Dr. Niklaus Oberholzer
Rechtsanwalt
Kesselhaldenstrasse 55
9016 St. Gallen

mail@niklausoberholzer.ch

Vorkommnisse im Ressort Cyber des Nachrichtendienstes des Bundes

Bericht der Administrativuntersuchung

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

15. August 2022

Zusammenfassung

Das Ressort Cyber ist eine Organisationseinheit innerhalb des Nachrichtendienstes des Bundes (NDB) und hat zur Aufgabe, Cyberangriffe auf Computersysteme zu erkennen, zu analysieren und nach Möglichkeit zu verhindern. Cyber NDB befasst sich vorwiegend mit Angriffen, die auf Spionage ausgerichtet sind und von staatlichen Akteuren ausgehen. Für nichtstaatliche Akteure (etwa Cyberkriminelle) sind in erster Linie das Nationale Zentrum für Cybersicherheit (NCSC) und die Melde- und Analysestelle Informationssicherung (MELANI) oder die kantonalen Strafverfolgungsbehörden zuständig.

Gewisse Vorkommnisse im Ressort Cyber veranlassten den vormaligen Direktor NDB im April 2021, eine interne Untersuchung anzuordnen. Diese führte im Dezember 2021 zur Erkenntnis, dass der Nachrichtendienst im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen in den Jahren 2015 bis 2020 auch Informationen über Netzwerkverkehrsdaten beschafft und bearbeitet hatte. Diese Randdaten des Fernmeldeverkehrs stehen unter dem Schutz des Fernmeldegeheimnisses und können nur unter Einhaltung der Bestimmungen des Nachrichtendienstgesetzes 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.

Die Erkenntnisse der internen Untersuchung werden in der hier vorliegenden Administrativuntersuchung im Wesentlichen bestätigt. Die Administrativuntersuchung führte hinsichtlich der Informationsbeschaffungsprozesse zu keinen wesentlich neuen Feststellungen. Die Abläufe im Ressort Cyber wurden im fraglichen Zeitraum nicht systematisch erfasst und dokumentiert, sodass sich eine nachträgliche Rekonstruktion der Vorgänge im Einzelnen als unmöglich erweist. Dies ändert jedoch nichts an der Feststellung, dass Cyber NDB während Jahren Daten ohne Einhaltung der gesetzlichen Bestimmungen und damit unrechtmässig beschafft hat.

Dabei ist jedoch zu relativieren, dass es sich bei den auf diese Weise beschafften Informationen nicht um besonders schützenwerte Personendaten, sondern um Randdaten des Netzwerkverkehrs gehandelt hatte, die primär einer rein technischen Analyse unterzogen wurden. Anhaltspunkte, dass daraus für individuelle Personen ein Nachteil entstanden sein könnte, liegen nicht vor.

Cyber NDB wurde 2014 unter hohem Zeit- und Erwartungsdruck aufgebaut. Vertiefte Abklärungen über Organisationsstrukturen, Prozesse und Abläufe wurden nicht getätigt. Eine Analyse der besonderen Informationsbedürfnisse des neuen Ressorts, das nicht eines der klassischen Themenfelder des Nachrichtendienstes bearbeitet, sondern vorwiegend auf die Auswertung digitaler Kommunikationsmittel und -wege ausgerichtet ist, fand nicht statt.

Obwohl Cyber NDB offensichtlich nicht in die vorhandenen Strukturen passte, herrschte die Auffassung vor, dass eine Einbindung ohne jegliche Anpassungen möglich sei. Dies erweist sich im Nachhinein als Fehleinschätzung. Es wird Aufgabe von Direktion und Geschäftsleitung sein, eine Auslegeordnung vorzunehmen und Massnahmen zu einer Neustrukturierung von Cyber NDB in die Wege zu leiten.

Bei der Einführung von Cyber NDB blieb es weitgehend dem damals neu ernannten Chef überlassen, die aus seiner Sicht geeigneten und erforderlichen Vorkehrungen zu treffen, um die in das Ressort gesetzten Erwartungen erfüllen zu können. Cyber NDB ging von einer

besonderen Stellung aus und entwickelte zunehmend eigene Methoden der Datenbeschaffung und -bearbeitung.

Das Eigenleben des Ressorts war auf der Führungsebene des Nachrichtendienstes, wenn auch nicht in allen Details, so doch in den Grundzügen bekannt. Der unmittelbare Vorgesetzte und auch die Geschäftsleitung hatten Kenntnis davon, dass sich die Arbeit von Cyber NDB im Wesentlichen auf die Auswertung von Randdaten des Netzwerkverkehrs stützte. Ebenso war allgemein bekannt, dass das Ressort die von ihm als notwendig erachteten Informationen weitgehend selbst beschaffte und nicht auf [redacted] zuständigen Direktionsbereichs [redacted] zurückgriff. Nachfragen zur konkreten Ausgestaltung der Arbeitsmethoden von Cyber NDB erfolgten trotzdem nicht. Unverständlich erscheint heute, dass die Geschäftsleitung und insbesondere der zuständige Direktionsbereichsleiter und Vorgesetzte bis September 2020 keine Kenntnis von der während Jahren praktizierten unrechtmässigen Datenbeschaffung des Ressorts hatten. Dies lässt eigentlich nur den Schluss zu, dass es an einer effizienten Führung und Beaufsichtigung fehlte.

Der NDB hat im Rahmen der internen Untersuchung eine externe Anwaltskanzlei beauftragt, eine rechtliche Beurteilung der Informationsbeschaffung und -bearbeitung im Zusammenhang mit Cyberangriffen vorzunehmen. Diese Beurteilung beruhte auf der Grundlage des geltenden Rechts und in Berücksichtigung der vom NDB vorgegebenen hypothetischen Sachverhaltsschilderungen und abstrakten Fragestellungen. Eine Auseinandersetzung mit den besonderen nachrichtendienstlichen Bedürfnissen und mit der Praxistauglichkeit der für den Nachrichtendienst geltenden Bestimmungen erfolgte damals, dem erteilten Auftrag entsprechend, nicht.

In der Administrativuntersuchung zeigte sich, dass die weitgehend unbesehene Überführung der im Strafprozessrecht entwickelten Regeln für genehmigungspflichtige Beschaffungsmassnahmen in das Nachrichtendienstgesetz zu hinterfragen ist. Während die Strafverfolgung repressiven Zwecken dient, ist die Tätigkeit des Nachrichtendienstes auf die präventive, frühzeitige Erkennung von Bedrohungslagen und Gefährdungen ausgerichtet. Diese unterschiedliche Zielsetzung verlangt unterschiedliche Arbeitsmittel und -methoden.

Die Analyse von Netzwerkverkehrsdaten zur Erkennung und Abwehr eines Cyberangriffs erfolgt nicht personen-, sondern primär gerätebezogen. Im Vordergrund steht eine Auswertung der Modalitäten des Datenverkehrs als solche, um daraus Rückschlüsse auf die Herkunft und Zielrichtung des Angriffs ziehen zu können. Dabei kommt dem Zeitfaktor eine entscheidende Bedeutung zu, da Angreifer ihre Mittel und Methoden ständig wechseln. Eine Verwendung der so erlangten Daten in einem späteren Strafverfahren ist theoretisch zwar denkbar, praktisch aber ausgeschlossen, weil die Angriffe in der Regel aus dem Ausland erfolgen, womit in dieser Konstellation die zur Verfolgung ausländischer, staatlicher Akteure erforderliche internationale Rechtshilfe nicht zu erlangen ist.

Angesichts des hohen Schadenspotenzials eines Cyberangriffs und der geringen Eingriffsintensität bei der Beschaffung von Randdaten des Netzwerkverkehrs, der vorwiegend technisch und nicht personenbezogenen Analyse der 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 der nachrichtendienstlichen Tätigkeit es und in Abstimmung mit den von der Schweiz eingegangenen Verpflichtungen zur internationalen Zusammenarbeit auf dem Gebiet der Cyberabwehr, erscheint es erforderlich und zugleich gerechtfertigt, die Beschaffung von Netzwerkverkehrsdaten durch den

NDB – jedenfalls soweit diese allein der Erkennung und Abwehr von Cyberangriffen dienen – wesentlich zu vereinfachen. Letztlich wird die Politik entscheiden müssen, welche Prioritäten sie im Bereich der Cyberabwehr setzen will. Dabei stellt sich die Frage, ob sie eine effiziente Früherkennung und Abwehr von Angriffen oder eine spätere, wenn auch keineswegs sichere Strafverfolgung der Täterschaft im Rahmen eines den Grundsätzen der Strafprozessordnung entsprechenden Strafverfahrens anstrebt.

Schliesslich bleibt noch die Frage nach einer allfälligen strafrechtlichen Relevanz der unrechtmässigen Datenbeschaffung zu klären: Sämtliche in irgendeiner Weise – sei es durch Handeln oder Unterlassen – beteiligten Mitarbeitenden des NDB gingen davon aus, dass sie berechtigt sind, Meldungen und Auskünfte von Drittpersonen entgegenzunehmen, solange dies freiwillig erfolgte. Dass dies für Daten des Fernmeldeverkehrs nicht ohne weiteres gilt, erkannten sie nicht. Auch wenn sich ihre Annahme im Nachhinein als falsch herausgestellt hat und Bestimmungen des Nachrichtendienstgesetzes verletzt worden sind, genügt die blosse Erfüllung des objektiven Straftatbestands für eine Bestrafung nicht. Nachdem es sich bei sämtlichen in Frage kommenden Straftatbeständen um Vorsatzdelikte handelt, müssten diese Personen vorsätzlich, d.h. mit Wissen und Wollen und zudem auch schuldhaft gehandelt oder pflichtwidrig untätig geblieben sein. Obschon Rechtsunkenntnis in der Regel nicht vor Strafe schützt, anerkennen das Gesetz und die darauf beruhende Rechtsprechung, dass nicht schuldhaft handelt, wer bei der Begehung der Tat nicht weiss und auch nicht wissen kann, dass er sich rechtswidrig verhält.

Meinungsverschiedenheiten über die korrekte Auslegung von Verfahrensbestimmungen bzw. über die Rechtmässigkeit bzw. Unrechtmässigkeit staatlichen Handelns zählen zum Alltag jeder Behörde und jeder Beamtin und jedes Beamten. Dies zeigt sich besonders deutlich in Bereichen, in denen Behörden staatliche Zwangsmassnahmenbefugnisse zukommen und damit berechtigt sind, in – vielfach auch strafrechtlich – geschützte Grundrechte einzugreifen. Dass die dabei vorzunehmende Abwägung auch zu unterschiedlichen Beurteilungen führen kann, ist vorgegeben. Das Recht räumt deshalb den Betroffenen vielfache Beschwerdemöglichkeiten ein, um fehlerhafte oder gar unrechtmässige Entscheide durch eine übergeordnete Instanz überprüfen und gegebenenfalls korrigieren zu lassen. Dabei dürfte es sich von selbst verstehen, dass nicht jede geschützte Beschwerde (z.B. eine Haftbeschwerde) zur Eröffnung eines Strafverfahrens gegen den verfügenden Beamten (bei einer Haftbeschwerde wegen Freiheitsberaubung) führen muss. Das Gleiche muss auch gelten, wenn eine langjährige, auf falscher Rechtsauslegung beruhende Praxis sich im Nachhinein als unrechtmässig erweist.

Soweit es vorliegend um die Unvermeidbarkeit der irrigen Rechtsauslegung durch Mitarbeitende des NDB geht, ist mit entscheidend, dass auch die Aufsichtsbehörde über den Nachrichtendienst (AB-ND) detaillierte Kenntnis über die Modalitäten der Datenbeschaffung durch Cyber NDB hatte: Sie thematisierte zwar die rechtliche Problematik, verzichtete aber trotzdem darauf, Sofortmassnahmen in die Wege zu leiten. Noch in ihrem Prüfbericht vom August 2021 vertrat sie den Standpunkt, dass es sich bei der auf freiwilliger Basis erfolgten Herausgabe bzw. Entgegennahme von Daten des Netzwerkverkehrs um einen rechtlichen Graubereich handle, der vom NDB näher abzuklären sei. Hat selbst die eigene Aufsichtsbehörde die Problematik einer unrechtmässigen, möglicherweise gar strafbaren, Datenbeschaffung nicht in ihrem vollen Ausmass erkannt, muss auch den Mitarbeitenden des NDB zugestanden werden, dass sie sich mit ihrer falschen Rechtsauslegung in einem unvermeidbaren Irrtum über die Rechtswidrigkeit befunden haben.

Inhalt

1 Fragestellung und Vorgehen

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) beauftragte den Unterzeichnenden am 27. Januar 2022 mit der Durchführung einer Administrativuntersuchung betreffend Vorkommnisse im Ressort Cyber des Nachrichtendienstes des Bundes (NDB).

1.1 Ausgangslage

Cyber NDB ist ein Ressort innerhalb des Nachrichtendienstes und war bis Januar 2022 organisatorisch dem Direktionsbereich Informationsmanagement/Cyber NDBI unterstellt[1]. Es hat den Auftrag, Cyberangriffe auf Computersysteme zu erkennen, zu analysieren und zu verhindern, sofern sie einen Bezug zum Schutz kritischer Infrastrukturen der Schweiz, zu terroristischen, gewalttätigen oder nachrichtendienstlichen Aktivitäten oder zu sicherheitspolitischen Vorgängen im Ausland aufweisen.

Nachdem der NDB Kenntnis von möglichen Unregelmässigkeiten erhalten hatte, erteilte der damalige Direktor NDB[2] im April 2021 der Abteilung Sicherheit NDB den Auftrag zur Durchführung einer internen Untersuchung. Die Untersuchung wurde im Dezember 2021 abgeschlossen. Sie führte zur Erkenntnis, dass der Nachrichtendienst im Zeitraum von 2015 bis 2020 im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen auch Informationen über Netzwerkverkehrsdaten beschafft hatte. Derartige Informationen stehen grundsätzlich unter dem Schutz des Fernmeldegeheimnisses. Sie können nach den massgebenden Bestimmungen des Nachrichtendienstgesetzes (NDG) nur in Form einer genehmigungspflichtigen Beschaffungsmassnahme (GEBM) angeordnet werden und bedürfen der Genehmigung durch das Bundesverwaltungsgericht (BVGer) und der politischen Freigabe durch die Vorsteherin VBS. Ein derartiges Bewilligungsverfahren wurde vom NDB nie eingeleitet. Von diesen Vorgängen waren ausländische Angreifer betroffen, die für ihre Cyberangriffe Server in der Schweiz (mit)benutzt hatten. Der NDB hat diese Aktivitäten des Ressorts Cyber nach Vorliegen der ersten detaillierten Meldungen über mögliche Unregelmässigkeiten eingestellt und verschiedene Massnahmen eingeleitet, um die Rechtmässigkeit der Informationsbeschaffung sicherzustellen.

Das VBS hat in der Folge im Dezember 2021 die Geschäftsprüfungsdelegation der Eidgenössischen Räte (GPDel) und die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND) über diese Vorkommnisse und die in der Zwischenzeit eingeleiteten Massnahmen informiert und im Januar 2022 die Durchführung einer Administrativuntersuchung angeordnet[3].

Die GPDel befasste sich bereits seit August 2021 mit dem als rechtlich problematisch erachteten "Geschäftsmodell" des Ressort Cyber NDB. Nach Kenntnisnahme der Ergebnisse der internen Untersuchung sah die GPDel keine Veranlassung, ihre laufenden

---

1 Das Ressort Cyber NDB wurde im Januar 2022 neu dem Direktionsbereich [redacted] unterstellt.

2 Jean-Philippe Gaudin, im Amt vom 01.07.2018 bis 31.08.2021.

3 Siehe Medienmitteilung des Bundesrats vom 26.01.2022.

Abklärungen in eine formelle Inspektion zu überführen. Damit stellt sich die Frage ihrer Ermächtigung[4] zu der vom VBS in Auftrag gegebenen Administrativuntersuchung nicht[5].

1.2 Auftrag und Gegenstand

Der Auftrag des VBS lautet wie folgt:

"Der Auftragnehmer führt eine Administrativuntersuchung im Sinne von Artikel 27a ff. Regierungs- und Verwaltungsverordnung (RVOV; SR 172.010.1) betreffend die Vorkommnisse im Ressort Cyber des NDB durch. Es ist abzuklären, ob ein Sachverhalt vorliegt, der im öffentlichen Interesse Massnahmen erfordert.

Dazu gilt es den Direktionsbereich Informationsmanagement/Cyber des NDB einer Aufgaben-, Leistungs- und Organisationsüberprüfung zu unterziehen. Dies mit dem Zweck die in der Ausgangslage dargelegten Vorkommnisse aufzuarbeiten um wenn angezeigt, weitere Schritte einleiten zu können. Es sind folgende Punkte abzuklären:

- Klärung und Darstellung sämtlicher Führungsabläufe innerhalb des NDB, welche im Zusammenhang mit der in der Ausgangslage beschriebenen Problematik stehen. Dies mit dem Ziel beurteilen zu können, welche Personen, wann, welche Entscheide getroffen haben.
- Prüfung, ob die Organisationsform des Direktionsbereichs Informationsmanagement/Cyber zur Aufgabenerfüllung zweckmässig ausgestaltet ist.
- [redacted]
- Klärung, inwiefern eine Weitergabe von Malware-Samples an Dritte, namentlich die [redacted], stattgefunden hat.
- Klärung sämtlicher Geldflüsse in diesem Zusammenhang.
- Klärung, ob bei den untersuchten Vorgängen eine strafrechtliche Relevanz vorliegt. Insbesondere ist zu klären, ob es zu einer Umgehung von rechtlichen Bestimmungen (bewilligungspflichtigen Beschaffungsmassahmen) gekommen ist."

1.3 Rechtsgrundlagen[6]

Die Administrativuntersuchung ist ein spezielles Verfahren im Rahmen der ständigen und systematischen Aufsicht des Bundesrats über die Bundesverwaltung, mit der abgeklärt wird, ob ein Sachverhalt vorliegt, der im öffentlichen Interesse ein Einschreiten von Amtes wegen erfordert. Sie richtet sich nicht gegen bestimmte Personen, sondern dient der vertieften Abklärung von besonderen Fragestellungen, die sich aus aktuellen

---

4 Nach Art. 154a Abs. 1 des Parlamentsgesetzes (ParlG) dürfen Disziplinaruntersuchungen oder Administrativuntersuchungen des Bundes, die Sachverhalte oder Personen betreffen, welche bereits Gegenstand einer Untersuchung durch die Geschäftsprüfungsdelegation sind, nur mit Ermächtigung der Geschäftsprüfungsdelegation angehoben oder weitergeführt werden.

