird. Folgt man dieser Strategie, kann dem NDB nicht zum Vorwurf gemacht werden, dass er im Bereich der Cyberabwehr mit Unternehmen im Bereich der Cybersicherheit zusammengearbeitet hat und in einem engen Informationsaustausch mit internationalen Partnerdiensten steht.

7 AB-ND, Tätigkeitsbericht 2021, S. 14.

3 Varianten für eine Neustrukturierung des Ressorts Cyber NDB

Bei der Einführung des Ressorts Cyber NDB herrschte die Auffassung vor, dass es sich bei Cyber einfach um ein weiteres Themengebiet des Nachrichtendienstes handelt und die für die anderen Arbeitsfelder geltenden Strukturen und Abläufe weitgehend unbesehen übernommen werden können. Unberücksichtigt blieb dabei, dass es sich bei Cyber nicht um ein neues Ziel von Bedrohungen der inneren oder äusseren Sicherheit, sondern um eine ganz bestimmte, von der konkreten Zielrichtung des Angriffs weitgehend unabhängige neue Methode der Bedrohung handelt. Die unmittelbare Bedrohung liegt nicht in den damit (sekundär) verfolgten individuellen Angriffszielen, sondern im Missbrauch digitaler Kommunikationsnetzwerke zu kriminellen Zwecken (irgendwelcher Art). Dementsprechend ist auch die auf Erkennung und Abwehr derartiger Angriffe ausgerichtete Tätigkeit von Cyber NDB primär auf eine Analyse der technischen Angriffsmethoden ausgerichtet. Für die Analysten von Cyber NDB stehen nicht personen-, organisations- oder lagebezogene Informationen im Vordergrund. Ihre Haupterkenntnisquelle liegt vielmehr in der Erfassung und Auswertung von technischen Vorgängen, Abläufen und Mustern. Das unterscheidet sie von den themenbezogenen Informationsbeschaffungsvorgängen im Nachrichtendienst, welche sich in erster Linie auf menschliches Verhalten und die davon ausgehende Gefährdungen beziehen.

Der NDB ist sich bewusst, dass die Organisationstrukturen und Prozesse bei Cyber NDB einer umfassenden Überprüfung zu unterziehen sind. Dies wird primär Aufgabe der Direktion und der Geschäftsleitung sein. Im Rahmen der Administrativuntersuchung können zwar Mängel festgestellt, im Hinblick auf deren Behebung aber nur Anregungen gemacht und Hinweise gegeben werden. Zum einen war das Untersuchungsthema auf Vorkommnisse im Ressort Cyber NDB begrenzt; zum andern fehlt es dem Beauftragten an einem umfassenden Überblick über die gesamten Organisationsstrukturen und Abläufe des NDB in seinen vielfältigen Bezügen. Erst dieses, allein bei den Mitarbeitenden des Dienstes vorhandene Spezial- und Detailwissen wird es erlauben, im Hinblick auf die Zukunft eine sachgerechte und erst noch umsetzbare Lösung zu finden.

Aus Sicht des Beauftragten stellt sich zunächst einmal die Frage, ob es sinnvoll erscheint, Cyber NDB weiterhin analog zu den anderen thematisch gegliederten Ressorts des NDB als selbstständige und den anderen Bereichen gleichgestellte Einheit zu betrachten. Stehen bei Cyber NDB nicht eher die technischen Modalitäten der Informations- bzw. Datenübermittlung und weniger die thematische Zielrichtung eines Angriffs im Vordergrund? Ist Cyber NDB ein eigenständiges Ressort oder nicht doch eher ein nachrichtendienstlicher Sensor, der etwa den Bereichen Operationen, HUMINT, OSINT, COMINT, IMINT etc. gleichgestellt werden müsste? Rechtfertigt sich damit weiterhin eine Zentralisierung in einem eigenen Ressort oder müssten die Mitarbeitenden der technischen Analyse (CyberLab) nicht konsequenterweise als Spezialisten der Beschaffung NDBB und die Mitarbeitenden der operativen Analyse der Auswertung NDBA zugewiesen und dort auf die einzelnen Themenbereiche verteilt werden? Welche Auswirkungen für die organisatorische Eingliederung kommt der Tatsache zu, dass sich im Bereich Cyber die Auswertung in zwei klar abgegrenzte Phasen gliedern lässt, d.h. eine rein technische Analyse des Datenverkehrs und eine sich darauf stützende operative Analyse unter Einbezug weiterer personen- und ereignisbezogener Erkenntnisse des Nachrichtendienstes?

