Mai 2020 · Kilian Vieth & Thorsten Wetzling

Datenbasierte Nachrichtendienst-kontrolle

Agenda für mehr Wirksamkeit

Stiftung
Neue
Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Zusammenfassung

Überwachungstechnologien entwickeln sich rasant. Nachrichtendienste auf der ganzen Welt treiben diese facettenreiche Entwicklung voran. In vielen Ländern besteht die Gefahr, dass Kontrollmechanismen mit diesem Trend nicht Schritt halten können. Moderne Datenanalysemethoden bergen zahlreiche Risiken in Bezug auf Datenmissbrauch und die Umgehung rechtlicher Standards. Hinzu kommt ein Mangel an leistungsfähigen Werkzeugen, Ressourcen und technischem Fachwissen, der eine wirksame Kontrolle noch zusätzlich untergräbt. Deswegen sind Aufsichtsgremien jetzt gefordert, effektivere Kontrollinstrumente einzufordern, zu entwickeln und einzusetzen. Die wachsenden Datenmengen, die im Nachrichtendienstbereich erfasst und verarbeitet werden, werden von den bestehenden rechtlichen Schutzmaßnahmen nicht adäquat berücksichtigt und überfordern die Kontrolle in der Praxis.

Einige Aufsichtsgremien in Europa haben im Laufe der letzten Jahre einen deutlich verbesserten Zugang zu den IT-Systemen und Datenbanken der Nachrichtendienste erhalten. Diese Studie nimmt diese Entwicklung zum Anlass, um mit Blick auf bekannte Herausforderungen bei verschiedenen Kontrollvorgängen über neue Lösungen nachzudenken. Wie könnte ein besserer Zugang zu den informationstechnischen Systemen noch sinnvoller als bisher genutzt werden? In dieser Studie schlagen wir sieben Ansätze für eine datenbasierte Kontrolle von nachrichtendienstlichen Tätigkeiten vor, die aus unserer Sicht Teil einer Reformagenda werden sollten. Einige der von uns vorgeschlagenen Instrumente werden bereits von Pionieren der nachrichtendienstlichen Aufsicht genutzt, während andere Praktiken sich in anderen Sektoren, wie der Finanzaufsicht und der IT-Sicherheit, bewährt haben.

Die folgende Tabelle fasst Herausforderungen für die nachrichtendienstliche Aufsicht zusammen (linke Spalte), und stellt ihnen Innovationen gegenüber (rechte Spalte), mit denen diese Herausforderungen wirksam begegnet werden könnte.

Herausforderungen ↔ Lösungsvorschläge	
Intransparente Filtertechnologie: Mitunter sieht das nationale Nachrichtendienstrecht strengere Datenschutzregeln für bestimmte Personengruppen vor. Um diese zu gewährleisten, werden die erhobenen Daten mittels umfangreicher technischer Verfahren gefiltert und gelöscht. Derartige 'Datenreduktion' ist für die Einhaltung der gesetzlichen Vorgaben entscheidend. Diese Filter werden jedoch selten einer unabhängigen Überprüfung auf Genauigkeit und Zuverlässigkeit unterzogen.	**(A) Unabhängige Überprüfung der Datenfilter:** Ein direkter Zugriff auf die gespeicherten Daten der Dienste ermöglicht es den Aufsichtsbehörden, die Genauigkeit der Datenfilterung zu testen. Dabei werden die Datenbanken mit Suchprogrammen nach Identifikatoren (z. B. Telefonnummern) durchsucht, die in den gefilterten Daten nicht enthalten sein sollten.
Missbräuchliche Datenbankabfragen: Immer öfter werden Fälle von illegaler und unangemessener Datennutzung öffentlich. Zum Beispiel wenn persönliche Daten ohne ausreichenden sachlichen Grund abgerufen werden und kein ausreichender Schutz gegen solchen Missbrauch vorhanden ist.	**(B1) Mustererkennung:** Nutzung von Software zur automatischen Analyse und Visualisierung der Nutzung von Datenbanken. Die Aufsichtsbehörden können damit die Protokolldateien auf potenziell verdächtige Muster prüfen.
Unzureichend kontrollierte nachrichtendienstliche Zusammenarbeit: Den meisten Aufsichtsbehörden fehlen Mechanismen, um zu prüfen, ob und wie die nationalen Nachrichtendienste Daten an ausländische Stellen weitergeben. Dementsprechend fehlt eine wirksame Kontrolle über die Verwendung der geteilten Daten.	**(B2) Warnmeldungen bei riskantem Datenaustausch:** Automatisierte Benachrichtigungen informieren Aufsichtsgremien über kennzeichnungspflichtige Datenweitergabe und ermöglichen gezielte Inspektionen im Nachgang.
Speicherfristen durchsetzen: Wenn Analyst:innen oder Systemadministrator:innen Daten aus Quellen zusammenführen, für die unterschiedliche Speicherfristen gelten, können die Daten unter Umständen auch nach Ablauf der Fristen in Datenbanken gespeichert bleiben und verwendet werden.	**(B3) Lösch-Statistiken:** Löschvorgänge werden in gut strukturierten Protokolldateien aufgezeichnet, so dass Aufsichtsorgane Unstimmigkeiten in den statistischen Mustern erkennen und aufspüren können.
Unwissen über den praktischen Umgang mit Anordnungen: Die Aufsichtsbehörden haben Mühe, mit der großen Zahl von Anträgen auf Überwachungsmaßnahmen Schritt zu halten. Es fehlt ihnen die Möglichkeit, den Umgang der Nachrichtendienste mit den genehmigten Datenerhebungen in der Praxis nachzuverfolgen. Diese Kontrolle wäre allerdings wichtig, da auch mit genehmigten Überwachungsdaten unzulässige Grundrechtseingriffe einhergehen können.	**(B4) Nachverfolgung von Anordnungen:** Die digitale Dokumentation von Überwachungsanordnungen ermöglicht es den genehmigenden Gremien die Notwendigkeit neuer Anordnungen im Lichte der abgeschlossenen und bereits laufenden Überwachungsmaßnahmen zu beurteilen. Zudem können unzureichend begründete Anträge bzw. unzulässige Wiederholungen in den Antragsbegründungen aufgespürt werden.

