Dr. Niklaus Oberholzer
Rechtsanwalt
Kesselhaldenstrasse 55
9016 St. Gallen

mail@niklausoberholzer.ch

Vorkommnisse im Ressort Cyber des Nachrichtendienstes des Bundes (NDB)

Bericht der Administrativuntersuchung

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

15. August 2022

Zusammenfassung der wesentlichen Erkenntnisse

1 Ressort Cyber NDB

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.

2 Ausgangslage und Auftrag zu einer Administrativuntersuchung

Nachdem der Nachrichtendienst Kenntnis von möglichen Unregelmässigkeiten erhalten hatte, erteilte der vormalige Direktor NDB im April 2021 der Abteilung Sicherheit NDB den Auftrag zur Durchführung einer internen Untersuchung. Diese führte im Dezember 2021 zur Erkenntnis, dass der Schweizerische Nachrichtendienst im Rahmen der Informationsbeschaffung zu möglichen Cyberangriffen in den Jahren 2015 bis 2020 auch Informationen über den Netzwerkverkehr potenzieller Angreifer beschafft und bearbeitet hatte. Derartige Informationen zählen zu den sogenannten Randdaten des Fernmeldeverkehrs und stehen unter dem Schutz des Fernmeldegeheimnisses. Sie können rechtmässig nur unter Einhaltung der Bestimmungen des Nachrichtendienstgesetzes (NDG) mittels genehmigungspflichtiger Beschaffungsmassnahmen erhoben werden. Die dazu erforderlichen Genehmigungen durch das Bundesverwaltungsgericht und die politische Freigabe durch die Vorsteherin VBS wurden vom NDB jedoch nicht eingeholt.

Das VBS informierte unverzüglich die Geschäftsprüfungsdelegation der Eidgenössischen Räte (GPDel) über die Erkenntnisse der NDB-internen Untersuchung und beauftragte im Januar 2022 Dr. Niklaus Oberholzer, Rechtsanwalt und ehemaliger Richter am Schweizerischen Bundesgericht, mit der Durchführung einer Administrativuntersuchung. Der Untersuchungsbeauftragte hatte Zugang zu allen Akten des NDB, die im Zusammenhang mit dem Untersuchungsgegenstand standen, und hörte im Verlauf der Untersuchung insgesamt 13 Mitarbeitende des NDB an. Er erstattete dem Departement seinen Schlussbericht im August 2022.

3 Berichterstattung zu den Ergebnissen der Administrativuntersuchung

Die Administrativuntersuchung ist ein spezielles Verfahren im Rahmen der ständigen und systematischen Aufsicht des Bundesrates über die Bundesverwaltung. Sie dient in erster Linie der Klärung eines Sachverhalts und soll den Auftraggeber auf systemische Mängel hinweisen, die im öffentlichen Interesse gegebenenfalls ein Einschreiten von Amtes wegen erfordern könnten. Eine Publikation ist gesetzlich nicht vorgesehen.

Der Schlussbericht der Administrativuntersuchung setzt sich auf rund 90 Seiten detailliert mit dem Aufbau, den Strukturen, der internen Organisation und den Arbeitsmethoden des Nachrichtendienstes auseinander. Der Bericht enthält nicht nur Informationen, die aus geheim klassifizierten Quellen stammen. Er beschreibt auch die spezifischen Informationsbedürfnisse sowie die konkreten Informationsbeschaffungs- und -bearbeitungsmethoden des Nachrichtendienstes bei der Abwehr von international koordinierten

Cyberangriffen und enthält darüber hinaus Hinweise zur Zusammenarbeit mit privaten Personen und Organisationen sowie nationalen und internationalen Partnerdiensten.

Das VBS hat sich deshalb entschieden, den Schlussbericht der Administrativuntersuchung als geheim zu klassifizieren, soweit dieser sich zu geheimhaltungsbedürftigen Tatsachen der nachrichtendienstlichen Organisation oder Methoden äussert. Den berechtigten Informationsbedürfnissen der Öffentlichkeit soll mit der vorliegenden Zusammenfassung der wesentlichen Erkenntnisse Rechnung getragen werden.