Es könnte deshalb – wie schon bei der Schaffung des neuen Ressorts – geprüft werden, ob Cyber NDB weiterhin als eigenständiges Themengebiet in die allgemeinen Strukturen

und Prozesse des Nachrichtendienstes eingebettet bleiben oder dafür neue Strukturen geschaffen werden sollen. Denkbar wäre es, Cyber NDB aus dem nachrichtendienstlichen Kontext zu lösen und dessen Aufgaben auf die rein wissenschaftlich-technisch Analyse von Daten des Netzwerkverkehrs zu beschränken. Cyber NDB würde damit zu einem forensischen Kompetenzzentrum[8] im Bereich der Erkennung und Analyse von Cyberangriffen, dessen besondere Fachexpertise unabhängig von der thematischen Ausrichtung des Angriffs von allen Fachbereichen des NDB in Anspruch genommen werden kann. Dies hätte zur Folge, dass Cyber NDB seine heutige Selbstständigkeit weitgehend verliert und nur noch im Auftrag der Beschaffung oder der Auswertung zur fachspezifischen Unterstützung beigezogen wird. Damit wäre nicht nur das Problem der Steuerung gelöst, sondern auch der Weg geöffnet, um mit aufgabenbezogenen Weisungen die spezifischen Datenbeschaffungs-, Verarbeitungs- und Aufbewahrungsmethoden allenfalls abweichend von den üblichen Prozessen und Abläufen zu reglementieren.

In die Diskussionen miteinbezogen werden könnte gar eine vollständige Herauslösung des Ressorts Cyber NDB aus dem NDB und die Schaffung eines eigenständigen Expertenpools für die Analyse von Daten des Netzwerkverkehrs. Dieser wäre sinnvollerweise wohl beim Nationalen Zentrum für Cybersicherheit (NCSC) anzusiedeln und stünde so allen Organisationseinheiten des Bundes, die im Bereich der Cybersicherheit tätig sind, zur Verfügung.

8 Durchaus vergleichbar mit dem Forensischen Institut Zürich (vgl. http://www.for-zh.ch) oder anderen polizeilichen Kompetenzzentren Forensik.

4 Cyber NDB und genehmigungspflichtige Beschaffungsmassnahmen

4.1 Ausführungen zur fehlenden Rechtmässigkeit der Informationsbeschaffung)

(...)

Der Bundesrat hatte bereits in seiner Medienmitteilung vom Januar 2022 festgehalten, dass gemäss derzeitigen Erkenntnissen der Nachrichtendienst im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen auch Informationen beschafft hatte, welche dem Fernmeldegeheimnis unterstehen. Derartige Informationen hätten nur auf den Weg der im Nachrichtendienst geregelten genehmigungspflichtigen Beschaffungsmassnahmen erlangt werden dürfen. Die dazu erforderlichen gerichtlichen und politischen Bewilligungen seien jedoch nicht eingeholt worden.

In der Administrativuntersuchung wurde diese rechtliche Einordnung bestätigt. Die entsprechenden Ausführungen beinhalten jedoch verschiedentlich Hinweise auf Tatsachen der nachrichtendienstlichen Organisation und Arbeitsmethoden, so dass sie aus Geheimhaltungsgründen nicht öffentlich zugänglich gemacht werden können. Im Rahmen dieses Auszugs aus dem Schlussbericht muss es deshalb einleitend bei der Feststellung sein Bewenden haben, dass der Nachrichtendienst bei der Beschaffung von Informationen über den Netzwerkverkehr die zwingend vorgeschriebenen prozessualen Abläufe nicht eingehalten hat und diese Art der Informationsbeschaffung somit unrechtmässig war.

4.2 Orientierung an strafprozessualen Grundsätzen

Mit dem Nachrichtendienstgesetz wurde dem NDB neu die Befugnis zur Überwachung des Post- und Fernmeldeverkehrs, zum Einsatz technischer Überwachungsgeräte sowie zum Eindringen in Computersysteme und Computernetzwerke eingeräumt[9]. In der Botschaft wurde darauf hingewiesen, dass der NDB genehmigungspflichtige Beschaffungsmassnahmen im Gegensatz zu den Strafverfolgungsbehörden, die solche Überwachungen im Rahmen eines Strafverfahrens zur Überführung eines Täters einsetzen (repressive Zielsetzung), ausschliesslich zu präventiven Zwecken anordnen können[10].