5 Siehe Medienmitteilung der GPDel vom 27.01.2022.

6 Vgl. zum Ganzen Art. 8 Abs. 3 Regierungs- und Verwaltungsorganisationsgesetz (RVOG) und insbesondere Art. 25 und 7a ff. Regierungs- und Verwaltungsorganisationsverordnung (RVOV); sowie die Berichte zu Administrativ- und Disziplinaruntersuchungen in der Bundesverwaltung der Geschäftsprüfungskommission (GPK) des Nationalrates vom 19. November 2019 (BBl 2020, S. 1659 ff.) und der Parlamentarischen Verwaltungskontrolle (PVK) vom 17. Juni 2019 (BBl 2020, S. 1681 ff.).

Ereignissen oder festgestellten Missständen ergeben[7]. Eine solche Untersuchung kann Personen ausserhalb der Bundesverwaltung übertragen werden[8]. Zur Feststellung des Sachverhalts bedient sich das Untersuchungsorgan der Beweismittel nach Art. 12 des Bundesgesetzes über das Verwaltungsverfahren (VwVG); in einer Administrativuntersuchung finden jedoch keine Zeugeneinvernahmen statt[9].

Die Administrativuntersuchung stellt kein eigentliches Verwaltungsverfahren dar, weshalb es auch keine Parteien gibt. Die betroffenen bzw. befragten Personen haben die Rechtsstellung einer Auskunftsperson; sie können weder Parteirechte geltend machen noch sind sie beschwerdelegitimiert. Auch der Schlussbericht stellt keine autoritative Verfügung dar, mit welcher Rechte oder Pflichten begründet, geändert oder aufgehoben werden, sodass dagegen kein Rechtsmittel gegeben ist[10].

Die in die Administrativuntersuchung einbezogenen Behörden und Angestellten des Bundes sind verpflichtet, an der Feststellung des Sachverhalts mitzuwirken[11]. Die Mitwirkungspflicht erstreckt sich nicht auf Personen ausserhalb der Bundesverwaltung. Die befragten Personen unterliegen einer Aussagepflicht, wenn sie Angestellte der Verwaltungsstelle sind, welche die Administrativuntersuchung in Auftrag gegeben hat[12]. Das Untersuchungsorgan weist Personen, die befragt werden sollen, darauf hin, dass sie die Aussage verweigern können, wenn sie sich mit dieser im Hinblick auf ein allfälliges Disziplinar- oder Strafverfahren selbst belasten würden. Es weist Personen ausserhalb der Bundesverwaltung darauf hin, dass ihre Auskunftserteilung freiwillig erfolgt[13]. Die einbezogenen Behörden und Angestellten des Bundes haben Gelegenheit, alle Akten, die sie betreffen, einzusehen und dazu Stellung zu nehmen. Sie haben Anspruch auf rechtliches Gehör[14].

Jedenfalls dann, wenn die Ergebnisse einer Administrativuntersuchung in einem sich daran anschliessenden Verfahren verwendet werden sollen, müssen die Verfahrensgrundsätze gewahrt werden. Dazu gehört insbesondere, dass den Betroffenen das rechtliche Gehör gewährt wird und das Verfahren angemessen dokumentiert ist[15].

Das Untersuchungsorgan liefert der anordnenden Stelle am Schluss sämtliche Untersuchungsakten sowie einen Bericht ab. Es stellt im Bericht den Ablauf sowie die Ergebnisse der Untersuchung dar und präsentiert Vorschläge für das weitere Vorgehen. Ein vorgängiges Äusserungsrecht der von der Administrativuntersuchung betroffenen Verwaltungsstelle ist nicht vorgesehen. Vielmehr informiert die anordnende Selle die in die Administrativuntersuchung einbezogenen Behörden und Personen über das Ergebnis[16].

---

7 Art. 27a RVOV.

8 Art. 27d Abs. 2 RVOV.

9 Art. 27g Abs. 1 RVOV.

10 Gutachten zuhanden der PVK von Felix Uhlmann und Jasmina Bukovac betreffend Administrativ- und Disziplinaruntersuchungen in der Bundesverwaltung vom 15. Mai 2019 (https://www.parlament.ch/centers/documents/de/gutachten-uhlmann-2019-05-16.pdf).

11 Art. 27g Abs. 2 RVOV.

12 Gutachten Uhlmann/Bukovac (Fn. 10), S. 19.

13 Art. 27h Abs. 2 und 3 RVOV.

14 Art. 27g Abs. 4 und 5 RVOV.

15 Bericht GPK NR zu Administrativ- und Disziplinaruntersuchungen in der Bundesverwaltung (Fn. 6), BBl 2020, S. 1668.

16 Art. 27j RVOV.

1.4 Beigezogene Unterlagen und eigene Abklärungen

1.4.1 Zur Verfügung gestellte Akten

Das VBS überliess dem Untersuchungsbeauftragten zu Beginn des Auftrags den von der Abteilung Sicherheit NDB verfassten Bericht über ihre Abklärung der "Rechtmässigkeit der Vorgänge bei Cyber NDB" vom 17. Dezember 2021. Die darin vorgenommene rechtliche Würdigung stützt sich ihrerseits auf den vom NDB im Rahmen der internen Untersuchung bei einer externen Anwaltskanzlei eingeholten Bericht "Rechtliche Beurteilung zur Informationsbeschaffung und -bearbeitung im Zusammenhang mit Cyberangriffen"[17]; das VBS stellte diesen Bericht dem Untersuchungsbeauftragten ebenfalls zur Verfügung.

1.4.2 Eigene Ermittlungen

Der Untersuchungsbeauftragte zog diverse Beilagen zum internen Bericht der Abteilung Sicherheit NDB, darunter sämtliche Protokolle der durchgeführten Befragungen, und weitere Unterlagen bei. Die Zusammenarbeit mit dem NDB und seinen Mitarbeitenden erwies sich als konstruktiv; es wurden sämtliche Fragen – soweit möglich – beantwortet und alle verlangten Unterlagen zur Verfügung gestellt.

Im Verlauf der Administrativuntersuchung hörte der Untersuchungsbeauftragte sodann folgende Personen an:

- Jürg Bühler, stellvertretender Direktor NDB/[redacted]
- [redacted] Vizedirektor NDB, Chef Informationsmanagement/Cyber (NDBI)
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted][18]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Für die Befragungen wurde in Absprache mit dem Auftraggeber [redacted] als Protokollführer beigezogen. [redacted] war bis zu seiner Pensionierung Ende 2021 als [redacted] tätig.

---

17 Anwaltskanzlei [redacted], Rechtliche Beurteilung zur Informationsbeschaffung und -bearbeitung im Zusammenhang mit Cyberangriffen vom 29. November 2021 (im Folgenden Rechtsgutachten genannt).

18 [redacted]

1.4.3 Rechtliches Gehör

Die befragten Personen wurden als Auskunftspersonen befragt und zu Beginn der Befragung auf ihr Aussageverweigerungsrecht hingewiesen. Die Befragungen wurden in deren Einverständnis auf Tonband aufgezeichnet. Gestützt darauf wurde ein schriftliches Protokoll erstellt und den Betroffenen zur Einsichtnahme und Genehmigung zugestellt[19].

Nicht das Untersuchungsorgan, sondern die anordnende Stelle informiert die in eine Administrativuntersuchung eingezogenen Behörden und Personen über das Ergebnis der Untersuchung[20]. In Absprache mit dem VBS wurde deshalb darauf verzichtet, den vorliegenden Bericht dem NDB zur vorgängigen Stellungnahme zu unterbreiten.

---

19 Das Bundesgericht verlangt selbst bei der Befragung im Rahmen einer Personensicherheitsüberprüfung nicht, dass das auf Tonträger gespeicherte Gespräch nachträglich noch in voller Länge und in seinem genauen Wortlaut in die schriftliche Form übertragen wird. Es lässt es dabei bewenden, dass der wesentliche Inhalt des Gesprächs schriftlich festgehalten wird, der Befragte Gelegenheit erhält, die Tonbänder im ganzen Umfang und im Original zu hören und er sich dazu uneingeschränkt äussern kann (BGE 130 II 473 E. 4 und 5).

20 Art. 27j Abs. 3 RVOV (siehe auch Ziffer 1.3, Seite 10).

2 Cyber NDB im Gesamtgefüge der Strategie zum Schutz vor Cyberrisiken

2.1 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

Der Bundesrat hat im April 2018 die zweite Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022 verabschiedet[21]. Der Bericht des Informatiksteuerungsorgans des Bundes (ISB) betont, dass der Schutz vor Cyberrisiken in der gemeinsamen Verantwortung von Wirtschaft, Gesellschaft und Staat liegt. Aus der gemeinsamen Verantwortung ergebe sich auch die gemeinschaftliche Umsetzung der Strategie. Bund, Kantone, Wirtschaft und Gesellschaft sollen die Massnahmen der NCS in enger Kooperation implementieren und dabei ihre jeweiligen Kompetenzen einbringen. Die Herausforderungen im Umgang mit Cyber seien gross, und sie würden weiter virulent bleiben. Umso wichtiger sei es, dass alle Akteure gemeinsam und koordiniert diese Herausforderungen angehen. Eine möglichst enge Zusammenarbeit aller kompetenten Stellen und eine systematische internationale Vernetzung seien entscheidend für die Schaffung eines sicheren Umfeldes für die Digitalisierung der Gesellschaft und der Wirtschaft[22].

Im Bericht werden folgende strategische Ziele genannt:[23]

- "Die Schweiz verfügt über die Kompetenzen, das Wissen und die Fähigkeiten, Cyber-Risiken frühzeitig zu erkennen und einzuschätzen.
- Die Schweiz entwickelt wirksame Massnahmen zur Reduktion der Cyber-Risiken und setzt diese im Rahmen der Prävention um.
- Die Schweiz verfügt in allen Lagen über die nötigen Kapazitäten und Organisationsstrukturen, um Cyber-Vorfälle rasch zu erkennen und auch dann zu bewältigen, wenn diese über längere Zeit andauern und verschiedene Bereiche gleichzeitig betreffen.
- Die Schweiz ist gegenüber Cyber-Risiken resilient. Die Fähigkeit der kritischen Infrastrukturen, wichtige Dienstleistungen und Güter zur Verfügung zu stellen, bleibt auch bei grossen Cyber-Vorfällen gewährleistet.
- Der Schutz der Schweiz vor Cyber-Risiken wird als gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat wahrgenommen, wobei die Verantwortungen und Zuständigkeiten klar definiert und von allen Beteiligten gelebt werden.
- Die Schweiz engagiert sich für die internationale Kooperation zur Erhöhung der Cyber-Sicherheit. Sie fördert den Dialog in der Cyber-Aussen- und Sicherheitspolitik, beteiligt sich aktiv in den internationalen Fachgremien und pflegt den Austausch mit anderen Staaten und internationalen Organisationen.
- Die Schweiz lernt aus Cyber-Vorfällen im In- und Ausland. Cyber-Vorfälle werden sorgfältig analysiert und aufgrund der Erkenntnisse entsprechende Massnahmen getroffen."

Dem NDB werden im Rahmen der nationalen Strategie folgende Zielvorgaben gemacht:[24]

> "Der Nachrichtendienst muss mittels einer systematischen Informationsbeschaffung und -auswertung in der Lage sein, neue Angriffsmuster möglichst frühzeitig zu entdecken. Weiter muss er eine möglichst genaue Feststellung der Urheberschaft von

---

21 Medienmitteilung Bundesrat 19.04.2018.

22 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), S. 2.

23 NCS, S. 8.

24 NCS, S. 24.

erfolgten Angriffen (Attribution) vornehmen können, damit die Handlungsfreiheit der politischen Behörden und der Strafverfolgungsbehörden gewahrt wird.
Bei Angriffen auf kritische Infrastrukturbetreiber muss der Nachrichtendienst unter Einbezug unterstützender Einheiten in der Lage sein, seinen Auftrag im Rahmen des NDG zu erfüllen."

Vom NDB werden folgende spezifischen Massnahmen erwartet:

- Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyberbedrohungslage:

  "Die Fähigkeiten zur Beschaffung, Einschätzung und Verifikation von Informationen zur Bedrohungslage im Nachrichtendienst sind weiter auszubauen. Dazu braucht es eine systematische Nutzung von Open Source Intelligence (OSINT) und den damit verbundenen Fachkenntnissen, die Nutzung technischer Hilfsmittel sowie die Pflege und den Ausbau des Netzwerkes an nationalen und internationalen Partnern. Die gewonnenen Erkenntnisse zur Bedrohungslage sind systematisch aufzuarbeiten, regelmässig zu aktualisieren und über den Lageradar zielgruppengerecht darzustellen. Es soll auch eine Version des Lageradars für die Öffentlichkeit erstellt werden"[25].

- Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution:

  "Das vorhandene Spezialwissen und die Fähigkeiten zur Informationsbeschaffung zwecks Früherkennung von Cyberangriffen und zur Identifikation der Urheberschaft werden weiterentwickelt, die Zusammenarbeit dazu zwischen Bund und Kantonen gestärkt und der Informationsaustausch mit der Wirtschaft ausgebaut. Der Nachrichtendienst des Bundes führt vertiefte Akteurs- und Umfeldanalysen durch, nutzt und entwickelt technische Hilfsmittel, die Fernmeldeüberwachung und Methoden der Human Intelligence. Erfolgte Cyberangriffe werden so systematisch aufgearbeitet und verfolgt"[26].

- Fähigkeit zur Durchführung von aktiven Massnahmen im Cyberraum:

  "Das VBS (NDB und Armee) verfügen über genügend qualitative und quantitative Kompetenzen und Kapazitäten, um gegebenenfalls Angriffe auf kritische Infrastrukturen zu stören, zu verhindern oder zu verlangsamen. Der Einsatz solcher Massnahmen erfolgt gemäss den gesetzlichen Vorgaben von NDG und MG"[27].

2.2 Strategie Cyber des VBS

Im Rahmen der Nationalen Strategie für Cybersicherheit ist das VBS zuständig für die Cyberdefence. Dazu gehört die Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, d.h. der Schutz der für die Sicherheit des Landes kritischen Systeme, die Abwehr von Cyberangriffen, die Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und der Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden. Dazu zählen insbesondere aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen[28].

---

25 NCS, S. 14.
26 NCS, S. 24.
27 NCS, S. 24.
28 NCS, S. 28.

Zur Umsetzung der Nationalen Strategie NCS hat das VBS im März 2021 ein Strategiedokument zu Cyber erarbeitet, in welchem die Organisation und die Vorgehensweise bis 2024 umschrieben werden. Einleitend wird festgehalten, dass der NDB eine deutliche Zunahme von Cyberangriffen auf Schweizer Interessen im In- und Ausland beobachtet. Zu den Zielen gehörten unter anderem die Behörden, die Armee, in der Schweiz angesiedelte internationale Organisationen und ausländische Vertretungen sowie der Finanz- und Technologiesektor. Der NDB zähle Angriffe mit Verschlüsselungstrojanern zu den grössten Bedrohungsformen, welche die kritischen Infrastrukturen der Schweiz und auch Unternehmen betreffen[29].

Das VBS zählt zu seinen Kernaufgaben im Bereich Cyber unter anderem die Erstellung einer umfassenden Bedrohungsbeurteilung und Lagedarstellung der staatlichen und nichtstaatlichen sicherheitspolitisch relevanten Cybervorfälle auf Schweizer Interessen. Dazu gehört die Attribution (Täteridentifikation), die sich aus der Analyse technischer Eigenschaften eines Cybervorfalls und dem geopolitischen Kontext ergibt. Dafür soll die Analyse technischer Eigenschaften von Cybervorfällen, die Beurteilung des internationalen Kontextes und der Nutzung des gesamten nachrichtendienstlichen Spektrums zur Informationsbeschaffung gestärkt werden[30].

Im Bericht zur Strategie Cyber VBS werden dem Nachrichtendienst des Bundes folgende Aufgaben zugewiesen[31]:

> "Der NDB ist ein sicherheitspolitisches Instrument, das gestützt auf das NDG Informationen beschafft und bearbeitet, um Bedrohungen der inneren und äusseren Sicherheit frühzeitig zu erkennen und zu verhindern. Im Mittelpunkt der nachrichtendienstlichen Aufgaben stehen die Sensibilisierung und Antizipation von Cyberangriffen auf Schweizer Interessen (z.B. kritische Infrastrukturen). Der NDB ist für die umfassende Beurteilung der Cyberbedrohungen zuständig. Die Beurteilungen und Lagedarstellungen werden dem Bundesrat, den Departementen und der militärischen Führung mit Beiträgen (z.B. Analysen) und mit einem Lageradar zur Verfügung gestellt. Zu den Kernaufgaben des NDB gehört die Attribution, d.h. die Identifikation eines Cyberangriffs, die Zuordnung des Angriffs zum Urheber. Dazu beschafft der NDB Informationen aus öffentlichen und nichtöffentlichen Quellen, führt vertiefte Akteur- und Umfeldanalysen durch und nutzt technische Instrumente sowie Fernmeldeüberwachung. Der NDB kann unter bestimmten Umständen zusammen mit der FUB (Führungsunterstützungsbasis der Armee) offensive Cyberoperationen durchführen. Der NDB ist in der Kerngruppe Sicherheit sowie der Kerngruppe Cyber vertreten. Das Operations- und Informationszentrum der Melde- und Analysestelle Informationssicherung unterstützt die Betreiber der kritischen Infrastrukturen subsidiär."

Soweit es um die Zusammenarbeit mit Privaten oder mit internationalen Partnern geht, wird im Bericht zur Strategie Cyber VBS ausgeführt, dass der NDB die Betreiber kritischer Infrastrukturen im Rahmen des Public Private Partnership-Ansatzes unterstützt und bei Bedarf sensiblen Unternehmen, Dienstleistern und Betreibern kritischer Infrastrukturen Sensibilisierungsarbeit anbietet. Das Nachrichtendienstgesetz schaffe zudem die gesetzlichen Rahmenbedingungen, um Letztere im Fall von Cyberangriffen zu unterstützen. Sodann sei eine regelmässige Zusammenarbeit mit ausländischen Partnern für

---

29 Cyber VBS (https://www.news.admin.ch/news/message/attacchments/66200.pdf), S. 11.
30 Cyber VBS, S. 31f.
31 Cyber VBS, S. 35.

die Einschätzung von Bedrohungen und Herausforderungen im Cyberbereich sowie im Hinblick auf Aufdeckung und Verhinderung von Cyberangriffen unverzichtbar[32].

2.3 Nationales Zentrum für Cybersicherheit und Einbettung des Ressort Cyber

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[33].

Cyber NDB ist in die Nationale Strategie zum Schutz der Schweiz von Cyberrisiken 2018–2022 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[34] 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[35].