Der Schlussbericht beschränkt sich nicht nur auf Tatsachenfeststellungen, sondern enthält auch rechtliche Analysen und Empfehlungen im Hinblick auf das weitere Vorgehen. Diese Ausführungen werden in einem separaten Bericht im Sinne eines Auszugs aus dem Schlussbericht weitgehend integral veröffentlicht. Dies betrifft im Wesentlichen die Empfehlungen zu einer organisatorischen Neuausrichtung von Cyber NDB und zu einer Revision der Bestimmungen des Nachrichtendienstgesetzes über die genehmigungspflichtigen Beschaffungsmassnahmen sowie die rechtliche Analyse einer allfälligen strafrechtlichen Relevanz der unrechtmässigen Datenbeschaffung und -bearbeitung durch den Nachrichtendienst.

4 Informationsbeschaffung ohne Einhaltung der gesetzlichen Bestimmungen

Die Administrativuntersuchung hat die bereits in der internen Untersuchung gewonnenen Erkenntnisse im Wesentlichen bestätigt. Das Ressort Cyber NDB hat zur Abwehr möglicher Cyberangriffe unter anderem auch Informationen beschafft, die dem Fernmeldegeheimnis unterstehen und deshalb nur unter Einhaltung der im Nachrichtendienstgesetz geregelten strengen Voraussetzungen (gerichtliche Genehmigung und politische Freigabe) hätten erlangt werden dürfen. Genauere Angaben über das tatsächliche Ausmass und die konkreten Modalitäten der einzelnen Aktionen konnte auch in der Administrativuntersuchung nicht erhoben werden, da die Abläufe im Ressort Cyber im fraglichen Zeitraum nicht systematisch erfasst und dokumentiert wurden. Eine nachträgliche Rekonstruktion der Vorgänge im Einzelnen erweist sich deshalb als weitgehend unmöglich. Dies ändert jedoch nichts an der Feststellung, dass Cyber NDB während Jahren Informationen ohne Einhaltung der gesetzlichen Bestimmungen und damit unrechtmässig Daten beschafft und bearbeitet hat.

Dabei ist jedoch zu relativieren, dass es sich bei den auf diese Weise beschafften Informationen nicht um besonders schützenswerte Personendaten, sondern um Randdaten des Netzwerkverkehrs gehandelt hatte, die primär einer rein technischen Analyse unterzogen und nicht im Hinblick auf personenbezogene Elemente analysiert wurden. Der Nachrichtendienst gelangte ohne Anwendung von Zwangsmassnahmen in den Besitz dieser Informationen; diese wurden ihm auf blosse Anfrage hin auf freiwilliger Basis herausgegeben. Anhaltspunkte, dass dadurch individuelle Personen einen Nachteil tatsächlicher oder rechtlicher Art erlitten haben könnten, liegen nicht vor.

Die Administrativuntersuchung hat ergeben, dass der Nachrichtendienst nicht vorsätzlich gegen Bestimmungen des Nachrichtendienstgesetzes verstossen hat, sondern die Rechtslage verkannt und die fernmelderechtliche Dimension der Datenbeschaffung und -bearbeitung nicht erkannt hatte. Die Mitarbeitenden waren offenbar davon ausgegangen, dass der Nachrichtendienst (gestützt auf Art. 23 NDG) berechtigt ist, von jeder Person Meldungen entgegenzunehmen, solange die Auskunft freiwillig erfolgt. Dies mag

allenfalls für die Zeit bis zum Inkrafttreten des Nachrichtendienstgesetzes (1. September 2017) noch nachvollziehbar sein; bis zu jenem Zeitpunkt verfügte der NDB über keine Befugnisse zur geheimen Überwachung elektronischer Kommunikationsvorgänge. Spätestens die Diskussionen um die Einführung der genehmigungspflichtigen Beschaffungsmassnahmen im neuen NDG hätten jedoch zwingend zum Anlass genommen werden müssen, die Beschaffungsabläufe innerhalb des Ressorts Cyber NDB einer genaueren Überprüfung zu unterziehen und im Hinblick auf deren Rechtmässigkeit zu überprüfen.

Unbestritten ist, dass die Arbeit von Cyber NDB in den Jahren 2015 bis 2020 sehr erfolgreich war. Dem NDB gelang es nicht nur, gegen schweizerische Interessen gerichtete Cyberangriffe zu erkennen und abzuwehren. Er verschaffte sich auch bei ausländischen Partnerdiensten hohes Ansehen, indem er ihnen Informationen zur Verfügung stellen konnte, welche ihrerseits für deren Erkennung und Abwehr von Cyberangriffen gegen ausländische Interessen von grosser Bedeutung waren. Dies darf aber nicht darüber hinwegtäuschen, dass der Erfolg unter anderem auch auf unrechtmässigen Beschaffungsmethoden von Cyber NDB beruhte und die internen Kontroll- und Aufsichtsmassnahmen versagt hatten.