In der Botschaft wurde grosses Gewicht darauf gelegt, dass die präventive Tätigkeit des NDB klar von der repressiven Tätigkeit der Strafverfolgungsbehörden abzugrenzen ist. Der NDB habe den primären Auftrag, sicherheitspolitische Bedrohungen gegen die Schweiz frühzeitig zu erkennen und darüber vor allem den zuständigen Behörden Bericht zu erstatten. Damit sollen Risiken minimiert werden. Der NDB nehme aber keine polizeilichen oder strafprozessualen Aufgaben wahr (z.B. Ermittlungen, Festnahmen, usw.). Nachrichtendienst und Strafverfolgung ergänzten sich somit und seien nicht die Vorstufe der jeweils anderen Instanz[11].

Trotzdem orientiert sich die gesetzliche Regelung der genehmigungspflichtigen Beschaffungsmassnahmen – abgesehen von gewissen Modifikationen bei der Eingriffsschwelle

---

9 Art. 26ff. NDG.

10 Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2164.

11 Botschaft zum Nachrichtendienstgesetz (Fn.10), BBl 2014, 2143.

(konkrete Bedrohung statt dringender Tatverdacht[12]), beim fehlenden Deliktskatalog[13], bei der Anordnungskompetenz (Antrag an das BVGer statt direkte Anordnung durch die Staatsanwaltschaft)[14] und dem politischen Freigabeprozess[15] – weitgehend an den Grundsätzen, die in der Strafprozessordnung und im BÜPF entwickelt worden sind. Sie dient demzufolge nicht der Gefahrenabwehr, sondern ist auf die Strafverfolgung ausgerichtet. In seinem damaligen Gutachten zur BWIS II Vorlage gelangte Giovanni Biaggini zur Feststellung, dass die Terminologie in mancher Hinsicht an die Regelungen im BÜPF bzw. in der StPO erinnert. Dabei dürfe man jedoch nicht ausser Acht lassen, dass die besonderen Mittel der Informationsbeschaffung hier in einem anderen – präventivpolizeilichen-verwaltungsrechtlichen, nicht strafprozessualen – Kontext sowie in einem anderen behördlich-organisatorischen Umfeld zum Einsatz kommen[16].

Der geltende Prozess für genehmigungspflichtige Beschaffungsmassnahmen sieht vor, dass der NDB vor der Durchführung der Massnahme die Genehmigung des Bundesverwaltungsgerichts sowie die Freigabe durch die Vorsteherin oder den Vorsteher des VBS einholt[17]: Zunächst unterbreitet der NDB dem Bundesverwaltungsgericht einen Antrag, der u.a. die Angabe des spezifischen Ziels der Beschaffungsmassnahme und der Begründung ihrer Notwendigkeit enthält[18]. Die Präsidentin oder der Präsident der zuständigen Abteilung des Gerichts entscheidet innerhalb von fünf Arbeitstagen nach Erhalt des Antrags[19]. Liegt die Genehmigung vor, entscheidet die Vorsteherin oder der Vorster des VBS nach vorheriger Konsultation der Vorsteherin oder des Vorstehers des EDA und der Vorsteherin oder des Vorstehers des EJPD über die Freigabe zur Durchführung. Fälle von besonderer Bedeutung können dem Bundesrat vorgelegt werden[20]. Die Direktorin oder der Direktor des NDB kann bei Dringlichkeit den sofortigen Einsatz von genehmigungspflichtigen Beschaffungsmassnahmen anordnen, orientiert aber umgehend das Bundesverwaltungsgericht und die Vorsteherin oder den Vorsteher des VBS. Sie oder er kann die Beschaffungsmassnahme mit sofortiger Wirkung beenden[21]. Einem erleichterten Genehmigungsverfahren unterstehen die Beschaffung von Informationen über Vorgänge im Ausland und die Kabelaufklärung[22].