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[36]. 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

---

32 Cyber VBS, S. 21.

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

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

35 NCS, S. 24.

36 Aktennotiz NDB zuhanden der Administrativuntersuchung 20.04.2022.

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, die einem anderen Staat zuordenbar sind. Reine Aktivitäten von Cyberkriminellen zählen nicht zu seinem Aufgabenbereich[37].

2.4 Auswirkungen auf die Arbeit von Cyber NDB

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 (siehe dazu Ziffer 9.5.2, Seite 68), 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 (siehe dazu Ziffer 7.2.1, Seite 42), 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 (siehe dazu Ziffer 8.2, Seite 49) und in einem engen Informationsaustausch mit internationalen Partnerdiensten steht.

---

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

3 Interne Untersuchung des NDB

3.1 Auslöser für die Anordnung der Untersuchung

Nachdem der [redacted] aufgrund gewisser Meldungen [redacted] interveniert hatte, erteilte der damalige Direktor NDB[38] am 29. April 2021 [redacted] den Auftrag, im Ressort Cyber NDB eine interne Untersuchung durchzuführen. Auslöser waren nicht primär Erkenntnisse des Nachrichtendienstes über ein möglicherweise unzulässiges Vorgehen bei der Informationsbeschaffung durch Cyber NDB, sondern im Wesentlichen Vorbehalte, die von [redacted] gegenüber [redacted] vorgebracht worden waren[39].

3.2 Durchführung

Das Ressort Sicherheit NDB führte im Rahmen der internen Untersuchung Befragungen durch und zog diverse Unterlagen bei. Die Untersuchung löste bei den Mitarbeitenden von Cyber NDB eine grosse Verunsicherung aus und führte innerhalb des Nachrichtendienstes selbst zu Kontroversen. Der Leiter der internen Untersuchung äusserte sich im Bericht zu den Rahmenbedingungen des Auftrags und hob hervor, sämtliche seiner Anträge für eine externe Vergabe der Untersuchung und für die Vergrösserung des Untersuchungsteams seien abgelehnt worden. Die Gründe für die Entscheidung des Direktors NDB und die darauffolgende Verkleinerung des Untersuchungsteams hätten einerseits in dringlichen operativen Geschäften [redacted] und andererseits in Unstimmigkeiten über die zu Beginn der Abklärungen gewählte Vorgehensweise gelegen[40].

In den Stellungnahmen zum Berichtsentwurf äusserten sich verschiedene Direktionsbereiche in gelegentlich schroffem Ton sehr kritisch. So bemängelte etwa der Direktionsbereich [redacted], die Unabhängigkeit der Untersuchung sei nicht immer gewährleistet gewesen[41]. Er verlangte zudem, im Bericht müsse ausdrücklich festgehalten werden, dass [redacted] an den Vorkommnissen im Ressort Cyber in keiner Weise beteiligt war; diese lägen ausschliesslich im Verantwortungsbereich von NDBI[42].

Das hauptsächlich betroffene Ressort Cyber NDB seinerseits vertrat in einer vorgängigen Stellungnahme an die interne Verfahrensleitung dezidiert den Standpunkt, dass die Informationsbeschaffung allein Sache des Direktionsbereichs [redacted] sei. Cyber NDB sei aber nicht [redacted], sondern dem Direktionsbereich Informationsmanagement/Cyber (NDBI) unterstellt und allein für die Analyse, nicht aber für die Beschaffung

---

38 Jean-Philippe Gaudin (Fn. 2)

39 Bericht zum Auftrag des Direktors NDB an [redacted] mit dem Zweck, die Rechtmässigkeit der Vorgänge bei Cyber NDB zu überprüfen vom 17. Dezember 2021 (im Folgenden: interner Bericht), S. 10.

40 Interner Bericht (Fn. 39), S. 7.

41 Im gleichen Sinn äusserte sich auch [redacted] in der Administrativuntersuchung (Anhörung [redacted], S. 18f.).

42 Stellungnahme [redacted] zum internen Berichtsentwurf (Dokument 709 der internen Untersuchung).

von Informationen zuständig. Allfällige Kontakte zu Netzbetreibern[43] könnten nur durch Mitarbeitende von [redacted] erfolgen[44].

Der Direktionsbereich NDBI legte in seiner Stellungnahme zum internen Bericht Wert darauf, dass von Anfang an eine Zweiteilung der Verantwortlichkeiten beschlossen worden sei. [redacted] sollte für die Informationsbeschaffung, NDBI für die Analyse verantwortlich sein. An diese Zweiteilung habe sich NDBI immer gehalten. Daran ändere auch die Tatsache nichts, dass einzelne Mitarbeitende von NDBI (Cyber NDB) "angesichts des schleppenden Stellenaufbaus bei [redacted] in Informationsbeschaffungsaktivitäten verwickelt waren". Diese Aktivitäten seien jedoch stets unter der Federführung von [redacted] erfolgt. Der Chef NDBI sei weder bei der Planung oder Beauftragung von Informationsbeschaffungen noch bei der Beschaffung von besonderen, verdeckten Infrastrukturen beigezogen worden[45]. Anlässlich seiner Anhörung im Rahmen der Administrativuntersuchung zeigte sich der Chef NDBI immer noch betroffen von einigen Stellungnahmen zuhanden der internen Untersuchung. Er habe den Eindruck, von Seiten [redacted] sei versucht worden, einen Sündenbock aufzubauen und ihm die gesamte Verantwortung anzulasten[46].

Auch der Chef [redacted] sprach von internen Beeinflussungsversuchen. Er selbst sei von Mitarbeitenden aus seinem Bereich, aber auch aus den Direktionsbereichen [redacted] und NDBI mit Informationen versorgt worden. Diese hätten sich daran gestört, dass im Ressort Cyber NDB auf eine Art und Weise gearbeitet worden sei, die stark nach Illegalität ausgesehen habe, und dass die Kritik daran nicht aufgenommen wurde. Gewissen Leuten innerhalb des Dienstes sei es nicht darum gegangen, den Sachverhalt zu klären, sondern die Quellen von Kritik mundtot zu machen[47]. Der Chef [redacted] hatte denn auch im Rahmen der internen Untersuchung dem Verfahrensleiter Unterlagen übergeben, die er von verschiedenen Mitarbeitenden des Dienstes erhalten hatte.

3.3 Ergebnisse

Gestützt auf die erhobenen Sachverhaltsfragmente entwickelte die Verfahrensleitung hypothetische Fallkonstellationen, formulierte abstrakte Fragestellungen und unterbreitete diese einer extern beigezogenen Anwaltskanzlei zur rechtlichen Beurteilung. Diese nahm gestützt auf die abstrakt geschilderten Vorkommnisse eine rechtliche Auslegeordnung vor und erstattete am 29. November 2021 Bericht[48]. Das Ressort Sicherheit NDB stützte seine rechtliche Einschätzung im Wesentlichen auf den Bericht der beigezogenen Experten und verfasste am 17. Dezember 2021 seinen Schlussbericht zuhanden des Direktors NDB.

---

43 Der grundsätzlich zutreffende Hinweis auf Kontakte zu Netzbetreibern erscheint insofern irreführend, als es bei den Diskussionen um die Beschaffung von Netzwerkverkehrsdaten immer nur um die Kontakte von Cyber NDB zu den Providern und nicht um die von [redacted] über den Dienst ÜPF zu vermittelnden Kontakte zu Netzbetreibern ging.

44 Stellungnahme Cyber NDB vom 02.09.2021 (Dokument 452 der internen Untersuchung).

45 Stellungnahme NDBI zum internen Berichtsentwurf (Dokument 710 der internen Untersuchung).

46 Anhörung [redacted], S. 17.

47 Anhörung [redacted], S. 13f. (siehe auch Ziffer 8.7, Seite 56).

48 Siehe Rechtsgutachten (Fn. 17).

Der Schlussbericht der internen Untersuchung ist in drei Teile aufgebaut. Nach einer Einleitung zur Ausgangslage und zum Auftrag folgt eine chronologische Darstellung mit einer kurzen Umschreibung der jeweiligen Ereignisse. Im zweiten Teil werden der Aufbau von Cyber NDB und Fragen zu den dortigen Abläufen behandelt. Der dritte Teil ist der Prüfung der Rechtmässigkeit bei der Beschaffung, Aufbewahrung und Weitergabe der Informationen gewidmet.

Das Ergebnis der internen Abklärungen wurde in der Medienmitteilung des Bundesrates vom Januar 2022[49] wie folgt zusammengefasst:

> "Im Zeitraum von 2015 bis 2020 wurden gemäss derzeitigen Erkenntnissen im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen auch Informationen beschafft, welche dem Fernmeldegeheimnis unterstehen. Solche Massnahmen sind gemäss dem Nachrichtendienstgesetz bewilligungspflichtig und nur mit Genehmigung des Bundesverwaltungsgerichts zulässig. Eine solche Bewilligung wurde nicht eingeholt. Zudem wurde, ebenfalls ohne gerichtliche Genehmigung, der Netzwerkverkehr von Servern, die von Cyberangreifern benutzt wurden, aufgezeichnet. Betroffen waren ausländische Angreifer, die Cyberangriffe gegen die Schweiz bzw. Schweizer Interessen oder von der Schweiz aus gegen ausländische Einrichtungen verübten.
> Die NDB-Direktion hat die Aktivitäten nach Vorliegen der ersten detaillierten Meldungen über mögliche Unregelmässigkeiten eingestellt und Ende April 2021 vertiefte Abklärungen ausgelöst und es wurden verschiedene Massnahmen eingeleitet."

3.4 Empfehlungen

Im internen Untersuchungsbericht finden sich die nachfolgenden Empfehlungen. In den jeweiligen Bemerkungen finden sich Angaben zu deren Umsetzung:

1. Umgehende Besetzung und allenfalls Ausbau der Stelle des Operationsführenden Cyber.
2. Abstimmung des NDB mit dem Dienst ÜPF im Hinblick auf die Beantragung genehmigungspflichtiger Beschaffungsmassnahmen.
3. Einheitliche Schulung der im Ressort Cyber tätigen Mitarbeitenden des NDB hinsichtlich der rechtlichen Grundlagen bei der Erfüllung ihrer Aufgaben.
4. Durchführung einer externen Untersuchung
   - im Sinne einer Aufgaben-, Leistungs- und Organisationsüberprüfung mit dem Fokus auf Fragen, die noch nicht abschliessend beantwortet werden konnten, wie potenzielle Geldflüsse an [redacted], aber auch die mögliche Weitergabe von Malware Samples an [redacted];
   - zur Abklärung einer allfälligen strafrechtlichen Relevanz entsprechend den Ausführungen im eingeholten Rechtsgutachten;
   - mit einem Schwerpunkt auf das Arbeitsklima im Ressort Cyber NDB.
5. Stärkung der Compliance im NDB, um die Einhaltung der rechtlichen Grundlagen auf periodischer Basis zu prüfen.
6. Stärkung der Governance und des Informationssicherheitsmanagementsystems (ISMS) im NDB durch personelle Aufstockung der Sicherheit NDB.
7. Überprüfung der organisatorischen Ansiedlung des Ressorts Cyber NDB hinsichtlich des ND-Zyklus.

---

49 Medienmitteilung des Bundesrates vom 26.01.2022.

8. Erteilung der im Gesetz und in den Verordnungen vorgesehenen Berechtigungen an den Chef Sicherheit.
9. Weiterentwicklung und Systematisierung der bereits initiierten Rollenklärung und der Vorgehensweise bei der Durchführung interner Untersuchungen.

3.5 Abgrenzung zwischen interner und administrativer Untersuchung

Im Rahmen der NDB-internen Untersuchung wurden die Vorkommnisse im Ressort Cyber weitgehend abgeklärt, soweit dies (noch) möglich war. Nachdem sie im Dezember 2021 Kenntnis vom internen Bericht erhalten hatte, ging auch die GPDel davon aus, dass mit dem Schlussbericht der internen Untersuchung und dem vom NDB eingeholten Rechtsgutachten der Sachverhalt und die Rechtslage weitgehend geklärt seien. Offen bleibe einerseits, welche Vorkehrungen aus Sicht des VBS im Hinblick auf die Zukunft von Cyber NDB getroffen werden müssen. Andererseits sei die Frage nach der allfälligen strafrechtlichen Relevanz des in der internen Untersuchung festgestellten Sachverhalts zu klären[50].

Die hier vorliegende Administrativuntersuchung baut auf dem Bericht der internen Untersuchung auf, versucht aber auch, die Akzente anders zu setzen. Gewisse Themen, die in der internen Untersuchung noch Gegenstand intensiver Abklärungen waren, sind heute in den Hintergrund getreten und wurden deshalb nicht mehr weiterverfolgt. Dazu zählen insbesondere die Fragen nach den internen Kommunikationsmitteln und der internen Datenablage von Cyber NDB sowie nach den Datenverarbeitungssystemen des NDB. Diese Aspekte sollen im Rahmen der laufenden Revision des Nachrichtendienstgesetzes ohnehin einer Neukonzeption unterzogen werden[51]. Weniger relevant dürften heute auch die genauen Modalitäten der Beendigung des Dienstverhältnisses mit dem ehemaligen Chef Cyber NDB (Rückgabe der Arbeitsmittel und Löschung von Daten) sein. Die gegenüber [redacted] vorgebrachten Vorbehalte konnten bereits in der internen Untersuchung nicht bestätigt, aber auch nicht restlos widerlegt werden. Sie dürften nach seinem Ausscheiden aus dem Dienst aber kaum mehr einen Einfluss auf die Tätigkeit des NDB haben.

Die Administrativuntersuchung legt das Schwergewicht auf eine Analyse der konkreten Arbeitsmethoden von Cyber NDB. Ausgehend davon sollen einerseits Fragen nach den Verantwortlichkeiten für die Vorkommnisse im Ressort Cyber NDB geklärt und andererseits Rückschlüsse auf allenfalls zu ändernde Strukturen und Prozesse innerhalb des NDB gezogen werden. Ein separates Kapitel wird der Frage nach der allfälligen strafrechtlichen Relevanz der Datenbeschaffung durch Cyber NDB gewidmet sein.

---

50 Medienmitteilung der GPDel vom 27.01.2022.

51 Erläuternder Bericht des Bundesrates zur Revision des Nachrichtendienstgesetzes vom Mai 2022, S. 15ff. (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-88899.html).

4 Prüfbericht der Aufsichtsbehörde über den Nachrichtendienst

Die unabhängige Aufsichtsbehörde über den Nachrichtendienst (AB-ND) hat im August 2021 einen speziellen Prüfbericht zum Schutz kritischer Infrastrukturen/Cyberabwehr verfasst[52]. Die AB-ND übt die unmittelbare Aufsicht über den Nachrichtendienst aus, hat Zugang zu allen sachdienlichen Informationen und Unterlagen und Zugriff auf sämtliche Informationssysteme des NDB. Sie teilt dem VBS das Resultat ihrer Überprüfungen schriftlich mit und kann Empfehlungen aussprechen[53]. Ihr Bericht ist insofern von besonderem Interesse, als es Aufgabe der AB-ND ist, die nachrichtendienstliche Tätigkeit des NDB auf ihre Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit zu überprüfen.

Aus dem Prüfbericht geht hervor, dass die AB-ND Kenntnis von den [redacted]

52 Prüfbericht der Aufsichtsbehörde über den Nachrichtendienst (AB-ND) in Sachen Schutz kritischer Infrastrukturen/Cyber-Abwehr vom 25. August 2021 (Dokument 447 der internen Untersuchung).

53 Art. 78 NDG.

[redacted]

[redacted][55].

54 Die letzte Aussage bezieht sich offenbar auf den vom [redacted] eingenommenen Rechtsstandpunkt.

55 Prüfbericht AB-ND 25.08.2021 (Fn. 52), S. 12.

5 Das Ressort Cyber im Gesamtgefüge des NDB

5.1 Aufgaben und hierarchische Unterstellung

Zu den Aufgaben des Ressorts Cyber NDB gehört, Cyberangriffe staatlichen Ursprungs, die gegen Schweizer Interessen gerichtet sind, mit operativen und analytischen Massnahmen zu identifizieren und zu bekämpfen sowie den Ursprung der Angriffe und die Interessen der Angreifer zu erkennen. Um dieses Ziel zu erreichen, beschafft Cyber NDB Informationen aus öffentlich zugänglichen und kommerziellen Quellen sowie aus Hinweisen von Behörden, Partnerdiensten und Privaten[56]. Im Fokus der NDB-internen Untersuchung und der vorliegenden Administrativuntersuchung steht vor allem die Beschaffung von Informationen von Internet-Service-Providern, die ihren Kunden Leistungen und Hardware (Router) anbieten, um diesen den Zugang zum Internet zu ermöglichen.

Das Ressort Cyber NDB wurde im Zuge der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken NCS 2012-2017 auf Anfang 2014 neu geschaffen. Als Chef des Ressorts wurde [redacted] ernannt, [redacted] brachte eine reiche Erfahrung und ein breites Netzwerk an Kontakten zu staatlichen und privaten Akteuren der Cybersicherheit ein[57]. Der Erwartungsdruck an die neu geschaffene Einheit des NDB war hoch. Dementsprechend schnell erfolgte der Aufbau der Strukturen von Cyber NDB.

Das Ressort Cyber NDB wurde dem Direktionsbereich Informationsmanagement/Cyber NDBI zugeordnet. Ausschlaggebend dafür war nach den Aussagen des Chefs NDBI die Tatsache, dass die Funktionen von Cyber NDB weder zur Beschaffung noch zur Auswertung oder zur Steuerung passten. Primär sei es um die fachliche Unterstützung der klassischen Bereiche der nachrichtendienstlichen Tätigkeiten gegangen[58]. Bald habe sich jedoch gezeigt, dass Cyber NDB über einen Steuerungs-, Beschaffungs- und Auswerteteil verfügt, wobei das Hauptgewicht auf der Analyse liege. In der Folge habe sich der NDB für eine Zusammenführung und Zentralisierung der Cyber-Spezialisten entschieden. [redacted] Werde Cyber NDB heute nicht mehr als Spezialistenteam, sondern als thematischer Bereich betrachtet, sei das Ressort – wie als Folge der internen Untersuchung angeordnet – [redacted] am richtigen Ort[59].