5 Systemische Ursachen für das Eigenleben von Cyber NDB

Im Zentrum der Administrativuntersuchung stand die Frage, wie es soweit kommen konnte, dass ein Ressort des Nachrichtendienstes ein weitgehendes Eigenleben entwickelte und ohne Einhaltung der gesetzlichen Bestimmungen während Jahren unrechtmässig Informationen beschafft und ausgewertet hatte. Wie sich zeigte, waren dafür verschiedene Umstände von Belang.

5.1 Hoher Erwartungsdruck

Die Erwartungen an das im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken neu geschaffene Ressort Cyber NDB waren hoch. Dem Nachrichtendienst wurde vom Bundesrat zum Ziel gesetzt, mittels einer systematischen Informationsbeschaffung und -auswertung neue Angriffsmuster möglichst frühzeitig zu entdecken und die Urheberschaft von erfolgten Angriffen möglichst genau zuzuordnen.

Damit der NDB diese Zielvorgaben erreichen kann, müssen ihm auch die nötigen Mittel zur Verfügung gestellt werden. Wie die vorliegende Untersuchung zeigt, scheint diesem Aspekt zu wenig Bedeutung zugemessen worden zu sein. Kann Cyber NDB die zur Entdeckung eine Cyberangriffs erforderlichen Informationen (insbesondere Randdaten des Fernmeldeverkehrs) rechtmässig nur auf dem Weg einer genehmigungspflichtigen Beschaffungsmassnahme erlangen, verstreichen Tage, wenn nicht gar Wochen, bevor das Ressort mit einer systematischen Auswertung der Daten und damit mit einer Analyse der Angriffsmuster beginnen kann. Die von der Politik verlangte Früherkennung dürfte damit illusorisch werden. Insofern mag es zwar nicht gerechtfertigt, aber doch nachvollziehbar sein, dass Cyber NDB in der vermeintlichen Überzeugung, Art. 23 NDB biete für eine freiwillige Datenherausgabe eine hinreichende Grundlage, eigenständig neue Mittel und Methoden zur Informationsbeschaffung gesucht hat, um die ihm zugewiesene Aufgabe erfüllen zu können.

5.2 Ungenügende Organisation und Einbindung

Cyber NDB wurde 2014 unter hohem Zeit- und Erwartungsdruck aufgebaut. Vertiefte Abklärungen über die Einordnung, die Unterstellung und die Arbeitsweise des neu geschaffenen Ressorts 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 erfüllen kann. 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. Unberücksichtigt blieb die Tatsache, dass es sich bei Cyberangriffen nicht um ein klassisches nachrichtendienstliches Themenfeld (wie etwa Spionage, Terrorismus oder gewalttätigen Extremismus), sondern um eine, vom angestrebten Ziel weitgehend unabhängige, spezifische Angriffsform handelt.

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. Für weitere Einzelheiten kann auf den separat veröffentlichten Auszug aus dem Schlussbericht der Administrativuntersuchung verwiesen werden.

5.3 Fehlende Kontrolle 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 Steuerung, Beschaffung und Auswertung 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. 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 die Mitwirkung des für geheime Beschaffungsmassnahmen zuständigen Direktionsbereichs Beschaffung (NDBB) zurückgriff. Nachfragen zur konkreten Ausgestaltung der Arbeitsmethoden von Cyber NDB erfolgten trotzdem nicht. Unverständlich erscheint heute, dass die Geschäftsleitung und insbesondere der zuständige Direktionsbereichsleiter (NDBI) bis September 2020 die Unrechtmässigkeit der während Jahren geläufigen Praxis nicht erkannten.

5.4 Gesamthafte Verantwortung des Nachrichtendienstes

Insofern fällt es schwer, die Verantwortung für die Vorkommnisse im Ressort Cyber NDB einer einzigen Person zuzuordnen. 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 Verwaltung von Daten, aber nichts mit deren Beschaffung und Auswertung 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.

6 Cyber NDB und genehmigungspflichtige Beschaffungsmassnahmen

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 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. Auch diesbezüglich kann auf den separat publizierten Auszug aus dem Schlussbericht verwiesen werden.

7 Allfällige strafrechtliche Relevanz der Vorkommnisse im Ressort Cyber NDB

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.