4.3 Präventive Ausrichtung des NDB

Die genehmigungspflichtigen Beschaffungsmassnahmen im NDG orientieren sich weitgehend an den Grundsätzen, die im Strafprozessrecht entwickelt worden sind und sich dort grundsätzlich bewährt haben. Eine erste Besonderheit der nachrichtendienstlichen Tätigkeit besteht aber darin, dass seine Aufgaben im Unterschied zu den Strafverfolgungsbehörden primär beobachtender Natur sind[23] und auf die frühzeitige Vereitelung

12 Art. 27 Abs. 1 NDG / Art. 269 Abs. 1 StPO.
13 Art. 269 Abs. 2 StPO.
14 Art. 29 Abs. 1 NDG / Art. 269 Abs. 1 i.V.m. Art. 272 Abs. 1 StPO.
15 Art. 30 NDG.
16 Giovanni Biaggini, Verfassungsrechtliche Abklärung betreffend die Teilrevision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Vorlage BWIS) vom Juni 2009; in: VPR 4/2009, S. 270.
17 Art. 27 Abs. 2 NDG.
18 Art. 29 Abs. 1 NDG.
19 Art. 29 Abs. 2 NDG.
20 Art. 30 Abs. 1 NDG.
21 Art. 31 Abs. 1 NDG.
22 Art. 36 ff.; Art. 39 ff. NDG.
23 Nadine Zurkinden, Verbrechensbekämpfung durch Nachrichtendienste in der Schweiz, in: Marc Engelhart/Mehmet Arslan (Hrsg.), Verbrechensbekämpfung durch Nachrichtendienste, Freiburg 2021, S. 158.

einer Straftat und nicht auf die spätere Strafverfolgung zielen. Die Strafbehörden sanktionieren begangenes Unrecht; ihr Blick ist deshalb retrospektiv in die Vergangenheit gerichtet. Demgegenüber ist das Handeln der Präventionsbehörden, auch der Polizei, soweit sie nicht kriminalpolizeiliche Funktionen wahrnimmt, prospektiv auf die Zukunft gerichtet[24]. Während die Staatsanwaltschaft für die gleichmässige Durchsetzung des staatlichen Strafanspruchs verantwortlich ist[25] und erst einschreitet, wenn ein hinreichender Tatverdacht auf eine bereits verübte Straftat gegeben ist[26], hat der NDB die Aufgabe, Bedrohungen der inneren oder äusseren Sicherheit der Schweiz (frühzeitig) zu erkennen und (nach Möglichkeit) zu verhindern[27]. Seine Tätigkeit ist somit weniger von feststehenden Tatsachen in der Vergangenheit als vielmehr von Ungewissheiten über künftige Entwicklungen geprägt. Dementsprechend breitgefächert und wenig zielgerichtet müssen die Informationen sein, auf welche der NDB Zugriff braucht.

Der Nachrichtendienst zählt – wie die Sicherheitspolizei – zu den Präventionsbehörden. Seine Tätigkeit wird nicht von strafprozessualen, sondern von staats- und verwaltungsrechtlichen Grundsätzen gelenkt. Während im Strafprozess für Einschränkungen von Grundrechten das strikte Legalitätsprinzip gilt, stösst das Bestimmtheitsgebot im Polizeirecht wegen der Besonderheiten des Regelungsbereichs auf besondere Schwierigkeiten. Trotz des Bemühens um Konkretisierung typisierter Handlungsformen kann nicht auf höchst unbestimmte Regelungen verzichtet werden, und zwar sowohl in Bezug auf die Voraussetzungen polizeilichen Handelns als auch im Hinblick auf die zu treffenden Massnahmen[28]. Die präventive Tätigkeit richtet sich gegen nicht im Einzelnen bestimmbare Gefährdungsarten und -formen in vielgestaltigen und wandelbaren Verhältnissen und ist deshalb situativ den konkreten Verhältnissen anzupassen[29]. Die Beantwortung der Frage, wie real und wie gross die abzuwendende Gefahr tatsächlich ist – und damit auch der Frage, welche Mittel zu deren Abwehr angemessen sind –, hängt letztlich nicht vom Ergebnis eines Beweisverfahrens, sondern von einer Einschätzung der (in diesem frühen Stadium meist nur spärlich) vorhandenen Informationen ab. Klarheit über das Ausmass einer Gefahr kann – wenn überhaupt – immer erst im Nachhinein geschaffen werden. Wer aber unter diesen Unsicherheitsbedingungen Entscheidungen treffen muss, geht immer das Risiko ein, später mit dem Vorwurf konfrontiert zu werden, entweder zu spät und zu wenig oder aber zu viel reagiert zu haben. Die Stossrichtung des Vorwurfs dürfte in der Regel davon abhängen, ob sich die Gefahr schliesslich realisiert hat oder abgewendet werden konnte.