5.2 Einbindung in die allgemeinen Strukturen des NDB

Bei der Einführung von Cyber NDB wurden keine neuen Reglemente oder Weisungen erlassen, welche auf die Organisation sowie die spezifischen Informations- und Datenverarbeitungsbedürfnisse eines weitgehend technisch (und nicht thematisch) ausgerichteten Ressorts Bezug nahmen. Der einzige, offiziell dokumentierte und von der Geschäftsleitung NDB genehmigte Prozess, der sich spezifisch auf Cyber NDB bezieht, ist

---

56 Interner Bericht (Fn. 39), S. 24.

57 Anhörung [redacted], S. 8.

58 Vgl. auch Anhörung [redacted], S. 2.

59 Anhörung [redacted], S. 3f.

mit [redacted] betitelt und datiert vom 22. Juli 2015. Er zeigt in einem rollenorientierten Ablaufdiagramm die Vorgehensweise bei Cyber-Abklärungen auf[60].

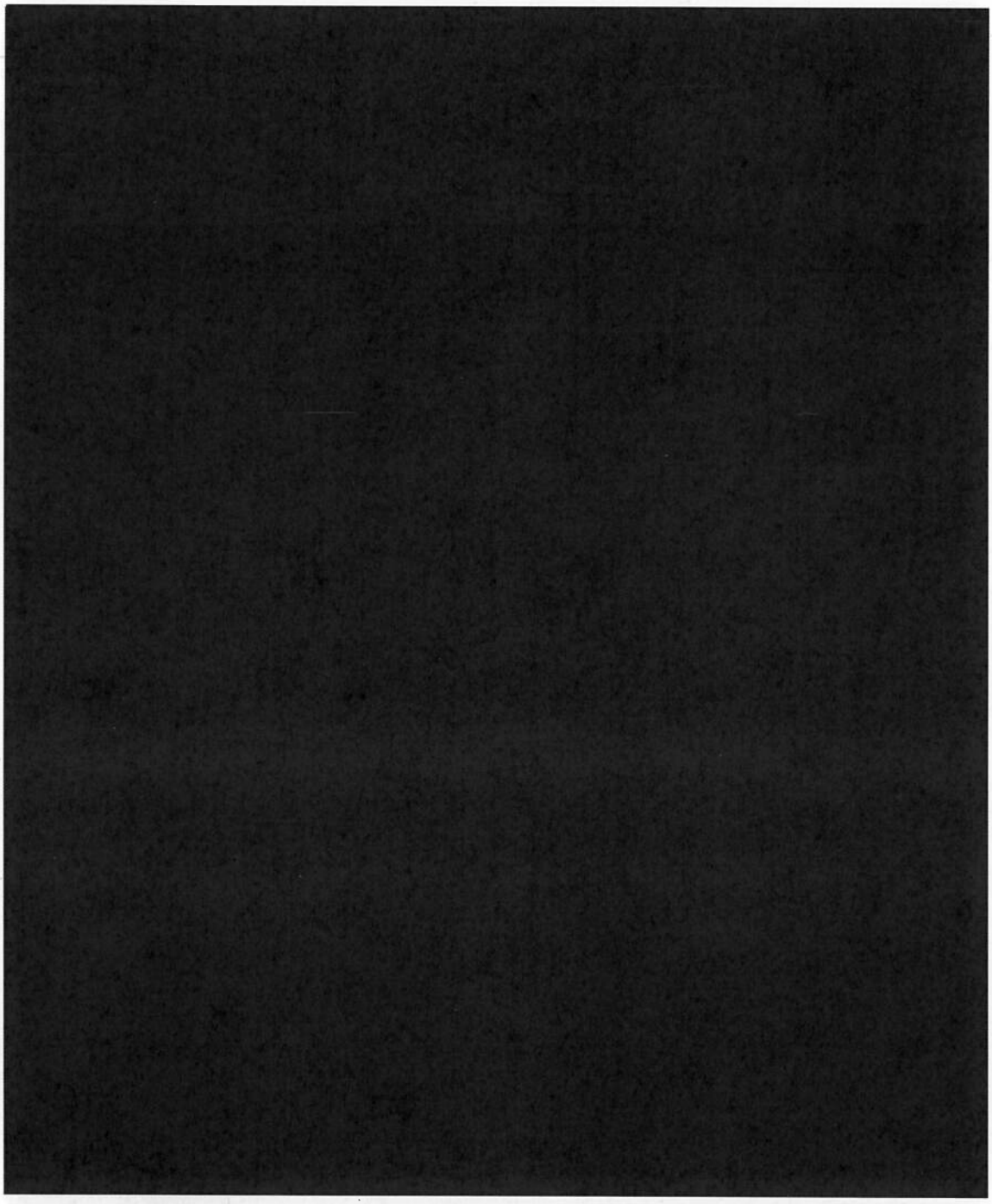
In der internen Untersuchung konnte allerdings kein Hinweis gefunden werden, dass der genannte Prozess zur Informationsbeschaffung im Rahmen einer Operation des NDB je zur Anwendung gelangte[61]. Im Übrigen liegen – bis zu den im Gefolge der Vorkommnisse erlassenen neuen Anordnungen – keine durch den Direktor NDB oder die Geschäftsleitung NDB genehmigten Prozesse oder schriftliche Weisungen zum Themenbereich Cyber vor[62]. Ebenso wenig hatte der ehemalige Chef Cyber NDB die für die Arbeitsweise des Ressorts relevanten Prozesse schriftlich festgehalten.

Zu Beginn war bloss vorgesehen, dass die Spezialisten von Cyber NDB primär für die technische Analyse von Daten zuständig sein sollen. An der üblichen Arbeitsteilung im Dienst – [redacted] – sollte grundsätzlich nichts geändert werden.

5.3 Informationsbeschaffung

[redacted]

60 Interner Bericht (Fn. 39), S. 31.
61 Interner Bericht (Fn. 39), S. 28.
62 Interner Bericht (Fn. 39), S. 25.
63 Art. 12 NDV.
64 Anhörung [redacted] S. 3; Anhörung [redacted], S. 3).
65 NDB, [redacted].



66 Anhörung [redacted] S. 3 f.
67 Interner Bericht (Fn. 39), S. 23.
68 Anhörung [redacted], S. 4 und 6.
69 [redacted] und [redacted] üben die Funktion [redacted].
70 Anhörung [redacted], S. 11.
71 Anhörung [redacted] S. 5.
72 Anhörung [redacted] i, S. 3.
73 Anhörung [redacted], S. 3 f; vgl. auch Anhörung [redacted], S. 4.
74 Stellungnahme [redacted] zum internen Berichtsentwurf (Dokument 709 der internen Untersuchung).

[redacted]

5.4 Datenablage und Kommunikationsmittel

Spezifische, auf die besonderen Bedürfnisse von Cyber NDB ausgerichtete Weisungen oder Reglemente wurden nicht erlassen. Das interne Untersuchungsteam fand auch keine Detailbeschreibungen über Kommunikationsvorgänge und technische Mittel für die Informationsbeschaffung zum Themengebiet Cyber[77].

Das Ressort Cyber NDB erschloss sich nicht nur neue Informationsquellen, sondern ging auch im Bereich der Kommunikationsmittel, der Dokumentation und der Datenverarbeitung eigene Wege. Aufträge zur Beschaffung und Bearbeitung von Informationen wurden nicht systematisch dokumentiert. Ebenso wenig findet sich eine systematische Dokumentation der [redacted][78]. Mangels entsprechender Dokumentationen können deshalb diesbezüglich auch im Rahmen der Administrativuntersuchung keine weiteren Angaben gemacht werden.

---

75 Anhörung [redacted] S. 3 ff.
76 Art. 14 Abs. 2 BWIS (heute Art. 23 NDG).
77 Interner Bericht (Fn. 39), S. 25.
78 Interner Bericht (Fn. 39), S. 34.

Das Ressort Cyber NDB benutzte zwar grundsätzlich die vom NDB zur Verfügung gestellte Informations- und Kommunikationstechnologien (IKT). Darüber hinaus betrieb es aber auch eine eigene IKT-Infrastruktur, welche eigene Server, Netzwerkspeicher, Netzwerkgeräte, Endgeräte sowie netzunabhängige Computer und Massenspeicher umfasste. Die eigene IKT-Infrastruktur wurde, soweit damit Auslagen verbunden waren, von Cyber NDB über die offiziellen Prozesse des NDB beschafft[79]. Die dazu befragten Mitarbeitenden von Cyber NDB betonten in der Administrativuntersuchung, dass ihr Vorgehen immer mit der Linie abgesprochen gewesen sei. Soweit sie eine eigene IKT-Struktur aufgebaut hatten, sei dies auf dem ordentlichen Beschaffungsweg erfolgt. Ihr ehemaliger Chef sei darüber informiert gewesen, und dieser habe seinerseits auch den vorgesetzten Direktionsbereich NDBI miteinbezogen[80].

Die Bearbeitung von Daten erfolgte weitgehend über separate Arbeitsplatzsysteme, die im Nachrichtendienstgesetz oder in der entsprechenden Ausführungsgesetzgebung nicht vorgesehen sind[81]. Eine Bearbeitung von Daten ausserhalb der Informationssysteme des NDB wäre zwar grundsätzlich zulässig, soweit dies aus Gründen des Quellenschutzes für besonders sensitive Daten erforderlich ist[82]. Derartige Gründe lagen jedoch in Bezug auf die von Cyber NDB analysierten Randdaten des Netzwerkverkehrs offensichtlich nicht vor. Erst im Dezember 2018 genehmigten der Chef NDBI und der ehemalige Chef Cyber NDB ein Informations- und Datenschutzkonzept über die Anwendungs- und Technologiearchitektur des NDB (ISDS-Konzept). Darin sind die von Cyber NDB verwendeten Datenverarbeitungssysteme zumindest teilweise aufgeführt[83].

Auch Daten des technischen Labors von Cyber NDB (technische Analyse), welche insbesondere Aufzeichnungen von Systemabbildern oder Netzwerkdaten betreffen, werden auf einem gesonderten Informationsverarbeitungssystem des NDB gespeichert und ausgewertet. Auch diesbezüglich wurde erst im Juli 2020 ein Bearbeitungsreglement erlassen[84].

Die Daten des aufgezeichneten Netzwerkverkehrs oder der Systemabbilder wurden nach der Auswertung und dem Abschluss eines Ereignisses regelmässig gelöscht, um Platz für neue Aufzeichnungen zu schaffen[85]. Eine Protokollierung der Löschvorgänge erfolgte nicht[86].

Die Mitarbeitenden von Cyber NDB betonten, dass keines der Datenverarbeitungssysteme des NDB für ihre Arbeit geeignet sei. Auch die aktuelle Verordnung – wie schon die vorausgegangenen Reglemente – seien nicht auf die von ihnen bearbeiteten Daten und die spezifischen Methoden der Arbeitsweise des Ressorts ausgerichtet. Dies sei ein wesentlicher Grund für die Notwendigkeit gewesen, eine eigene IKT-Infrastruktur zu entwickeln. Eine der Aufgaben von Cyber NDB bestehe u.a. darin, Malware zu analysieren, d.h. [redacted]

79 Interner Bericht (Fn. 39), S. 29.

80 Anhörung [redacted], S. 16 f.

81 Art. 47 ff. NDG und insbesondere Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS NDB); siehe dazu auch interner Bericht, S. 26 ff.

82 Art. 7 Abs. 1 VIS-NDB.

83 Interner Bericht (Fn. 39), S. 28.

84 Interner Bericht (Fn. 39), S. 28.

85 Interner Bericht (Fn. 39), S. 35.

86 Anhörung [redacted], S. 17.

[redacted] Hinzu komme, dass die von Cyber NDB bearbeiteten Daten praktisch ausschliesslich technischer Natur seien und ein allfälliger Personenbezug nicht bestehe: Cyber NDB habe keinen Bedarf, nach Personendaten zu suchen; von Interesse seien technische Indikatoren und Vorgehensweisen, welche vollständig personenunabhängig seien[87].

[redacted]

87 Anhörung [redacted], S. 16 f.
88 Interner Bericht (Fn. 39), S. 29.
89 Anhörung [redacted], S. 7.
90 Anhörung [redacted], S. 6;
91 Anhörung [redacted] S. 6.

6 Konkrete Arbeitsweise von Cyber NDB

[redacted]

6.1 Hinweise auf Cyberangriffe

Cyberangriffe sind im Vornhinein praktisch nicht auszumachen, da es für sie keine Anzeichen oder gar Warnungen gibt. Vielfach ist gar nicht erkennbar, dass ein derartiger Angriff geführt wurde bzw. geführt wird[92]. [redacted]

[redacted]

[redacted]

---

92 Peter Harbich, Die wachsende Bedeutung privater Akteure im Bereich der Intelligence, Arbeitspapiere zur Internationalen Politik und Aussenpolitik 3/2006, S. 57.

93 Der Club de Berne ist ein informeller Zusammenschluss der Leiter der Sicherheits- und Nachrichtendienste der EU-Mitgliedsstatten sowie Norwegens und der Schweiz. Die Mitglieder kommen in regelmässigen Abständen zusammen, um nachrichtendienstliche und sicherheitsrelevante Themen zu erörtern (vgl. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-24089-html).

94 Anhörung [redacted], S. 25 f.

[redacted]

Die Anbieterinnen von Fernmeldedienstleistungen sind verpflichtet, u.a. die Identität des Teilnehmers oder der Teilnehmerin und die Adressierungselemente zu erfassen und auf Verlangen dem Dienst ÜPF darüber Auskunft zu erteilen[95]. Der NDB seinerseits ist berechtigt, diese Elemente im Rahmen einer nicht genehmigungspflichtigen Anfrage beim Dienst ÜPF in Erfahrung zu bringen.[96]. Er wird damit in die Lage versetzt, einerseits den Internet Service Provider (ISP)[97] zu bestimmen, über dessen Server der mit einer bestimmten IP-Adresse verknüpfte Datenverkehr ausgetauscht wird, und andererseits den beim Provider registrierten Benutzer dieser IP-Adresse zu identifizieren.

6.2 Beizug von Netzwerkaufzeichnungen und Serverabbildern

Um einen Cyberangriff analysieren zu können, bedarf es in der Regel entsprechender Feststellungen des Opfers (z.B. Veränderungen in den Datenstrukturen, Veröffentlichung geleakter Daten etc.) oder einer Überwachung des über den Server abgewickelten Datenverkehrs. Als Ausgangspunkt dient die IP-Adresse in ihrer Eigenschaft als eindeutiger Identifizierungsfaktor für den betreffenden Server. Die Überwachung kann [redacted]

Im Verlauf der Jahre hatte Cyber NDB, insbesondere [redacted], Kontakte zu privaten Unternehmen aufgebaut, die im Bereich der Cybersicherheit tätig sind oder

---

95 Art. 21 BÜPF.

96 Art. 25 NDG i.V.m. Art. 15 BÜPF.

97 Anbieter von Dienstleistungen, der Dienste, Inhalte oder technische Leistungen an Endnutzer zur Verfügung stellt, um diesen die Kommunikation über das Internet zu ermöglichen. Zu den angebotenen Dienstleistungen zählt insbesondere auch die Vermietung von Servern, die ihre Ressourcen in einem Netz für andere Nutzer zur Verfügung stellen.

98 [redacted]; in der [redacted] erstellten Aktennotiz (siehe dazu Ziffer 8.4, Seite 51) ist von [redacted] Providern die Rede.

als Provider ihren Kunden an einem Standort in der Schweiz Server zur Verfügung stellen. Gemäss Abklärungen der internen Untersuchung verfügte Cyber NDB bei insgesamt [redacted] Unternehmen über Ansprechpersonen, zu denen es regelmässige Kontakte unterhielt[99]. [redacted][100].

[redacted]

Die [redacted] Daten über den Netzwerkverkehr flossen in das gesonderte Netzwerk des Labors von Cyber NDB (CyberLab), welches technische Daten aus unterschiedlichen Quellen enthält und das der nachfolgenden Analyse dient[105]. Ein Bearbeitungsreglement für die Netzwerkdaten des Labors wurde erst im Juli 2020 geschaffen; dieses sieht ein separates Speicher- und Auswertungssystem vor[106].

Für die rechtliche Einordnung kann auf Ziffer 7.2 (Seite 42) verwiesen werden.

---

99 Interner Bericht (Fn. 39), S. 32.
100 Anhörung [redacted], S. 11.
101 Interner Bericht (Fn. 39), S. 30.
102 Interner Bericht (Fn. 39), S. 17, 49.
103 Interner Bericht (Fn. 39), S. 14 f.
104 Anhörung [redacted], S. 7; vgl. auch interner Bericht (Fn. 39), S. 46.
105 Interner Bericht (Fn. 39), S. 39.
106 Bearbeitungsreglement für die Netzwerkdaten Cyber vom 6. Juli 2020; vgl. auch interner Bericht (Fn. 39), S. 39

6.3 Art der zur Analyse benutzten Daten

Bei der Analyse des aufgezeichneten Netzwerkverkehrs stehen für Cyber NDB die Verkehrsdaten (Randdaten) im Vordergrund. Randdaten sind nach Art. 8 Abs. 1 lit. b des BG betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) diejenigen Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung. Diese Randdaten dokumentieren allein den äusseren Ablauf des über den überwachten Server laufenden Informationsaustauschs. Sie geben Auskunft über die IP-Adressen der Kommunikationspartner sowie über den Zeitpunkt, die Dauer und die technischen Merkmale der Verbindung. Aus diesen Daten kann (soweit die IP-Adresse nicht bereits einer bestimmten Person zugeordnet werden konnte) nicht zwingend auch auf die Identität der Kommunikationsteilnehmer geschlossen werden.

Auch der Inhalt des [redacted] Datenverkehrs wäre grundsätzlich lesbar, [redacted][107]. Inhaltliche Aspekte könnten allenfalls für die Opfer eines Angriffs von Bedeutung sein, indem sich daraus Rückschlüsse auf die vom Angreifer verfolgten Ziele ziehen lassen. Wie die Mitarbeitenden von Cyber NDB betonen, gehe es aber bei der technischen Analyse im Wesentlichen um die Auswertung der Kommunikation zwischen zwei Geräten[108].

Die technische Analyse arbeitet nicht personen-, sondern gerätebezogen. Die ausgewerteten Randdaten des Datenverkehrs können auch nicht einer bestimmten Person zugeordnet werden, da [redacted][109].

[redacted][110].

---

107 Anhörung [redacted], S. 8;
108 Anhörung [redacted], S. 13.
109 Anhörung [redacted], S. 12 ff;
110 Anhörung [redacted], S. 12f.

[redacted][113].

[redacted][114].

111 In einem Protokoll festgehaltene Daten aller oder bestimmter Aktionen von Prozessen auf einem Computer.
112 Anhörung [redacted], S. 9.
113 Anhörung [redacted], S. 5.
114 Anhörung [redacted], S. 14.