Knappe Ressourcen: Die Aufsichtsbehörden setzen ihre begrenzten Ressourcen noch zu unsystematisch und ineffektiv ein.	**(C) Risikoabschätzung:** Zur besseren Planung und Priorisierung ihrer Kontrolltätigkeiten führen die Aufsichtsbehörden eine umfassende Risikobewertung durch. Auf Basis von Risiko-Punkten, die für die Missbrauchsgefahr einzelner Datenbanken vergeben werden, kann eine Priorisierung von Kontrollaufgaben und Inspektionen vorgenommen werden.
Undurchsichtige Interaktion der Nachrichtendienste mit privaten Akteuren: Um Rechtsverstöße zu vermeiden, ist es besonders wichtig unzulässige Datenerfassungen an der Datenquelle zu vermeiden. Die Aufsichtsbehörden wissen aber in der Praxis zu wenig darüber, wie die Betreiber von Telekommunikations- und Internetdiensten in der Praxis mit den Sicherheitsbehörden zusammenarbeiten, um etwaige Fehler aufspüren zu können.	**(D) Dialog zwischen Kontrollgremien und Dienstanbietern:** Ein systematischer Austausch zwischen Betreibern von Telekommunikationsdiensten und Aufsichtsgremien ermöglicht es den Prüfer:innen die Implementierung der Datenerhebung genauer nachzuverfolgen. In Verbindung mit einer Fehler-Meldepflicht auf Seiten der Provider kann so die Einhaltung gesetzlicher Vorgaben an der Schnittstelle zu den privaten Betreibern gefördert werden.

Wir laden politische Entscheidungsträger:innen in Parlamenten und Regierungen, sowie Vertreter:innen von Nachrichtendiensten und Aufsichtsgremien ein, die in dieser Studie skizzierten Ideen zu diskutieren und kontextspezifische Strategien für eine datenbasierte Nachrichtendienstaufsicht zu entwickeln. Für eine erfolgreiche Umsetzung der vorgeschlagenen Instrumente, raten wir den Aufsichtsbehörden, sie nicht als Ersatz für etablierte Kontrollmechanismen zu betrachten. Sie sind vielmehr als notwendige Ergänzung zu den bestehenden Instrumenten und Inspektionsverfahren zu verstehen.

Eine Verbesserung der Nachrichtendienstaufsicht wird mehr erfordern als eine Anpassung bestehender Gesetze. Zu lange wurde versucht, technischen Herausforderungen allein mit Veränderungen des Nachrichtendienstrechts zu begegnen. Diese Studie zeigt, dass gesetzliche Vorgaben nicht wirksam durchgesetzt werden können, wenn nicht auch praktische Veränderungen beim Kontrollverfahren ergriffen werden. Es bedarf daher einer gemeinsamen Anstrengung, hin zu einer besseren Kontrollpraxis.