Die Verfassung – und auch Gesetzgebung, Rechtsprechung und Literatur – tragen den Ungewissheiten bei der Gefahrenabwehr Rechnung und sehen im Sinne der polizeilichen Generalklausel für Fälle ernster, unmittelbarer und nicht anders abwendbarer Gefahren eine Ausnahme vom Bestimmtheitsgebot vor[30]. Ist die Polizei präventiv tätig, ist sie auch ohne besondere gesetzliche Grundlage ermächtigt, unaufschiebbare Massnahmen zu treffen, um unmittelbar drohende oder eingetretene Störungen der öffentlichen Sicherheit und Ordnung abzuwehren oder zu beseitigen[31]. Damit kommt im Bereich der

---

24 Marcel Niggli/Stefan Maeder, Was schützt eigentlich Strafrecht (und schützt es überhaupt etwas?), AJP 2011, 452 f.

25 Art. 16 Abs. 1 StPO.

26 Art. 309 Abs. 1 StPO.

27 Art. 6 Abs. 1 NDG.

28 BGE 128 I 327 E. 4.

29 BGE 143 I 310 E. 3.3.1.

30 Art 36 Abs. 1 Satz 3 BV.

31 BGE 136 I 87 E. 3.1.

präventiven Tätigkeit der individuellen Interessenabwägung und der Verhältnismässigkeitsprüfung im konkreten Einzelfall die entscheidende Bedeutung zu. Zum Schutz vor schwerwiegenden, nicht anders abwendbaren Gefahren können im Präventionsbereich möglicherweise Massnahmen gerechtfertigt sein, die zur Verfolgung von begangenen Straftaten nicht in Frage kommen können[32].

Das Recht der Polizei, auch ohne gesetzliche Grundlage unaufschiebbare Massnahmen zu treffen, um unmittelbar drohende oder eingetretene Störungen der öffentlichen Sicherheit und Ordnung abzuwehren oder zu beseitigen, ist nur auf echte und unvorhersehbare sowie gravierende Notfälle ausgerichtet und auf Fälle beschränkt, in denen keine gesetzlichen Mittel vorhanden sind, um einer konkreten Gefahr zu begegnen. Die polizeiliche Generalklausel kann nicht angerufen werden, wenn typische und erkennbare Gefährdungslagen trotz deren Kenntnis nicht normiert werden[33]. Einer direkten Berufung auf die polizeiliche Generalklausel sind deshalb sehr enge Grenzen gesetzt[34]. Trotzdem bleibt zu bedenken, ob nicht bereits der Gesetzgeber bei der Reglementierung der Tätigkeit des Nachrichtendienstes, insbesondere bei genehmigungspflichtigen Beschaffungsmassnahmen, vermehrt ihre präventive Ausrichtung und die Besonderheiten von Cyber NDB berücksichtigen müsste, indem anstelle formeller Vorgaben eine Interessenabwägung und Verhältnismässigkeitsprüfung im konkreten Einzelfall in den Vordergrund gerückt wird.

Dies war im Zusammenhang mit der weitgehend unbesehenen Übernahme der strafprozessualen Bestimmungen zur Überwachung des Fernmeldeverkehrs nicht der Fall: Verstreichen bei einem vermuteten Cyberangriff für die Antragsstellung und den gerichtlichen Genehmigungsentscheid schon mindestens fünf Arbeitstage und nimmt der politische Freigabeprozess nochmals mehrere Tage[35] in Anspruch, dürfte der Angreifer – falls er eruiert und ihm die Tat nachgewiesen werden kann, die erforderlichen Rechtshilfeverfahren zum Tragen kommen und auch sonst keine strafprozessualen Probleme auftauchen – zwar eines Tages strafrechtlich verfolgt und zur Rechenschaft gezogen werden können. Der Angriff selbst dürfte aber schon längst stattgefunden und möglicherweise schwerwiegenden Schaden angerichtet haben.

Bevor Instrumente des Strafprozessrechts zur Informationsbeschaffung unbesehen auf die Tätigkeit der Präventivbehörden übertragen werden, gilt es, die unterschiedliche Zielrichtung von präventiver Straftatvereitelung und repressiver Strafverfolgung zu beachten: Für die Verhinderung einer Straftat sind nicht nur andere Informationen erforderlich, sondern auch andere Informationsbeschaffungsmethoden als für die ordentliche Strafverfolgung. Darauf soll im Folgenden näher eingegangen werden.