7 Grundsätzliche Problemfelder

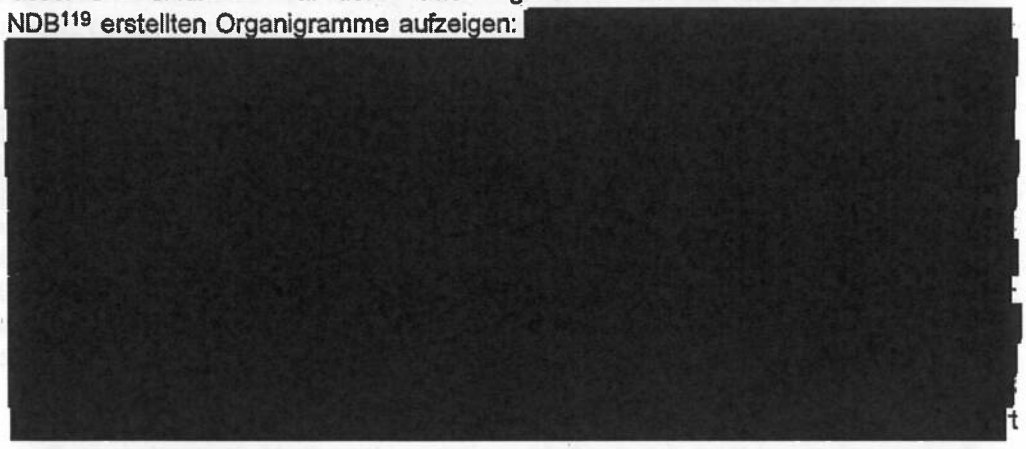
7.1 Faktische Stellung und Rolle des Ressorts Cyber im NDB

7.1.1 Ungenügende Einbindung in die bestehenden Strukturen des NDB

Das Ressort Cyber NDB wurde 2014 unter hohem Zeit- und Erwartungsdruck neu aufgebaut (siehe dazu Ziffer 5.1, Seite 25). Vertiefte Abklärungen über die richtige Einordnung, die Unterstellung und die Arbeitsweise der neu geschaffenen Einheit erfolgten nicht. Insbesondere wurde nicht darüber diskutiert, ob Cyber NDB die ihm zugedachten Aufgaben auf der Grundlage des geltenden Rechts und in Berücksichtigung des allgemeinen nachrichtendienstlichen Instrumentariums überhaupt erfüllen kann[115], die im Dienst üblichen Strukturen, Prozesse und Standards angesichts der klaren Unterschiede einfach übernommen werden können[116] oder diesbezüglich gewisse Änderungen erforderlich sind.

Direktion und Geschäftsleitung beschränkten sich weitgehend darauf, Cyber NDB in die bestehenden Strukturen einzugliedern. Nachdem mit dem Direktionsbereich Informationsmanagement (NDBI) bereits eine Dienststelle bestand, die sich u.a. mit Informatikfragen befasste, schien es naheliegend zu sein, Cyber NDB diesem Direktionsbereich zuzuordnen[117]. Im Übrigen wurde Cyber NDB als ein weiteres Themengebiet des Nachrichtendienstes betrachtet, das sich problemlos in die allgemeinen Strukturen und Prozessabläufe des NDB eingliedern lässt. Der Erlass spezifischer Weisungen oder Reglemente schien nicht erforderlich, da Cyber NDB nicht anders arbeiten sollte als die anderen, nach Themen aufgeschlüsselten Ressorts des NDB[118] (siehe dazu Ziffer 5.2, Seite 25).

Die Schwierigkeiten, die mit der ursprünglich geplanten Einbindung von Cyber NDB in die bestehenden Strukturen und Prozesse des Nachrichtendienstes verbunden waren, lassen sich eindrücklich an der Entwicklung der von den beiden früheren Direktoren NDB[119] erstellten Organigramme aufzeigen: [120]



115 Vgl. Anhörung [redacted], S. 9.
116 Vgl. Anhörung [redacted], S. 4.
117 Dieser Entscheid wurde in der Zwischenzeit korrigiert; seit Januar 2022 ist Cyber NDB einstweilen dem Direktionsbereich [redacted] unterstellt.
118 Anhörung Jürg Bühler, S. 2.
119 Markus Seiler (im Amt von 01.01.2010 bis 30.11.2017); Jean-Philippe Gaudin (Fn. 2).
120 Organigramme NDB 01.11.2013, 01.02. 2015, 01.04.2017, 01.12.2018, 01.09.2020.

[redacted]

Auch wenn Organigramme nicht immer die tatsächlich gelebte Realität widerspiegeln mögen, zeigen die im Lauf der Jahre eingeführten Neuerungen doch deutlich auf, dass mit der Einbindung von Cyber NDB in die klassischen Strukturen des Nachrichtendienstes – [redacted] – doch nicht alles so klar war, wie es heute gelegentlich dargestellt wird.

7.1.2 Ungenügende Führung und Aufsicht

Mit dem neu ernannten (ehemaligen) Chef Cyber NDB stand eine fachkundige, innovative und bestens vernetzte Person zur Verfügung, die mit grossem Engagement schon bald die ersten Erfolge vorweisen konnte. Der fehlende Einbezug der für [redacted] zuständigen Direktionsbereiche wie auch die Arbeitsmethoden von Cyber NDB waren auf der Führungsebene des NDB – wenn auch nicht in den Details, so doch in den allgemeinen Grundzügen – weitgehend bekannt. Vorgesetzte und Geschäftsleitung liessen es im Wesentlichen dabei bewenden, sich vom ehemaligen Chef Cyber NDB vergewissern zu lassen, dass alles in Ordnung sei. Zielführende Nachfragen, vertiefte Kontrollen oder gar eigentliche Überprüfungen fanden kaum statt, ansonsten es wohl kaum möglich gewesen wäre, dass Cyber NDB während Jahren ohne Eröffnung von Operationen und auf freiwilliger Basis Daten aus Netzwerkaufzeichnungen von Providern beziehen und auswerten konnte.

Insofern fällt es schwer, die Verantwortung für die Vorkommnisse im Ressort Cyber NDB einer bestimmten Person zuzuordnen. Einerseits erscheint es verständlich, dass der ehemalige Chef die ihm gewährte Freiheit nutzte und das Ressort nach seinen eigenen Vorstellungen aufbaute, zumal ihm die erzielten Erfolge recht zu geben schienen. Andererseits fehlte es aber auch von Seiten der Führungsebene an einem klaren Konzept für das neu geschaffene Ressort. Bestrebungen zu einer Neuausrichtung waren zwar vorhanden, verliefen aber im Sande[122].

Eine Intervention von Seiten der Geschäftsleitung NDB erfolgte erst, nachdem [redacted] gegenüber dem ehemaligen Direktor NDB Vorbehalte geäussert hatten, einen Datenabfluss befürchteten und [redacted]. Erst dieser Umstand – verbunden mit den ohnehin schon seit geraumer Zeit bekannten Spannungen innerhalb des Ressorts Cyber NDB und den Meinungsverschiedenheiten mit dem Direktionsbereich [redacted] – veranlassten die Führungsebene im September 2020, den ehemaligen Chef Cyber NDB zu einer Aussprache zu zitieren, um Klarheit über das Ausmass der Zusammenarbeit mit Internet-Service-Providern und insbesondere über die von diesen bezogenen Daten zu erhalten.

Zusammenfassend lässt sich der Schluss ziehen, dass die Vorkommnisse im Ressort Cyber NDB letztlich auf eine Kombination von eigenmächtigem Vorgehen und fehlender

---

121 Interner Bericht (Fn. 39), S. 14.

122 So berichtete etwa der Chef [redacted], dass er mehrmals versucht habe, Vorschläge zu einer Neustrukturierung des Dienstes und der Prozesse in die Wege zu leiten und dabei insbesondere den "Gemischtwarenladen" NDBI zu entschlacken. Seine Vorschläge seien zwar auf Gehör gestossen, letztlich aber nie umgesetzt worden (Anhörung [redacted] S. 8.).

oder ungenügender Führung und Beaufsichtigung zurückzuführen sind. Auf der einen Seite stand ein Chef dem Ressort Cyber NDB vor, der von seinen Vorstellungen und Fähigkeiten sowie von seiner Aufgabe überzeugt, ausgesprochen initiativ und erst noch erfolgreich war, für rechtliche Vorgaben und institutionalisierte Prozessabläufe innerhalb eines staatlichen Dienstes aber wenig Verständnis zeigte. Auf der anderen Seite war er einem Direktionsbereich zugeordnet, der zwar viel mit der [redacted] von Daten, aber nichts mit [redacted] zu tun hatte, und dessen Chef ihn weitgehend gewähren liess. Die Geschäftsleitung schliesslich gab sich mit den spärlichen Auskünften zufrieden, verzichtete weitgehend auf jede Kontrolle und Überprüfung und schritt erst ein, als sich die Probleme im Ressort Cyber NDB nicht mehr länger verbergen liessen.

7.1.3 Massnahmen des NDB nach der internen Untersuchung

Der Prozess der Neustrukturierung des Ressorts Cyber NDB ist im Gange. Direktion und Geschäftsleitung haben bereits während der internen Untersuchung und insbesondere nach deren Abschluss verschiedene Massnahmen in die Wege geleitet.

Erlass einer Weisung

Noch während der laufenden internen Untersuchung stellte die Direktion NDB mit dem Erlass der Weisung "betreffend die nachrichtendienstlichen Tätigkeiten im Themengebiet Cyber im NDB" vom Oktober 2021[123] klar, dass sich auch das Ressort Cyber NDB an den für den gesamten Nachrichtendienst geltenden allgemeinen Grundsätzen und Prozessabläufen zu orientieren hat. Eine erste Revision der Weisung war geplant, wurde aber bis zum Abschluss der Administrativuntersuchung einstweilen zurückgestellt. Die Weisung sieht insbesondere vor, dass sämtliche Kontakte im Themengebiet Cyber über die definierten Prozesse und die offiziellen Kommunikationsmittel und -prozesse des NDB abzuwickeln und zu dokumentieren sind: [redacted]

[redacted][127]. Der NDB kann freiwillige

123 Weisungen des stellvertretenden Direktors NDB betreffend die nachrichtendienstlichen Tätigkeiten im Themengebiet Cyber im NDB 01.10.2021.

124 Art. 15 BÜPF

125 Art. 26 ff. NDG.

126 Art. 39 ff. NDG.

127 i.S.v. Art. 12 NDV.

Meldungen von Fernmeldedienstanbieterinnen entgegennehmen[128] und bearbeiten. [redacted] lässt solche Meldungen beim Rechtsdienst NDB daraufhin überprüfen, ob Überwachungsvorgänge betroffen sind oder die Informationen dem Fernmeldegeheimnis unterstehen, und sorgt für die ordentliche Dokumentation des Vorgangs beim NDB. Die Weisung sieht weiter vor, dass alle mit Cyberarbeiten befassten Organisationseinheiten des NDB Kontakte wahrnehmen können, soweit diese nicht der nachrichtendienstlichen operativen Beschaffung dienen. Finanzrelevante Beziehungen regeln sie über Bedarfsanmeldungen in der elektronischen Geschäftsverwaltung (GEVER) und mit dem Abschluss entsprechender Verträge. [redacted].

Freistellung des Chefs Cyber NDB und Anforderungen an die Führungsperson

Bereits vor der Eröffnung der NDB-internen Untersuchung war der ehemalige Chef Cyber NDB [redacted]. Das Arbeitsverhältnis wurde auf [redacted] aufgelöst (siehe dazu Ziffer 8.7, Seite 56).

Ein erster Versuch, die Leitung von Cyber NDB, wenn einstweilen auch nur vorübergehend, neu zu besetzen, ist bereits nach kurzer Zeit gescheitert (siehe dazu Ziffer 8.8, Seite 58). Umso wichtiger erscheint es deshalb, dass Direktion und Geschäftsleitung NDB der Auswahl des neuen Chefs oder der neuen Chefin hohe Priorität einräumen. Aufgrund der gemachten Erfahrungen und der heutigen Situation im Ressort Cyber NDB wird es eine prioritäre Aufgabe der neuen Führungsperson sein, die Mitarbeitenden zu führen, auf eine gemeinsame Linie zu bringen und für ihre Tätigkeit im Interesse des gesamten Nachrichtendienstes zu motivieren. Neben den unerlässlichen technischen Kennnissen, wird vor allem auch die Fähigkeit gefragt sein, sich in die übergeordneten Interessen des Dienstes einzuordnen, rechtliche Rahmenbedingungen zu akzeptieren und den Sinn strukturierter Prozessabläufe zu erkennen[129].

Neuunterstellung des Ressorts Cyber

Im Sinne einer Sofortmassnahme wurde im Januar 2022 die organisatorische Zuordnung von Cyber NDB zum Direktionsbereich Informationsmanagement/Cyber NDBI aufgehoben und das Ressort neu der Auswertung [redacted] unterstellt. Die [redacted] ist damit unbelastet von den früheren Vorkommnissen. Sie hat nach Vorliegen des internen Untersuchungsberichts umgehend versucht, sich ein eigenständiges Bild von der Vorgeschichte, den Hintergründen und den Abläufen zu verschaffen. Zu diesem Zweck führte sie zahlreiche Gespräche mit Mitarbeitenden aus dem Umfeld des Ressorts Cyber NDB, aber auch der [redacted] Wie sie anlässlich der Anhörung ausführte, legt sie besonderes Gewicht auf die Absprache und die Koordination der verschiedenen Aufgabenbereiche innerhalb des NDB. [redacted]

128 Art. 23 NDG.

129 Siehe dazu auch Anhörung [redacted], S. 4f.

[redacted] betonte aber auch, dass die Arbeiten zu einer Neustrukturierung des Ressorts Cyber NDB sich einstweilen noch im Stadium einer Analyse des IST-Zustandes befinden[131].

Wie [redacted] weiter ausführte, sollen die Vorschläge für eine Neuausrichtung des Ressorts Cyber NDB nach den Vorstellungen des neuen Direktors NDB[132] von der Basis eingebracht werden. Ein eigens dafür vorgesehenes und aus den unterschiedlichen Bereichen stammendes Kernteam soll diese Vorstellungen sammeln und aufarbeiten, die rechtlichen Grundlagen überprüfen und anschliessend die Machbarkeit klären. Im Verbund mit den verschiedenen Partnern des NDB soll eine einheitliche Cyberstrategie entwickelt und der von Cyber NDB zu erbringende Mehrwert definiert werden. Dabei werde insbesondere auch das Verhältnis des Ressorts Cyber NDB zum Nationalen Zentrum für Cybersicherheit (NCSC) sowie zur Melde- und Analysestelle Informationssicherung (MELANI) zu klären sein. Eines der grössten Probleme liege darin, dass sich das Phänomen Cyber nicht wirklich einordnen lässt, das Gefahrenpotential nicht sichtbar ist und auch Cyberangriffe im Ausland eine direkte Bedrohung für die Schweiz darstellen können. Nach [redacted] Ansicht wäre es denkbar, die Tätigkeit des Ressorts auf die technischen Aspekte zu beschränken, diese Aufgabe [redacted] zuzuordnen und die operativen Analysten in [redacted] zu integrieren[133].

7.1.4 Neustrukturierung des Ressorts: Mögliche Varianten

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 (siehe dazu Ziffer 5.2, Seite 25 und Ziffer 7.1.1, Seite 36). 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.

---

130 Prozess der Entwicklung von Rohinformationen zu fertigen nachrichtendienstlichen Informationen für politische Entscheidungsträger. Dabei geht es vor allem um die Anforderung, Planung und Lenkung, Sammlung, Verarbeitung und Nutzung, Analyse und Produktion sowie Verbreitung von Informationen.

131 Anhörung [redacted], S. 5f.

132 Christian Dussey hat sein Amt als Direktor NDB am 01.04.2022 angetreten.

133 Anhörung [redacted], S. 7f.

Der NDB ist sich bewusst, dass die Organisationstrukturen und Prozesse bei Cyber NDB einer umfassenden Überprüfung zu unterziehen sind (siehe dazu Ziffer 7.1.3, Seite 38). 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, [redacted]? Rechtfertigt sich damit weiterhin eine Zentralisierung in einem eigenen Ressort oder müssten die Mitarbeitenden der technischen Analyse (CyberLab) nicht konsequenterweise als Spezialisten [redacted] und die Mitarbeitenden der operativen Analyse der [redacted] 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[134] 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.

---

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

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 NCSC anzusiedeln und stünde so allen Organisationseinheiten des Bundes, die im Bereich der Cybersicherheit tätig sind, zur Verfügung.

7.2 Umgang mit Aufzeichnungen über den Netzwerkverkehr

[redacted]

7.2.1 Verkennung der Rechtslage

Cyber NDB unterhielt u.a. Kontakte zu verschiedenen Internet-Service-Providern [redacted]

[redacted] konnte sich an [redacted] nicht mehr erinnern[136]. Wie dessen unmittelbarer Vorgesetzter, Chef [redacted], ausführte, sollen der stellvertretende Direktor NDB und er auf Wunsch [redacted][137] beigezogen worden sein, um [redacted] mitzuwirken. Sie hätten in der Folge gewisse Anpassungen vorgenommen und insbesondere klargestellt, dass der Provider nicht zur Herausgabe von Informationen verpflichtet ist, sondern diese freiwillig herausgibt[138]. Der stellvertretende Direktor und er seien damals davon ausgegangen, dass der Provider die von Cyber NDB gewünschten Informationen herausgeben darf, und sie hätten die fernmelderechtlichen Probleme nicht erkannt. Der stellvertretende Direktor NDB seinerseits hatte Kenntnis [redacted], wusste aber anlässlich der Anhörung nicht, [redacted]. Auch er bestätigte aber, dass er die Tragweite der Praxis des Ressorts Cyber NDB ebenso wenig erkannt habe,

135 Dokument 400 der internen Untersuchung.
136 Anhörung [redacted], S. 6.
137 [redacted].
138 Anhörung [redacted], S. 6.

wie den Umstand, dass von ihr Bereiche tangiert wurden, die auf dem Weg genehmigungspflichtiger Beschaffungsmassnahmen hätten abgedeckt werden müssen[139].

In der Folge spielte sich bei Cyber NDB offenbar die Praxis ein, [redacted].

Das vom NDB im Rahmen der internen Untersuchung eingeholte Rechtsgutachten gelangte zum Schluss, dass [redacted] die auf freiwilliger Basis erfolgte Herausgabe der Daten nicht rechtmässig war[140].

Cyber NDB stellte [redacted] nach dem Ausscheiden des ehemaligen Chefs spätestens im Dezember 2020 ein[141].

In den Anhörungen ergab sich, dass der ehemalige Chef Cyber NDB – in Übereinstimmung mit seinem Vorgesetzten, Chef NDBI, und dem stellvertretenden Direktor NDB – damals der Überzeugung war, das Vorgehen lasse sich auf Art. 23 NDG[142] stützen: Demnach kann der NDB von jeder Person Meldungen entgegennehmen und durch schriftliche oder mündliche Anfragen gezielt Informationen einholen, die der Dienst zur Erfüllung seiner Aufgaben benötigt. Die um Auskunft ersuchte Person hat er darauf aufmerksam zu machen, dass sie freiwillig Auskunft erteilt.