---

32 Dies zeigt sich etwa bei den Regelungen zum polizeilichen Schusswaffengebrauch, wonach die Polizei zum Schutz besonders wichtiger Interessen oder Rechtsgüter in einer den Umständen angemessenen Weise von der Schusswaffe Gebrauch machen (und damit einen Menschen verletzen oder möglicherweise gar töten) darf, wenn andere Mittel nicht ausreichen

33 BGE 130 I 369 E. 7.3; vgl. aber auch die mit BGE 137 II 341 E. 3.3.2 erfolgte Relativierung, jedenfalls soweit es um die Wahrnehmung staatlicher Schutzpflichten geht.

34 Vgl. Rainer Schweizer/Lucien Müller, Zwecke, Möglichkeiten und Grenzen der Gesetzgebung im Polizeibereich, LeGes2008/3, S. 383.

35 In den Anhörungen war die Rede von 10 bis 15 Tagen.

4.4 Internationales Übereinkommen über die Cyberkriminalität

Die Schweiz hat 2011 das Internationale Übereinkommen über die Cyberkriminalität (CCC)[36] 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[37].

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[38], die umgehende Weitergabe von Verkehrsdaten, welche aufgrund eines vorsorglichen Ersuchens gesichert wurden[39] sowie den direkten grenzüberschreitenden Zugriff in jenen Fällen, bei denen ein Berechtigter (etwa ein ausländischer Internetservice-Provider[40]) der Datenerhebung zugestimmt hat[41].

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 Erkenntnisse im Strafverfahren gegen den Gefährder aber nicht verwendet werden dürfen[42].

---

36 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).

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

38 Art. 29 CCC.

39 Art. 30 CCC.

40 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.

41 Art. 32 lit. b CCC.

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

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[43]. 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[44]. 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.

4.5 Besonderheiten der Informationsbeschaffung durch Cyber NDB

4.5.1 Spezifische Informationsbedürfnisse

(...)

Im Einleitungskapitel zu den Besonderheiten der Informationsbeschaffung durch Cyber NDB werden konkrete nachrichtendienstliche Arbeitsmethoden dargestellt, die der Geheimhaltungspflicht unterliegen.

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 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

---

43 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).

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

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.

4.5.2 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 (eine konkrete Bedrohung[45]), 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[46]: 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.

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. Der Chef Operationen Cyber NDB 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 kompliziert (...). 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. In die gleiche Richtung argumentierte die Steuerungsverantwortliche Cyber NDBS 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.

(...)

---

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

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

4.5.3 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[47]. Ergeben sich Anhaltspunkte auf ein möglicherweise strafbares Verhalten, zählt zu diesen anderen Dienststellen insbesondere die Bundesanwaltschaft (BA) in ihrer Eigenschaft als Strafverfolgungsbehörde des Bundes[48], soweit für die Verfolgung der entsprechenden Delikte die Bundesgerichtsbarkeit[49] 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 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[50]. 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.

(...)

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 wer-

47 Art. 6 Abs. 3 NDG.
48 Art. 2 Abs. 1 des Strafbehördenorganisationsgesetzes (StBOG).
49 Art. 23f. StPO.
50 Anhörung Miriam Hayryam/Peter Haag, S. 31.

den sollen – wesentlich zu vereinfachen und im Gegenzug in Kauf zu nehmen, dass sie in einem späteren Strafverfahren nicht verwendet werden können.

4.5.4 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.

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[51]. Folgerichtig soll auch bei den genehmigungspflichtigen Überwachungsmassnahmen der strikte Bezug zu einer konkreten und unmittelbaren Bedrohung der Sicherheitsinteressen der Schweiz gelockert werden.

---

51 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).

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[52]. 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 ausgeräumt sein. Gelöst sind damit aber keineswegs sämtliche Probleme, die sich im Zusammenhang mit der Genehmigungspflicht bzw. mit dem Genehmigungsverfahren stellen können.

4.6 Revision der genehmigungspflichtigen Beschaffungsmassnahmen

4.6.1 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[53]. 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[54]. Der damit verbundene Eingriff in das Fernmeldegeheimnis wiegt deshalb bei Randdaten "deutlich weniger schwer" als in den Fällen der inhaltlichen Kommunikationsüberwachung[55]. 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

---

52 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, S. 11 (https://www.vbs.admin.ch/de/sicherheit/nachrichtenbeschaffung/nachrichtendienstgesetz.detail.document.html/vbs-internet/de/documents/nachrichtendienst/nachrichtendienstgesetz/Erlaeuternder-Bericht-Revision-Bundesgesetz-Nachrichtendienst-d.pdf.htm).