Über die Frage der Rechtmässigkeit einer freiwilligen Herausgabe von Netzwerkverkehrsdaten wurde zwar intern gelegentlich diskutiert[143]. So wies insbesondere [redacted] darauf hin, dass er gemeinsam mit dem Chef [redacted] im September 2020 den stellvertretenden Direktor NDB darauf aufmerksam gemacht habe, dass ihres Erachtens die Beschaffung von Netzwerkaufzeichnungen unter Umgehung der Bestimmungen über die geheimen Beschaffungsmassnahmen nicht ganz legal sein dürfte. Die Reaktion des stellvertretenden Direktors NDB sei heftig gewesen; dieser habe vom ehemaligen Chef Cyber NDB eine schriftliche Offenlegung aller Fakten verlangt Der heutige Chef [redacted] bemängelte, dass die Fragen schon seit Jahren im Raum gestanden hätten und es immer wieder Personen gegeben habe, die darauf hingewiesen hätten. Die gegen die Vorgehensweise von Cyber NDB vorgebrachten Einwendungen seien von den verantwortlichen Führungspersonen aber einfach nicht wahrgenommen worden[144].

---

139 Anhörung Jürg Bühler, S. 4, 11.
140 Rechtsgutachten (Fn. 17), Rz. 304-308.
141 Interner Bericht (Fn. 39), S. 25.
142 Damals auf Art. 14 Abs. 2 BWIS.
143 Anhörung [redacted], S. 12.
144 Anhörung [redacted], S. 10.

7.2.2 Informationsstand Direktionsbereich NDBI und Geschäftsleitung NDB

Klarheit über die konkrete Art der Zusammenarbeit von Cyber NDB [redacted]. Der stellvertretende Direktor verlangte in der Folge vom ehemaligen Chef Cyber NDB umgehend einen schriftlichen Bericht [redacted] (siehe dazu die unter Ziffer 8.4 [Seite 37] erwähnte Aktennotiz).

Die angehörten Mitglieder der Geschäftsleitung NDB betonten, dass sie bis September 2020 keine genauen Kenntnisse über [redacted] durch Cyber NDB hatten. So erklärte der stellvertretende Direktor [redacted], für ihn sei es immer klar gewesen, dass die Anfragen an die Internet-Service-Provider nur kommerzielle und nicht Daten umfassen dürfen, die dem Fernmeldegeheimnis unterstehen. Später habe sich gezeigt, dass Cyber NDB dies offenbar anders gesehen habe. Der ehemalige Chef Cyber NDB habe zwar einmal an einer Sitzung der Geschäftsleitung und später an einem Kaderrapport in allgemeine und eher auf die Zukunft ausgerichtete Weise über den Informationsaustausch und die Zusammenarbeit der Cyberabwehr mit privaten Anbietern referiert. Die Geschäftsleitung habe dies zur Kenntnis genommen und auf die Grenzen der Gesetzgebung hingewiesen. Diskutiert worden sei auch immer wieder über die Arbeitsweise von Cyber NDB an sich und über die teilweise mangelhafte Einbindung des Ressorts in den restlichen Dienst. Nach einer Präsentation von Cyber NDB zur Bedeutung der Kontakte zu [redacted][145] habe er seine Bedenken gegenüber dem Chef NDBI geäussert. Dieser habe ihm nach einer Überprüfung gesagt, dass alles in Ordnung und sauber sei; die vom ehemaligen Chef Cyber NDB aufgebauten Kontakte seien gut. Er selbst habe die Tragweite der Praxis von Cyber NDB damals ebenso wenig erkannt wie den Umstand, dass von ihr Bereiche tangiert waren, die mittels genehmigungspflichtiger Beschaffungsmassnahmen hätten abgedeckt werden müssen. Dass Cyber NDB von Providern auf freiwilliger Basis [redacted] erhalten habe, habe er erstmals anlässlich der Besprechung mit dem ehemaligen Chef Cyber NDB im September 2020 erfahren, nachdem [redacted]. Wahrscheinlich habe die nötige Sensibilisierung auf beiden Seiten gefehlt: bei Cyber [redacted] hinsichtlich des Schutzes von Personendaten und auf der Leitungsebene für die fehlende Sensibilität von Cyber NDB[146].

Der Chef des Direktionsbereichs [redacted] gab zu Protokoll, dass er über die Zusammenarbeit des Ressorts Cyber NDB mit privaten Anbietern von Cyber-Infrastrukturen oder Cyber-Sicherheitsdienstleistungen nur aus Besprechungen innerhalb der Geschäftsleitung oder vom Hörensagen informiert gewesen sei. Vor 2019 sei der Themenbereich Cyber für ihn zweite Priorität gewesen, [redacted]. Von verdeckten Beschaffungsmassnahmen sei ihm praktisch nichts bekannt gewesen. Aus einer Präsentation [redacted]

145 [redacted]

146 Anhörung Jürg Bühler, S. 5, 11 f.

habe er nur Kenntnis von [redacted] erhalten; ob damals überhaupt die Rede von Internet-Service-Providern gewesen sei, könne er heute nicht mehr sagen. Der [redacted] durch Cyber NDB sei in der Geschäftsleitung nie thematisiert worden. Wenn schon hätte das Thema durch den direkt betroffenen Direktionsbereich NDBI eingebracht werden müssen. Der Beschaffungsteil von Cyber NDB sei im Aufbau begriffen gewesen, womit sich automatisch die Frage gestellt habe, woher und in welchem rechtlichen Rahmen Informationen bezogen werden sollen[147].

Der Chef Informationsmanagement/Cyber NDBI räumte ein, dass zwar jeder von Kontakten des Ressorts Cyber NDB zu Providern gewusst habe. Ein Zusammenhang mit der direkten Beschaffung von Informationen, die dem Fernmeldegeheimnis unterstehen könnten, sei aber nicht erkannt worden. Im Nachhinein müsse er sich vorwerfen lassen, nicht nachgefragt zu haben; damals habe er aber keinen Handlungsbedarf gesehen. Erst als ihn der stellvertretende Direktor NDB (wohl im September 2020) darauf aufmerksam gemacht habe, habe er die Problematik gesehen. Als er seinerzeit zusammen mit dem stellvertretenden Direktor NDB [redacted] habe für sie beide die Freiwilligkeit im Vordergrund gestanden. Sie seien davon ausgegangen, dass die Provider die Informationen freiwillig herausgeben dürfen; den Konnex zum Fernmeldegeheimnis hätten sie nicht erkannt.[148]

Der Rechtsdienst NDB war in die Frage der Informationsbeschaffung durch Cyber NDB nicht involviert. [redacted][149].

Der ehemalige Chef Cyber NDB gab zu Protokoll, dass sein unmittelbarer Vorgesetzter (Chef NDBI) und [redacted] immer darüber informiert gewesen seien, [redacted] Im Übrigen sei es jährlich zu einer Feedbackrunde mit der Geschäftsleitung gekommen, bei der [redacted] gemeinsam mit [redacted] und [redacted] über die Tätigkeit von Cyber NDB rapportiert hätten[150].

147 Anhörung [redacted] 7, 11.
148 Anhörung [redacted] S. 5 ff.
149 Anhörung [redacted], S. 4, 7.
150 Anhörung [redacted], S. 3.

7.2.3 Würdigung

Das Ressort Cyber NDB entwickelte weitgehend selbstständig die Praxis, [redacted] Er erkannte die Bedeutung dieser Daten für eine erfolgreiche Cyberabwehr, die Wichtigkeit der Zusammenarbeit mit privaten Partnern im Bereich der Cybersicherheit und auch [redacted]. Die Frage nach der Rechtmässigkeit der freiwilligen Herausgabe bzw. des formlosen Bezugs von Daten des Netzwerkverkehrs wurde innerhalb des Ressorts Cyber NDB aber ebenso wenig thematisiert wie diejenige nach den gesetzlich vorgegebenen und vom Dienst näher definierten Organisationsbestimmungen und Prozessabläufen. Dabei mag wohl auch die berufliche Herkunft und Sozialisation der Mitarbeitenden eine gewisse Rolle gespielt haben. Zumindest dürfte es nicht weiter überraschen, dass Mitarbeitende aus technischen Disziplinen eher eine geringe Sensibilität für rechtliche Fragestellungen an den Tag legen und einfach handeln, wenn sie dies als sinnvoll erachten[151]. Umso wichtiger wären eine klare Führung und eine bessere Einbettung des Ressorts in den Nachrichtendienst gewesen.

Nachdem das "System" Cyber NDB etabliert war, der direkte Vorgesetzte nicht (oder nicht genügend deutlich) führte und auch Direktion und Geschäftsleitung keinen Anlass sahen, den Aufbau und die weitere Entwicklung des Ressorts hinreichend zu begleiten, nahmen die Dinge ihren Lauf. Es bedurfte schliesslich der Intervention [redacted] um eine nähere Überprüfung in Gang zu setzen und dabei festzustellen, dass Cyber NDB offenbar während Jahren Daten des Netzwerkverkehrs von Providern bezogen hatte, ohne das dafür gesetzlich vorgesehene Verfahren einzuhalten.

Im Nachhinein erscheint es verhängnisvoll, dass der ehemalige Chef Cyber NDB in seinem Vorgehen – jedenfalls hinsichtlich der freiwilligen Herausgabe von Netzwerkverkehrsdaten – von seinem unmittelbaren Vorgesetzten (Vizedirektor NDB und Chef NDBI), dem stellvertretenden Direktor [redacted] sowie [redacted] noch bestärkt wurde, indem diese [redacted] in rechtlicher Hinsicht überprüft, angepasst und damit faktisch genehmigt hatten (siehe dazu Ziffer 7.2, Seite 42). Sowohl der stellvertretende Direktor NDB wie auch der Chef NDBI betonen zwar, dass für sie damals die Freiwilligkeit der Auskunftserteilung im Vordergrund gestanden habe. Sie seien nicht davon ausgegangen, dass die von Cyber NDB eingeholten Auskünfte auch Daten umfassen könnten, die dem Fernmeldegeheimnis unterstehen. Zugleich räumen sie aber ein, die rechtliche Problematik einer freiwilligen Datenherausgabe nicht erkannt zu haben.

Dass auf der Führungsebene des Nachrichtendienstes die rechtliche Problematik des Beizugs von Daten des Netzwerkverkehrs auf freiwilliger Basis bis zum Vorliegen der im Rahmen der internen Untersuchung eingeholten rechtlichen Beurteilung durch eine externe Anwaltskanzlei nicht erkannt wurde, ist schwer nachvollziehbar. [redacted] wurde ausdrücklich auf Informationen verwiesen, "die sich beispielsweise aus den Verbindungsdaten ergeben können". Ein Bezug zum Fernmeldegeheimnis wurde zwar hergestellt, aber trotzdem klar auf die Bedeutung der Verbindungsdaten für die Arbeit von

151 Anhörung Jürg Bühler, S. 8.

Cyber NDB hingewiesen. Selbst wenn beim Chef NDBI und beim stellvertretenden Direktor NDB Unklarheiten über die genaue Art der von Cyber NDB beschafften Daten bestanden haben sollten, stellt sich die Frage, weshalb sich der Chef NDBI als unmittelbarer Vorgesetzter beim ehemaligen Chef Cyber NDB nicht weiter nach der konkreten Art der Daten erkundigt hatte, [redacted], und auch auf jede weitere Überprüfung der Abläufe im Ressort Cyber NDB und der von den Providern gelieferten Daten verzichtet hatte.

Spätestens die Diskussionen um das am 1. September 2017 in Kraft getretene Nachrichtendienstgesetz, mit welchem dem NDB erstmals Befugnisse zu genehmigungspflichtigen Beschaffungsmassnahmen eingeräumt wurden, hätten zwingend zum Anlass genommen werden müssen, die Beschaffungsabläufe innerhalb des Ressorts Cyber NDB einer genaueren Überprüfung zu unterziehen. Schon damals musste der Geschäftsleitung bekannt gewesen sein, dass sich die Arbeit von Cyber NDB im Wesentlichen auf die Auswertung von Randdaten des Netzwerkverkehrs stützte. Ebenso war allgemein bekannt, dass das Ressort Cyber NDB [redacted] Nachfragen zur konkreten Ausgestaltung der Arbeitsmethoden von Cyber NDB erfolgten jedoch nicht. Unverständlich erscheint heute, dass der zuständige Direktionsbereichsleiter und die Geschäftsleitung bis September 2020 keine Kenntnis von der während Jahren praktizierten unrechtmässigen Informationsbeschaffung des Ressorts hatten (siehe dazu Ziffer 7.2.2, Seite 44). Dies lässt eigentlich nur den Schluss zu, dass es an einer effizienten Führung und Beaufsichtigung fehlte.

7.3 Cyber NDB und die Strategie des Nachrichtendienstes

Im Bereich der Führungs- und Diskussionskultur innerhalb des NDB besteht Optimierungspotential. Die Vorkommnisse bei Cyber NDB sind im Nachhinein auch deshalb nur erklärbar, weil die einzelnen Direktionsbereiche im Wesentlichen die ihnen zugewiesenen "Gärtchen gepflegt" und zu wenig den Blick auf das Gesamte gelegt haben. Während zu langer Zeit stand auf der Führungsebene des NDB das Bestreben im Vordergrund, sich gegenseitig abzugrenzen, auf formellen Verantwortlichkeiten zu beharren, aufkeimende Fragen oder Kritik von Mitarbeitenden nicht genügend erst zu nehmen und im Wesentlichen darauf zu vertrauen, dass alles wohl in Ordnung ist.

Die unterschiedlichen Reaktionen der einzelnen Direktionsbereiche auf die interne Untersuchung (siehe Ziffer 3.2, Seite 19), aber auch Erkenntnisse aus der Untersuchung selbst (siehe Ziffer 7.1, Seite 36), vermitteln den Eindruck, dass es auf der obersten Führungsebene gelegentlich an einer ganzheitlichen Betrachtungsweise und damit auch

an einem Bewusstsein für eine Gesamtverantwortung gefehlt zu haben scheint[152]. Einzelne Direktionsbereiche zogen es vor, die eigenen Interessen in den Vordergrund zu stellen, sich nicht gross in die Belange anderer Bereiche einzumischen und sich auch nicht für dort allenfalls vorhandene, den Dienst als Ganzes betreffende Problemstellungen zu interessieren. Dies zeigte sich besonders deutlich bei den Diskussionen über die Verantwortlichkeit für die unrechtmässigen Beschaffungsmethoden von Cyber NDB: Der [redacted] legte allein Wert darauf, dass [redacted]. Demgegenüber stellte sich der für Cyber NDB zuständige NDBI auf den Standpunkt, dass die Beschaffung von Informationen nicht sein Direktionsbereich Informationsmanagement/Cyber zu verantworten habe, sondern grundsätzlich in der Zuständigkeit von [redacted] liege. Cyber NDB seinerseits versuchte gar, noch im Rahmen der internen Untersuchung den Eindruck zu erwecken, dass es sich bei seinen Aktivitäten gar nicht um Beschaffungsmassnahmen gehandelt habe. Das fehlende Bewusstsein für eine gemeinsame Führungsverantwortung zeigt sich aber auch darin, dass während Jahren weder Direktion noch Geschäftsleitung die rechtliche Problematik der unrechtmässigen Beschaffung von Aufzeichnungen des Netzwerkverkehrs durch Cyber NDB erkannten. Sie wurden erst aktiv, nachdem [redacted] Vorbehalte [redacted] vorgebracht hatten, worauf der Chef [redacted] deswegen eine Untersuchung verlangt hatte. Erst dann wurde auch die Vorgehensweise von Cyber NDB näher überprüft, wobei – quasi als "Beifang"[153] – bekannt wurde, dass das Ressort während Jahren ohne Einhaltung der Bestimmungen über genehmigungspflichtige Beschaffungsmassnahmen von Internet-Service-Providern [redacted]

Im Rahmen einer Administrativuntersuchung muss es bei diesen Feststellungen bleiben. Es wird Aufgabe des Direktors NDB sein, gemeinsam mit den Mitgliedern der Geschäftsleitung die ihm geeignet erscheinenden Massnahmen in die Wege zu leiten, um die Zusammenarbeit der verschiedenen Direktionsbereiche zu fördern, bestehende Spannungen abzubauen und eine gemeinsame Führungs- und Verantwortungskultur zu entwickeln.

---

152 So sprach etwa [redacted], von einer fehlenden Diskussionskultur auf der Führungsebene des Nachrichtendienstes (Anhörung [redacted], S. 5).

153 Anhörung [redacted] S. 15.

8 Weitere Feststellungen

8.1 Informationsaustausch mit ausländischen Partnerdiensten

Die Zusammenarbeit, insbesondere der Informationsaustausch mit ausländischen Nachrichtendiensten und Sicherheitsbehörden, ist im Nachrichtendienstgesetz geregt (Art. 12 NDG) und gibt im vorliegenden Zusammenhang zu keinen Bemerkungen Anlass. Eine intensive internationale Zusammenarbeit und Vernetzung ist – wie auch in den von Bundesrat und Departement verabschiedeten Cyberstrategien betont wird (siehe dazu Ziffer 2, Seite 14) – ohnehin unabdingbar.

8.2 Zusammenarbeit mit privaten Unternehmen im Bereich der Cybersicherheit

In Bezug auf die Zusammenarbeit mit Privatpersonen sieht Art. 23 NDG vor, dass der NDB von jeder Person Meldungen entgegennehmen kann. Er kann durch Anfragen gezielt Informationen einholen, die er zur Erfüllung seiner Aufgaben benötigt. Die um Auskunft ersuchte Person ist darauf aufmerksam zu machen, dass sie freiwillig Auskunft gibt.

Im Bereich der "Cyber-Threat-Intelligence"[154] sind nicht nur staatliche Nachrichtendienste, sondern auch private Unternehmen aktiv. [redacted][156].

[redacted][157].

154 Evidenzbasierte Informationen über Cyberangriffe, die von Experten geordnet und analysiert werden und von auf Cybersicherheit spezialisierten Unternehmen weiteren Abnehmern kommerziell zur Verfügung gestellt werden. Diese können Angaben zu den Mechanismen eines Angriffs, zur Erkennbarkeit eines Angriffs, zu den Beeinträchtigungen eines Angriffs oder zu massnahmenorientierten Empfehlungen zur Abwehr eines Angriffs enthalten.