53 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.

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

55 BGE 139 IV 98 E. 4.2.

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[56].

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[57]. Dies ist selbst dann nicht genehmigungspflichtig, wenn die Staatsanwaltschaft zu diesem Zweck beim Dienst ÜPF die Herausgabe des PUK-Codes verlangt[58]. 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[59].

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

56 Vgl. etwa Art. 95 Abs. 2 StPO für die Beschaffung von Personendaten.
57 BGE 143 IV 270 E.4.6; vgl. auch BGE 140 IV 181 E. 2.
58 BGE 141 IV 423 E. 1.
59 BGer 1B_26/2016 E.4.2-4.4.

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

4.6.2 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[61]. 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[62] – Monate verstreichen.

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 Überwa-

---

60 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).

61 Art. 27 Abs. 2 NDG.

62 Vgl. Art. 29 Abs. 5 NDG.

chungsmassnahmen 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[63]. 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[64]. Diese Regelung ist jedoch auf Ausnahmefälle zugeschnitten[65] 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 werden und sich demzufolge der Eingriff nach der Praxis des Bundesgerichts als "deutlich weniger einschneidend" erweist[66]. 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.

63 Vgl. Art. 274 Abs. 1 StPO.
64 Art. 31 Abs. 1 NDG.
65 Botschaft zum Nachrichtendienstgesetz (Fn.10), BBl 2014, 2163.
66 BGE 142 IV 34 E. 4.3.2; BGE 139 IV 98 E. 4.2.

5 Strafrechtliche Relevanz der Vorkommnisse im Ressort Cyber NDB

5.1 Beurteilung durch die interne Untersuchung des NDB

(...)

Im Rahmen der internen Untersuchung wurde die Frage offengelassen, ob und allenfalls welche Straftatbestände im Zusammenhang mit der unrechtmässigen Informationsbeschaffung durch Cyber NDB erfüllt sein könnten. Als möglicherweise in Betracht fallende Straftatbestände wurden genannt: 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); im Weitern wurde auf eine mögliche Teilnahme durch Anstiftung hingewiesen.

5.2 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[67]) zur Diskussion steht, wird es trotzdem unumgänglich sein, auch zu den einzelnen Straftatbeständen Stellung zu nehmen.

(...)

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[68]. 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[69].

---

67 Art. 24 f. StGB.

68 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".

69 BGer 6B_833/2019 E. 2.4.2.

5.3 Bemerkungen zu den einzelnen Straftatbeständen

5.3.1 Unbefugte Datenbeschaffung (Art. 143 StGB)

Bei sämtlichen (...) aufgelisteten Straftatbestände handelt es sich um Vorsatzdelikte. Bei der unbefugten Datenbeschaffung wird zusätzlich eine Bereicherungsabsicht des Täters verlangt.

(...)

Eine Bereicherungsabsicht im Zusammenhang mit der fehlenden Einholung der für geheime Beschaffungsmassnahmen erforderlichen Genehmigungen kann ausgeschlossen werden.

5.3.2 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[70]. Es erlischt nach Ablauf von drei Monaten, nachdem der antragsberechtigten Person der Täter bekannt wird[71]. Ein Strafantrag liegt nicht vor, und es ist auch nicht ersichtlich, welche Person ihn realistischerweise stellen könnte[72].

5.3.3 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[73].

---

70 Art. 30 Abs. 1 StGB.

71 Art. 31 StGB.

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

73 Art. 26 StGB.

Der Bericht (...) 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. 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[74].

Der fragliche Entscheid ist nicht nur in der Lehre auf massive Kritik gestossen[75], sondern führte auch zu einer Verurteilung der Schweiz durch den Europäischen Gerichtshof für Menschenrechte wegen Verletzung der Meinungsäusserungsfreiheit[76]. 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[77] 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[78]. 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 (...) kaum gegeben sein. Wie (...) dokumentiert ist, 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[79] verlangt würde, kann keine Rede sein.

5.3.4 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 Persönlichkeitsrechte der Betroffenen gegen Beeinträchtigungen irgendwelcher Art. Sie erfassen nur einzelne Aspekte des Persönlichkeitsschutzes, insbesondere die Verletzung des

---

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

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

76 EGMR 24.04.2006; Requête n° 77551/01.

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

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

79 Art. 24 Abs. 1 StGB.

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[80], 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.

(...) 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[81]. 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.