155 [redacted]

156 Vgl. dazu Clement Guitton, Der Schweizer Nachrichtendienst seit der Fichenaffäre. Was er kann und was er darf, Zürich 2018, S. 198f.

157 Anhörung [redacted] S. 10.

[redacted][158].

[redacted][159].

[redacted]

8.3 Zahlungen an [redacted]

[redacted][161].

158 Anhörung [redacted] und [redacted], S. 8.
159 Stellungnahme Ressort Cyber NDB 02.09.2021 (Dokument 452 der internen Untersuchung), S. 4.
160 Interner Bericht (Fn. 39), S. 34.
161 Anhörung [redacted], S. 5.

[redacted][162].

[redacted].

[redacted].

8.4 Zahlungen an Internet-Service-Provider

[redacted].

[redacted][164].

Der interne Bericht stützt seine Aussage im Wesentlichen auf eine vom ehemaligen Chef Cyber NDB erstellte Aktennotiz ab. Die Aktennotiz ist zwar weder datiert noch unterzeichnet und enthält auch sonst keine Hinweise auf den Verfasser. Sie dürfte aber mit höchster Wahrscheinlichkeit vom ehemaligen Chef Cyber NDB im Anschluss an die Aussprache vom 29. September 2020 erstellt worden sein. Anlässlich jener Besprechung wurde der ehemalige Chef Cyber NDB vom stellvertretenden Direktor NDB [redacted] ultimativ aufgefordert, das konkrete Vorgehen von Cyber NDB bei der

---

162 Anhörung [redacted], S. 10; vgl. auch Anhörung [redacted], S. 4; Anhörung [redacted], S. 11.

163 Interner Bericht (Fn. 39), S. 15 und 17.

164 Interner Bericht (Fn. 39), S. 50.

Beschaffung von Netzwerkaufzeichnungen in schriftlicher Form detailliert darzulegen (siehe dazu Ziffer 7.2.2, Seite 44)[165].

In dieser Aktennotiz betont der ehemalige Chef Cyber NDB die Wichtigkeit [redacted]. Zugleich legt er die konkreten Modalitäten der Informationsbeschaffung offen, welche [redacted]. Er brachte vor, es sei möglich, dass [redacted] es sei aber auch möglich, dass [redacted]. Ein erheblicher Teil von Anfragen [redacted] habe Server betroffen, die von [redacted] gehostet werden. Cyber NDB habe 2015 über [redacted] einen Kontakt etabliert. Zwischen 2015 und 2018 sei die Kontaktperson mit [redacted] Franken pro Jahr für die Aufwendungen im Zusammenhang mit der Erstellung von Serverabbildern entschädigt worden. Neben [redacted] seien [redacted] weitere Provider für ihre Aufwendungen im Zusammenhang mit der Zurverfügungstellung von Serverabbildern entschädigt worden.

In der Notiz des ehemaligen Chefs Cyber NDB wird weiter festgehalten, dass die Kontaktperson bei [redacted] aus dem Unternehmen ausgeschieden sei und [redacted]. Seit dem Ausscheiden der Kontaktperson beziehe der NDB keine Netzwerkverkehrsdaten mehr und habe dafür auch keine Zahlungen mehr geleistet. [redacted]

Der ehemalige Chef Cyber NDB hatte die in der Aktennotiz festgehaltenen Positionen bereits anlässlich der Besprechung u.a. mit dem stellvertretenden Direktor NDB [redacted] vom September 2020 mündlich vorgetragen. Dieser lehnte eine Variantendiskussion ab und erteilte dem ehemaligen Chef Cyber NDB den Auftrag, zunächst die Fakten der bisherigen Zusammenarbeit mit [redacted] detailliert und schriftlich darzustellen und insbesondere den Chef NDBI darüber zu informieren, welche Art von Daten auf welchem Weg beschafft werden. Es müsse geprüft werden, ob die von Cyber NDB beschafften Daten allenfalls unter den Anwendungsbereich des

165 Dokumente 600 bis 602 der internen Untersuchung.

Fernmeldegeheimnisses fallen[166]. Wie der stellvertretende Direktor [redacted] in der Administrativuntersuchung ausführte, erfuhr er erstmals an dieser Besprechung Details über die Art der von Cyber NDB durch Vermittlung von [redacted] beschafften Daten. Er habe dem ehemaligen Chef Cyber NDB erklärt, dass man sich damit mit grösster Wahrscheinlichkeit auf sehr heikles Gebiet begebe. Solange die Frage der Rechtmässigkeit der Datenbeschaffung nicht geklärt sei, kämen finanzielle Investitionen nicht in Frage. Eine mögliche Beteiligung des NDB an [redacted] müsste im Übrigen auch politisch geklärt werden, zumal der NDB nach den Vorgaben der GPDel aufgrund der Inspektion zum Fall Crypto AG mindestens an das Departement, wenn nicht an den Bundesrat gelangen müsste[167].

Die Aktennotiz fand keinen Eingang in die offiziellen Unterlagen des NDB und konnte – wohl durch Vermittlung eines Mitarbeitenden oder einer Mitarbeitenden von Cyber NDB oder von [redacted] – erst in der internen Untersuchung beigebracht werden. Damals führte der stellvertretende Direktor NDB ([redacted]) aus, er habe einen ersten Bericht des ehemaligen Chefs Cyber NDB, dessen Detaillierungsgrad allerdings ungenügend gewesen sei, wohl einmal erhalten, in der Folge aber wieder zurückgegeben. Der Chef NDBI gab in der Administrativuntersuchung zu Protokoll, dass er die Aktennotiz erstmals im Dezember 2021 im Rahmen der internen Untersuchung gesehen habe[168]. Der Chef [redacted] führte aus, dass er von den Beschaffungsmassnahmen von Cyber NDB praktisch nichts gewusst habe, da das Ressort nicht ihm, sondern dem Chef NDBI unterstellt gewesen sei. Der Chef Cyber NDB habe einmal in der Geschäftsleitung von [redacted] gesprochen, die sehr teuer, aber für seine Arbeit essenziell seien. Ob damals auch von privaten Anbietern von Server-Dienstleistungen die Rede gewesen sei, könne er heute nicht mehr sagen[169].

Der ehemalige Chef Cyber NDB konnte sich anlässlich seiner Anhörung in der internen Untersuchung nicht mehr an das fragliche Dokument erinnern. Hingegen räumte er ein, dass damals auch eine Übernahme von [redacted] durch den NDB als mögliches Szenario erwähnt worden sei. In der Administrativuntersuchung bestätigte er, dass er sich an jenes Papier nicht mehr erinnern könne. Es sei ihm bekannt, dass [redacted], aber auch andere Provider, dafür entschädigt worden seien, dass sie ihre Infrastruktur dem NDB zur Verfügung gestellt hatten. Die Zahlungen seien aber sicher nicht von Cyber NDB selbst geleistet worden; sein Ressort habe [redacted] über die normalen Beschaffungswege gekauft; schwarze Kassen für Zahlungen an Provider hätten keine bestanden. Auch von überteuerten [redacted] sei ihm nichts bekannt gewesen[170].

Ob und allenfalls welche Zahlungen der NDB an [redacted] und allenfalls andere Provider für das Zur-Verfügung-Stellen von Netzwerkverkehrsdaten geleistet hatte, konnte weder in der internen Untersuchung noch in der Administrativuntersuchung geklärt werden. Im Buchhaltungssystem des NDB sind keine Transaktionen an Internet-

166 Interner Bericht (Fn. 39), S. 50f.
167 Anhörung Jürg Bühler, S. 8.
168 Anhörung [redacted], S. 17.
169 Anhörung [redacted], S. 6f, 17.
170 Anhörung [redacted], S. 7 f.

Service-Provider oder deren Kontaktpersonen, mit denen Cyber NDB zusammengearbeitet hatte, erfasst[171].

Im Rahmen der Administrativuntersuchung wurde dem Chef [redacted]) eine Liste mit neun namentlich bezeichneten Unternehmen und den Namen von weiteren [redacted] Privatpersonen zum Zweck der Abgleichung mit den Buchhaltungsunterlagen des NDB unterbreitet. In der Buchhaltung finden sich für die Jahre 2015 bis 2020 ausschliesslich Zahlungen an [redacted] Cybersicherheitsunternehmen, mit denen Verträge [redacted] bestehen. Die übrigen Organisationen oder Privatpersonen sind in der Buchhaltung nicht verzeichnet.

[redacted] zählte zu den Zahlungsempfängern des NDB. Die entsprechenden Zahlungen beliefen sich für die Jahre 2015 bis 2017 auf je [redacted]; ab 2018 erfolgte eine Erhöhung auf [redacted]. 2019 wurde mit [redacted] zusätzlich zum bestehenden Vertrag [redacted] ein zweiter Vertrag mit zusätzlichen Leistungen [redacted]) abgeschlossen, womit sich die jährlichen Kosten auf [redacted] erhöhten[172].

Anhaltspunkte dafür, dass es sich beim zweiten Vertrag nicht um die Abgeltung zusätzlicher Leistungen von [redacted] handelt, bestehen nicht, zumal der für die Antragstellung zuständige Direktionsbereichsleiter NDBI auf dem internen Laufblatt die beiden Verträge als unerlässliche Grundlage für Cyber NDB bezeichnet hatte. Auffallend könnte allein der Zeitpunkt [redacted] sein, der mit dem Bekanntwerden [redacted] korreliert. Die Herleitung eines direkten Zusammenhangs zu verdeckten Zahlungen an [redacted] würde jedoch auf rein spekulativen Überlegungen beruhen. Keine der angehörten Personen hatte Kenntnis von offenen oder verdeckten Zahlungen an [redacted] oder andere Internet-Service-Provider. Der ehemalige Chef Cyber NDB, der die seinerzeitigen Vertragsverhandlungen mit [redacted] geführt hatte, beharrte darauf, dass [redacted] ausschliesslich [redacted] auf dem ordentlichen Beschaffungsweg gekauft habe; von verdeckten Zahlungen oder überteuerten [redacted] sei ihm nichts bekannt.

Der Chef NDBI sagte in der internen Untersuchung aus, es sei ihm nie aufgefallen, dass der NDB bei [redacted] zu überteuerten Preisen eingekauft habe und ein Teil des Geldes an [redacted] weitergeflossen sein könnte. In der Administrativuntersuchung betonte er, dass er als Direktionsbereichsleiter [redacted] über keine schwarze Kasse oder über besondere Möglichkeiten zur Finanzierung von Quellen verfüge, wie dies allenfalls im Bereich [redacted] vorgesehen sei[173]. Der stellvertretende Direktor [redacted]) erklärte im Verlauf der internen Untersuchung, es erscheine ihm durchaus plausibel, dass der NDB mit überteuerten [redacted] bei [redacted] das Unternehmen [redacted] querfinanziert haben könnte. Weitere Angaben konnte aber auch er dazu nicht machen. Auf möglicherweise verdeckte Zahlungen angesprochen, erklärten die Mitarbeitenden von Cyber NDB, dass alles was verdeckt sei, sicher nicht bei ihnen geschehe[174].

---

171 Interner Bericht (Fn. 32), S. 21.
172 Buchhaltungsunterlagen NDB.
173 Anhörung [redacted], S. 10; vgl. auch Anhörung [redacted], S. 4.
174 Anhörung [redacted], S. 11.

Auf eine Anhörung des ehemaligen Chefs [redacted][175] wurde wie schon in der internen Untersuchung auch in der Administrativuntersuchung verzichtet. Einerseits sieht das Gesetz Entschädigungen an Quellen explizit vor und verpflichtet den NDB zum Schutz seiner Quellen[176]. Es lässt damit verdeckte Zahlungen und Massnahmen zu deren Verschleierung ausdrücklich zu und nimmt so in Kauf, dass verdeckt geleistete Zahlungen nicht aufgeklärt werden können. Der Beauftragte geht im Weitern davon aus, dass auch nach einem personellen Wechsel das institutionelle Wissen innerhalb des Nachrichtendienstes erhalten bleibt und folglich die jetzigen Funktionsträger die erforderlichen Auskünfte erteilen können. Schliesslich kommt hinzu, dass der ehemalige Chef [redacted], sodass er [redacted][177]. Sollte die Auftraggeberin eine Anhörung des ehemaligen Chefs [redacted] zur Abklärung allfällig geleisteter Zahlungen des NDB an Internet-Service-Provider als erforderlich oder sinnvoll erachten, kann dies nachgeholt werden.

8.5 [redacted]

[redacted]

8.6 Informations- und Speichersysteme des Ressorts Cyber

Das Nachrichtendienstgesetz bezeichnet insgesamt neun Informationssysteme, welche der NDB zur Erfüllung seiner Aufgaben betreibt (Art. 47 NDG). Das Gesetz umschreibt die in den jeweiligen Informationssystemen aufzunehmenden Daten und regelt die Zugriffsberechtigung (Art. 48 bis 57 NDG). Zugleich verpflichtet es den Bundesrat, für jedes Informationssystem den Katalog der Personendaten, die Zuständigkeiten bei der Datenbearbeitung, die Zugriffsrechte, die Häufigkeit der Qualitätssicherung, die Aufbewahrungsdauer der Daten, die Löschung der Daten sowie die Datensicherheit zu regeln. Gestützt darauf hat der Bundesrat die Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes erlassen. Die Verordnung umfasst 75 Artikel, die mit insgesamt 13 Anhängen ergänzt werden.

Cyber NDB hat zwar im Bereich der Datenablage und der Kommunikationsmittel eigene Systeme entwickelt (siehe dazu Ziffer 5.4, Seite 28). Die entsprechenden Anschaffungen wurden aber von den zuständigen Instanzen genehmigt und sind in der Buchhaltung

175 [redacted].
176 Art. 15 Abs. 2 und 3 NDG.
177 Art. 27g Abs. 2 und Art. 27h Abs. 3 RVOV.

ausgewiesen. Von einem eigenmächtigen Vorgehen des Ressorts kann in diesem Zusammenhang nicht gesprochen werden. Dass entsprechende Reglemente nicht oder erst sehr spät erlassen wurden, fällt nicht in den Verantwortungsbereich von Cyber NDB. Hingegen muss es sich den Vorwurf gefallen lassen, seine Arbeitsweise nicht hinreichend dokumentiert zu haben. Deshalb lassen sich gewisse Elemente der seinerzeitigen Vorkommnisse heute nicht mehr rekonstruieren.

Die im internen Bericht erhobenen Beanstandungen der internen Datenerfassung und -verwaltung durch Cyber NDB[178] dürften mit der laufenden Revision des NDG weitgehend hinfällig werden. Der Revisionsentwurf sieht ein vollständig neues Datenhaltungskonzept vor. Die neue Datenbearbeitungskonzeption zeichnet sich durch eine Fokussierung auf die Daten und deren Bearbeitung aus. Die Eingangsprüfung, die Qualitätssicherung der Daten und die Datenbekanntgabe werden einheitlich geregelt. Zentral ist dabei der Verzicht auf eine Differenzierung in verschiedene Informations- und Speichersysteme[179].

Spezifisch auf die Bedürfnisse von Cyber NDB ausgerichtet ist Art. 49 Abs. 2 lit j des Vorentwurfs: Daten aus der technischen Analyse von sicherheitspolitisch bedeutsamen Cyberangriffen werden neu besonders gekennzeichnet. Es geht um die Daten des Technischen Labors Cyber NDB, welche auf einem gesonderten Netzwerk gespeichert und ausgewertet werden. Diese technischen Daten dienen der dynamischen Analyse von technisch kompromittierten Netzwerken und Computern. Bezeichnend ist, dass dabei keine Personendaten bearbeitet werden[180]. Die Zusammenfassung und Auswertung der Daten erfolgt heute im Informations- und Analysesystem Allsource (IASA) des NDB.

Auch hier wird es Aufgabe der Direktion und der Geschäftsleitung NDB sein, die im Hinblick auf eine Umsetzung des vorgesehenen Datenbearbeitungs- und Datenhaltungskonzepts erforderlichen Arbeiten an die Hand zu nehmen und dabei insbesondere auf die spezifische Art der von Cyber NDB zu bearbeitenden Daten Rücksicht zu nehmen.

8.7 Abgang des ehemaligen Chefs des Ressorts Cyber

[redacted] hatten anlässlich von bilateralen Treffen mit Mitarbeitenden des NDB erstmals im Herbst 2018 Vorbehalte gegenüber dem ehemaligen Chef Cyber NDB geäussert. Ab Frühjahr 2020 nahmen die Interventionen zu; und im Dezember 2020 kam es schliesslich zu einem Treffen auf Direktionsstufe. Die Vorbehalte bezogen sich im Wesentlichen auf eine angeblich zu grosse Nähe des ehemaligen Chefs Cyber NDB zum Unternehmen [redacted] sprachen von einem äusserst kritischen Datenabfluss an [redacted], wobei die Gefahr bestehe, dass die Informationen [redacted][181].

178 Interner Bericht (Fn. 39), S. 28 ff.
179 Erläuternder Bericht des Bundesrates zur Revision des Nachrichtendienstgesetzes (Fn. 51), S. 15 f.
180 Erläuternder Bericht des Bundesrates zur Revision des Nachrichtendienstgesetzes (Fn. 51), S. 20.
181 [redacted]

Noch vor der Eröffnung der NDB-internen Untersuchung zu den Vorkommnissen im Ressort Cyber NDB nahm die Geschäftsleitung NDB Abklärungen zu den erhobenen Vorwürfen auf. Die Vorbehalte [redacted] konnten nicht erhärtet, teilweise aber widerlegt werden; Soweit dies nicht gelang, konnte zumindest eine nachvollziehbare Erklärung für die Reaktionen [redacted] gefunden werden[182].

[redacted][183]. Der ehemalige Chef Cyber NDB [redacted] trat Ende Februar 2021 aus dem Dienst aus. Gegenüber dem Personal wurde die Auflösung des Arbeitsverhältnisses zunächst dahingehend kommuniziert, dass der Direktor NDB entschieden habe, [redacted][185], stiess aber bei den Mitarbeitenden teilweise auf geringes Verständnis und trug wenig zu einer Verbesserung der Arbeitsatmosphäre im Ressort Cyber NDB bei[186].

Das Ausscheiden des ehemaligen Chefs Cyber NDB bildete auch Gegenstand der im April 2021 angeordneten internen Untersuchung. Dort konnten keine Hinweise gefunden werden, die im Zusammenhang mit dem Ausscheiden des ehemaligen Chefs Cyber NDB auf Unregelmässigkeiten bei der Datenlöschung bzw. Datenvernichtung schliessen liessen[187]. Der Austrittsprozess des ehemaligen Chef Cyber NDB ist dokumentiert; es wurde sichergestellt, dass keine physischen oder digitalen Datenträger vernichtet werden konnten[188]. Die Administrativuntersuchung hat sich deshalb mit diesem Aspekt nicht mehr näher befasst.

Die Administrativuntersuchung ergab auch bezüglich der von [redacted] gegenüber dem ehemaligen Chef Cyber NDB geäusserten Bedenken keine neuen Erkenntnisse. Der Chef [redacted] brachte jedoch vor, dass im Zusammenhang mit den geäusserten Vorbehalten an falschen Orten gesucht worden sei, wo nichts habe gefunden werden können. Die erst im Rahmen der internen Untersuchung neu aufgetauchten Chat-Protokolle des ehemaligen Chefs und der Mitarbeitenden von Cyber NDB seien damals, d.h. zum Zeitpunkt der von [redacted] vorgebrachten Vorbehalte, noch nicht bekannt gewesen. Mobilgeräte, Laptops etc. des ehemaligen Chefs und der Mitarbeitenden von Cyber NDB seien bis heute nicht ausgewertet. Eine Auswertung läge im Interesse der Glaubwürdigkeit des Dienstes,

---

[redacted]:
).

182 E-Mail [redacted] an [redacted] und [redacted] 30.10.2020 (Dokument 421 der internen Untersuchung); vgl. auch Anhörung [redacted] S. 14ff.; Anhörung [redacted], S. 7.

183 Befragung [redacted] in der internen Untersuchung; vgl. auch Anhörung [redacted], S. 7.

184 Interner Bericht (Fn. 39), S. 15; E-Mail-Kommunikation NDB an alle Mitarbeitenden 27.01.2021 (Dokument 631 der internen Untersuchung).

185 Bericht Abklärungsauftrag [redacted] (Dokument 607 der internen Untersuchung).

186 Stellungnahme [redacted] zum internen Berichtsentwurf (Dokument 709 der internen Untersuchung).

187 Interner Bericht (Fn.39), S. 34.

188 Dokumente 435 und 608 der internen Untersuchung.

auch wenn diese "nur" zum Resultat käme, dass sich auch dort nichts finden lässt. Für die Auswertung der Chatverläufe müsste jemand aus dem Team Cyber beigezogen werden, der diese interpretieren und in einen Kontext stellen könnte. Den Aufwand könne er nicht abschätzen, er wäre aber gewaltig[189].

Das vom [redacted] geäusserte Bedürfnis nach völliger Klarheit über den Informationsaustausch von Cyber NDB ist verständlich. Es scheint aber fraglich, ob die von ihm gewünschte Gewissheit tatsächlich geschaffen werden kann: Zum einen lassen sich negative Tatsachen (z.B. kein unerlaubter Informationsabfluss) ohnehin nicht beweisen. Zum andern wurden die von [redacted] erhobenen Vorbehalte – soweit sie auf feststellbaren Tatsachen beruhten – abgeklärt und konnten teilweise widerlegt oder zumindest plausibel erklärt werden. Die Kontakte von Cyber NDB zu [redacted], die zu den Vorbehalten geführt hatten, bestehen heute nicht mehr.

Mit den in der Zwischenzeit vorgenommenen Reorganisationsmassnahmen wurde die Arbeit von Cyber NDB auf eine neue Grundlage gestellt. Sowohl die Prozesse wie auch die Dokumentationspflichten wurden neu geregelt. Offenbar scheint sich mit dem Weggang des ehemaligen Chefs auch die Zusammenarbeit mit den [redacted] wieder normalisiert und stabilisiert zu haben, so dass aus Sicht des Untersuchungsbeauftragten diesbezüglich auf weitere Abklärungen verzichtet werden kann. Kommt hinzu, dass die Auswertung von internen Chatprotokollen, Computern und Kommunikationsmitteln nicht nur besondere technische Fertigkeiten und Spezialkenntnisse voraussetzt, sondern auch einen nicht absehbaren Aufwand verursachen würde.

8.8 Das Ressort Cyber nach dem Ausscheiden des ehemaligen Chefs

Das Ressort Cyber steht seit [redacted] des ehemaligen Chefs Cyber NDB [redacted] und seinem definitiven Ausscheiden per Ende Februar 2021 unter interimistischer Leitung. Die Stelle wurde bis zum Abschluss der Administrativuntersuchung nicht definitiv besetzt. Der erste Chef a.i.[190] wurde schon rasch wieder freigestellt. Seiner Stellvertreterin[191] wurde eine interne Versetzung in Aussicht gestellt, worauf sie im Mai 2022 ihre Kündigung einreichte und ebenfalls freigestellt wurde[192]. Seither verfügt das Ressort Cyber NDB wiederum lediglich über eine interimistische Leitung[193] (siehe dazu auch Ziffer 7.1.3, Seite 38).

Nach dem Abgang des ehemaligen Chefs war die Verunsicherung innerhalb des Ressorts Cyber NDB gross. So gab der stellvertretende Direktor NDB zu Protokoll, dass die interne Untersuchung und die damit verbundenen Entscheide sehr viel Angst und Verunsicherung ausgelöst und zu einer permanenten Verschlechterung der Stimmung und zur Bildung von rivalisierenden Gruppen geführt hatten. Nicht zuletzt aufgrund der beschönigenden Kommunikation der Direktion des NDB (siehe dazu Ziffer 8.7, Seite 56) hätten sich die Mitarbeitenden für „dumm verkauft" gefühlt. Die Ernennung des neu eingesetzten und schon bald wieder abgelösten Chefs ad Interim habe wenig zur

189 Anhörung [redacted] S. 9ff.
190 [redacted]
191 [redacted]
192 Siehe dazu Anhörung [redacted] S. 3.
193 [redacted]

Stabilisierung beigetragen. Mitarbeitende hätten sich mit Beschwerden an die Sicherheit und auch an die Vertrauensstelle für das Bundespersonal gewandt. Die Geschäftsleitung sei deshalb zum Schluss gekommen, dass es so nicht weitergehen könne, und habe das Ressort Cyber NDB neu [redacted] unterstellt. Weil [redacted] nicht vorbelastet gewesen und habe eine neutralere Sicht auf die involvierten Personen gehabt[194].

Wie bereits dargelegt, führte der Chef [redacted] aus, dass es innerhalb des NDB erhebliche Widerstände gegen die Durchführung der internen Untersuchung gegeben habe (siehe Ziffer 3.2, Seite 19). Mit dem Weggang des ehemaligen Chefs und des Chefs a.i. sei wieder etwas Ruhe eingekehrt. Diejenigen Mitarbeitenden von Cyber NDB, die auf die Missstände hingewiesen hätten, hätten heute aber einen schweren Stand, weil sie nach Ansicht der „früheren Führungsclique" ein vermeintlich so gut funktionierendes System „kaputt" gemacht hätten. Andere würden sich fragen, warum sie nicht wieder so arbeiten können wie bisher. Das zeige die ganze Tragik der Entwicklung der letzten Jahre[195].

Auf die Wichtigkeit einer sorgfältigen Auswahl bei der Neubesetzung der Stelle Chef Cyber NDB wurde bereits hingewiesen (siehe Ziffer 7.1.3, Seite 38). Aufgabe der Direktion und der Geschäftsleitung NDB wird es sein, für Cyber NDB klare Strukturen zu schaffen und Prozesse zu definieren. Die Mitarbeitenden müssen klare Vorgaben erhalten und vor allem wissen, was von ihnen erwartet wird, welche Aufgaben sie zu erfüllen und an welche Vorgaben sie sich zu halten haben. Gemeinsam mit [redacted] und der Führungsebene des Nachrichtendienstes wird es eine der zentralen Aufgaben des neuen Chefs oder der neuen Chefin Cyber NDB sein, Ruhe in den Betrieb zu bringen, bestehende Fronten aufzulösen und das Ressort als gleichberechtigtes und gleichgestelltes Team in das Gesamtgefüge des Nachrichtendienstes zu integrieren.

Die im Rahmen der internen Untersuchung eingeholte rechtliche Beurteilung der Datenbeschaffung, -auswertung und -weitergabe hat bei den Mitarbeitenden des Ressorts Cyber NDB erhebliche Verunsicherung ausgelöst. Sie wissen nicht mehr, was sie noch vorkehren dürfen und welche Konsequenzen sich möglicherweise aus ihrem Handeln ergeben können[196]. Es wird deshalb auch hier nötig sein, klare Handlungsanweisungen zu erlassen, um für die Mitarbeitenden allfällige Risiken strafrechtlicher oder anderer Natur auszuschliessen (siehe dazu Ziffer 10, Seite 77).

8.9 Stellenwert der Leistungen von Cyber NDB: Eine Einschätzung

Es ist unbestritten sein, dass die Arbeit von Cyber NDB in den Jahren 2015 bis 2020 sehr erfolgreich war. [redacted]

194 Anhörung Jürg Bühler, S. 9.

195 Anhörung [redacted], S. 12 und 14.

196 So spricht etwa der [redacted] davon, dass er früher dem Opfer eines Cyberangriffs vor Ort das Vorgehen erklärt habe. Heute wisse er aber nicht einmal mehr, ob er es nach Logfiles oder Verbindungsdaten fragen darf. Gemäss Rechtsgutachten "nein", gemäss Geschäftsleitung "ja". Er brauche eine klare Anweisung, die bis heute fehle (Anhörung [redacted], S. 19).

[redacted]. Dies darf aber nicht darüber hinwegtäuschen, dass einerseits der Erfolg u.a. auf unrechtmässigen Beschaffungsmethoden beruhte und andererseits das weitgehende Eigenleben des Ressorts Cyber NDB innerhalb des Nachrichtendienstes zu schwerwiegenden Spannungen führte.

9 Cyber NDB und genehmigungspflichtige Beschaffungsmassnahmen

9.1 Erkenntnisse des vom NDB eingeholten Rechtsgutachtens

In der internen Untersuchung hat die Anwaltskanzlei [redacted] im Auftrag des NDB eine "rechtliche Beurteilung zur Informationsbeschaffung und -bearbeitung im Zusammenhang mit Cyberangriffen" vorgenommen und darüber im November 2021 einen Bericht verfasst. Grundlage der rechtlichen Beurteilung bildeten nicht die konkreten Vorkommnisse bei Cyber NDB, sondern verschiedene hypothetische Sachverhalte, die vom internen Untersuchungsteam des NDB aufgrund seiner vorläufigen Erkenntnisse aus der internen Untersuchung zusammengestellt und mit abstrakt formulierten Fragestellungen zur Rechtslage ergänzt worden waren[197].

Der externe Bericht erweist sich in diesem Sinn als weitgehend abstrakt gehaltene, allgemeine Auslegeordnung der rechtlichen Grundlagen für die Informationsbeschaffung und -bearbeitung des NDB im Zusammenhang mit Cyberangriffen. Der Ausgangslage entsprechend (hypothetische Sachverhalte und abstrakte Fragestellungen), werden die massgebenden Rechtsnormen dargestellt und unter Berücksichtigung der allgemeinen Auslegungskriterien sowie der Literatur und Rechtsprechung einer dogmatischen Einzelanalyse unterzogen.

Der Bericht setzt sich aber nicht näher mit den spezifischen Anforderungen des Nachrichtendienstes, den konkreten Informationsbedürfnissen und Arbeitsmethoden von Cyber NDB und auch nicht mit den Problemstellungen im konkreten Arbeitsalltag auseinander. In Übereinstimmung mit ihrem Auftrag nehmen die Verfasser und Verfasserinnen eine Einordnung auf der Grundlage des geltenden Rechts vor, ohne dieses im Hinblick auf seine Praxistauglichkeit zu hinterfragen. Abschliessend weisen sie zwar in allgemeiner Form darauf hin, dass die gesetzlichen Grundlagen wenig stringent, in wichtigen Fragen unklar und zuweilen sogar lückenhaft sind. Sie konkretisieren dies aber nicht näher und bemerken, dass Vorschläge, um hier de lege ferenda Abhilfe zu schaffen, im Rahmen der zur Verfügung gestellten Ressourcen leider nicht möglich gewesen seien[198].

Den Ausführungen der externen Anwaltskanzlei zur allgemeinen rechtlichen Beurteilung der Informationsbeschaffung und -bearbeitung durch Cyber NDB ist im Rahmen der Administrativuntersuchung nichts beizufügen. Auch wenn in diesem wissenschaftlich wenig erforschten und von der Rechtsprechung kaum erfassten Bereich der Nachrichtendienstgesetzgebung verschiedene Fragen zwangsläufig offenbleiben müssen, ist ein Bedarf nach zusätzlicher Kommentierung nicht gegeben. In Ergänzung zu dem bereits vom NDB eingeholten Rechtsgutachten wurde aber versucht, das geltende Recht unter Berücksichtigung der konkreten Arbeitsweise und der praktischen Verfahrensabläufe bei Cyber NDB im Hinblick auf seine Praxistauglichkeit zu hinterfragen und zugleich Vorschläge für sich allenfalls aufdrängende Gesetzesrevisionen zu erarbeiten.

Die externe Anwaltskanzlei gelangte zum Ergebnis, dass Daten des Netzwerkverkehrs unter den Geltungsbereich des Fernmeldegeheimnisses fallen, bei Internet-Service-Providern nicht direkt angefordert und von diesen auch nicht freiwillig herausgegeben

197 Rechtsgutachten (Fn. 17), RZ 9-19, S. 6-10.
198 Rechtsgutachten (Fn. 17), RZ 472, S. 142.

werden können, und vom NDB allein unter Einhaltung der Bestimmungen über die genehmigungspflichtigen Beschaffungsmassnahmen rechtmässig hätten beschafft werden können[199]. Dieser Feststellung bleibt nichts anzufügen. Die aktuelle Regelung der genehmigungspflichtigen Beschaffungsmassnahmen unterscheidet nicht zwischen der unterschiedlichen Eingriffsintensität von laufender Überwachung und Randdatenerhebung, nimmt keine Differenzierung in Bezug auf die mit der Überwachung verfolgten Ziele vor und berücksichtigt auch die mit dem Eingriff für die Betroffenen verbundenen unterschiedlichen Konsequenzen nicht. Insofern erweist sich die rechtliche Beurteilung der externen Anwaltskanzlei als Konsequenz einer undifferenzierten Gesetzgebung.

Im Folgenden ist deshalb der Frage nachzugehen, inwieweit sich die Arbeitsmethoden von Strafverfolgungsbehörden und polizeilichen Präventionsbehörden unterscheiden. Dabei wird sich zeigen, dass nicht nur andere Informationsbedürfnisse bestehen, sondern insbesondere auch die Methoden der technischen Analyse von Netzwerkverkehrsdaten zur präventiven Erkennung oder Abwehr eines Cyberangriffs wenig Gemeinsamkeiten mit der Auswertung von Randdaten zur nachträglichen Abklärung einer bereits verübten Straftat haben.

9.2 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[200]. 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[201].

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[202].

Trotzdem orientiert sich die gesetzliche Regelung der genehmigungspflichtigen Beschaffungsmassnahmen – abgesehen von gewissen Modifikationen bei der Eingriffsschwelle (konkrete Bedrohung statt dringender Tatverdacht[203]), beim fehlenden Deliktskatalog[204], bei der Anordnungskompetenz (Antrag an das BVGer statt direkte Anordnung durch die

---

199 So schon BGE 141 IV 108 E. 5.1 und 5.2; BGer 6B_656/2015, E. 1.4.
200 Art. 26ff. NDG.
201 Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2164.
202 Botschaft zum Nachrichtendienstgesetz (Fn. 201), BBl 2014, 2143.
203 Art. 27 Abs. 1 NDG / Art. 269 Abs. 1 StPO.
204 Art. 269 Abs. 2 StPO.

Staatsanwaltschaft)[205] und dem politischen Freigabeprozess[206] – 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[207].

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[208]: Zunächst unterbreitet der NDB dem Bundesverwaltungsgericht einen Antrag, der u.a. die Angabe des spezifischen Ziels der Beschaffungsmassnahme und der Begründung ihrer Notwendigkeit enthält[209]. Die Präsidentin oder der Präsident der zuständigen Abteilung des Gerichts entscheidet innerhalb von fünf Arbeitstagen nach Erhalt des Antrags[210]. 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[211]. 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[212]. Einem erleichterten Genehmigungsverfahren unterstehen die Beschaffung von Informationen über Vorgänge im Ausland und die Kabelaufklärung[213].

9.3 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[214] und auf die frühzeitige Vereitelung einer Straftat und nicht auf die spätere Strafverfolgung zielen. Die Strafbehörden sanktionieren begangenes Unrecht; ihr Blick ist deshalb retrospektiv in die Vergangenheit

---

205 Art. 29 Abs. 1 NDG / Art. 269 Abs. 1 i.V.m. Art. 272 Abs. 1 StPO.

206 Art. 30 NDG.

207 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.

208 Art. 27 Abs. 2 NDG.

209 Art. 29 Abs. 1 NDG.

210 Art. 29 Abs. 2 NDG.

211 Art. 30 Abs. 1 NDG.

212 Art. 31 Abs. 1 NDG.

213 Art. 36 ff.; Art. 39 ff. NDG.

214 Nadine Zurkinden, Verbrechensbekämpfung durch Nachrichtendienste in der Schweiz, in: Marc Engelhart/Mehmet Arslan (Hrsg.), Verbrechensbekämpfung durch Nachrichtendienste, Freiburg 2021, S. 158.

gerichtet. Demgegenüber ist das Handeln der Präventionsbehörden, auch der Polizei, soweit sie nicht kriminalpolizeiliche Funktionen wahrnimmt, prospektiv auf die Zukunft gerichtet[215]. Während die Staatsanwaltschaft für die gleichmässige Durchsetzung des staatlichen Strafanspruchs verantwortlich ist[216] und erst einschreitet, wenn ein hinreichender Tatverdacht auf eine bereits verübte Straftat gegeben ist[217], hat der NDB die Aufgabe, Bedrohungen der inneren oder äusseren Sicherheit der Schweiz (frühzeitig) zu erkennen und (nach Möglichkeit) zu verhindern[218]. 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[219]. 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[220]. 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[221]. 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[222]. Damit kommt im Bereich der präventiven Tätigkeit der individuellen Interessenabwägung und der

---

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

216 Art. 16 Abs. 1 StPO.

217 Art. 309 Abs. 1 StPO.

218 Art. 6 Abs. 1 NDG.

219 BGE 128 I 327 E. 4.

220 BGE 143 I 310 E. 3.3.1.

221 Art 36 Abs. 1 Satz 3 BV.

222 BGE 136 I 87 E. 3.1.

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[223].

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[224]. Einer direkten Berufung auf die polizeiliche Generalklausel sind deshalb sehr enge Grenzen gesetzt[225]. 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[226] 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.

---

223 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

224 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.

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

226 In den Anhörungen war die Rede von [redacted] bis [redacted] Tagen.