5.4 Fehlender Vorsatz bzw. Irrtum über die Rechtswidrigkeit

5.4.1 Vorsatz und Irrtum

Letztlich kann es dahingestellt bleiben, ob allenfalls der objektive Tatbestand irgendeiner Strafbestimmung erfüllt sein könnte. Sämtliche im Zusammenhang mit der Datenbe-

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

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

schaffung- 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[82]. 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[83]. 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[84]. 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.

5.4.2 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[85]. 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[86]. Diese Regelung beruht auf dem Gedanken, dass sich der dem Recht Unterworfene um die Kenntnis der Rechtslage zu bemühen hat und deren Unkenntnis nur in besonderen Fällen vor Strafe schützt[87].

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

82 Art. 12 Abs. 1 und 2 StGB.
83 Art. 13 StGB.
84 Art. 21 StGB.
85 Stefan Trechsel/Bijan Fateh-Moghadam, Schweizerisches Strafgesetzbuch Praxiskommentar, 4. Aufl., Zürich 2021, N. 1 zu Art. 21 StGB.
86 BGE 104 IV 217 E. 3a.
87 BGE 129 IV 238 E. 3.1.

besonderen Natur und erhöhten Komplexität nicht erkennen konnte und deshalb auf die Auskünfte eines eigens dafür beigezogenen Rechtsberaters abstellte[88].

Eine irreführende Auskunft oder Anweisung der zuständigen Behörde bildet regelmässig eine ausreichende Grundlage für einen unvermeidbaren Verbotsirrtum[89]. 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[90].

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

5.4.3 Kontroversen über die Rechtmässigkeit staatlichen Handelns

Sämtliche Beteiligten des NDB, die in irgendeiner Weise an der auf freiwilliger Basis erfolgten (Informationsbeschaffung) involviert waren, handelten in der – wenn auch irrigen – Annahme, dass ihr Vorgehen in rechtlicher Hinsicht durch Art. 23 NDG (bzw. da-

88 BGE 98 IV 293 E. 4a.

89 Stefan Trechsel/Bijan Fateh-Moghadam (Fn. 85), N. 11 zu Art. 21 StGB.

90 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.

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

mals durch Art. 14 Abs. 2 BWIS) gedeckt ist. Die irrtümliche Annahme, ein tatbestandsmässiges Verhalten sei im konkreten Fall rechtmässig, weil ein Rechtfertigungsgrund[92] 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[93].

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 (...). 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 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[94]. Zu erinnern ist in diesem Zusammenhang etwa an die Entscheide zur verdeckten Ermitt-

---

92 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."

93 BGE 116 IV 56 E. II 3a.

94 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.

lung in Chat-Räumen[95], zu Alkoholtestkäufen bei Jugendlichen[96], zu Scheinkäufen bei Drogendelikten[97] oder auch zu den Sozialdetektiven[98]. Das sind alles Entscheide, die – wie hier – Beschaffungsmassnahmen ohne Einholung der erforderlichen Genehmigungen zum Gegenstand hatten.

5.4.4 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[99]. Ihren Stellungnahmen kommt somit erhebliches Gewicht zu. Die AB-ND hat im August 2021 einen Prüfbericht i.S. (...) 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 (...) hinsichtlich der Einsichtnahme in Randdaten des Datenverkehrs als rechtskonform gelten dürfe bzw. welche Voraussetzungen dazu erfüllt sein müssten. Diese Empfehlung hat der NDB unverzüglich umgesetzt, die bisherige Praxis der Datenbeschaffung sofort eingestellt und (...) 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 (...) 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 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.

5.4.5 Opportunität einer Strafanzeige

Gewiss, definitive Klarheit bei der Subsumierung eines konkreten Verhaltens unter einen bestimmten Straftatbestand können nur Staatsanwaltschaft und Strafgerichte schaffen.

---

95 BGE 134 IV 266.
96 BGer 6B_272/2009.
97 BGer 6B_743/2009.
98 BGE 143 I 377.
99 Art. 78 NDG.

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 (...), 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 (...) 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[100], 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 – 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[101]. 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.

---

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

101 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.

Hinzu kommt schliesslich, dass es sich bei den zur Diskussion stehenden Straftatbeständen[102] 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[103]. Die für den Entscheid über die Einleitung oder Nichteinleitung eines Strafverfahrens erforderlichen Informationen liegen der Bundesanwaltschaft bereits heute in den wesentlichen Grundzügen vor (...). 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.

---

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

103 Art. 7 Abs. 1 StPO.