Vorbemerkung

Diese Studie wurde von der Deutschen Forschungsgemeinschaft (DFG-Projektnummer 396819157) und dem Information Program der Open Society Foundations (Grant OR2018-45772) gefördert. Die Autoren danken den Mitgliedern des Europäischen Netzwerk Nachrichtendienstkontrolle (European Intelligence Oversight Network – EION) für konstruktives Feedback. Zudem bedanken wir uns bei Giles Herdale, Eric Kind, Jan-Peter Kleinhans, Jörg Pohle und Félix Tréguer für wertvolle Kommentare. Die Autoren sind allein verantwortlich für den Inhalt. Diese Studie wurde auf Englisch verfasst und von den Autoren ins Deutsche übersetzt.

Inhaltsverzeichnis

Vorwort

Dass Kontrollverfahren und -behörden in den meisten Sektoren in ihrem Ansatz eher konservativ sind, ist nicht verwunderlich. Dies hat viel mit Regulierungsprozessen im Allgemeinen zu tun, sei es in der Regierung oder in anderen Bereichen.

Die vorliegende, beeindruckende Studie, die sich aus dem Europäischen Netzwerk Nachrichtendienstkontrolle speist, wirft zwei zentrale Fragen auf: Erstens, wie kann sich die Aufsicht anpassen, um mit der rasanten technologischen Entwicklung der zu kontrollierenden Überwachungsmethoden Schritt zu halten? Und zweitens, welche Möglichkeiten gibt es, die neuesten Werkzeuge und Techniken im Kontrollprozess selbst einzusetzen? Beide Fragen weisen auf wichtige neue Bereiche der interdisziplinären Forschung hin; es geht nicht nur um die Technologie selbst, sondern auch um die rechtlichen und ethischen Rahmenbedingungen. Es ist sehr wichtig, dass die Sicherheitsbehörden, aber auch die Aufsichtsorgane und -mechanismen, nachweislich mit öffentlicher und demokratischer Zustimmung innerhalb der Rechtsstaatlichkeit arbeiten.

Diese Studie ist reich an Hintergrundinformationen über die aktuellen Möglichkeiten, sowie über spezifische und allgemeinere Herausforderungen für die Zukunft. Es stellt sich, wie die Autoren herausarbeiten, nicht die Frage ob, sondern wie, leistungsfähigere datengesteuerte Kontrollinstrumente implementiert werden können. Sie betonen die Notwendigkeit, dass die Aufsichtsbehörden technische Beratung aus anderen Sektoren erhalten müssen, was im Vereinigten Königreich zu einem kleinen Teil vom gesetzlich verankerten Technologie-Beirat der Kontrollbehörde IPCO geleistet wird. Sie haben auch Recht damit, dass es keine Einheitslösung gibt und dass keiner von uns dieses Problem allein lösen kann.

Diese fundierte Studie bietet reichlich Anregungen für sorgfältige Reflektion und ist sowohl Handlungsgrundlage als auch Denkanstoß. Ich freue mich auf die spannenden Entwicklungen, die sie in diesem wichtigen Bereich auslösen wird.

Sir Bernard Silverman FRS
Emeritierter Professor an den Universitäten Bristol und Oxford Vorsitzender, Technologie-Beirat (Technology Advisory Panel), Investigatory Powers Commissioner's Office (IPCO)
Vereinigtes Königreich

1. Einführung: Warum Kontrollinnovationen nötig sind

> *„Entweder wir werden die neuen Techniken für uns nutzen oder wir riskieren, dass unsere Arbeit irrelevant wird.“*[1]
> (Paul Killworth, stellvertretender Direktor für Strategie und Planung, GCHQ)

> *„Ist die Exekutivbefugnis in einem Gesetz weit gefasst und die Aufsicht nur darauf beschränkt zu überprüfen, ob eine Behörde innerhalb ihres gesetzlichen Auftrags bleibt, dann ist die Aufsicht von begrenztem Nutzen.“*[2]
> (Venedig-Kommission des Europarates, 2015)

High-Tech-Nachrichtendienst trifft auf Low-Tech-Kontrolle

Nachrichtendienste sind dafür bekannt sich dem technologischen Wandel schnell anzupassen und ihn selbst aktiv voranzutreiben. Die schiere Menge der zur Verfügung stehenden Daten und die steigenden Übertragungs- und Rechenkapazitäten treiben die Entwicklung von Überwachungstechnologie voran. Sicherheitsbehörden in ganz Europa bringen neue Methoden zum Einsatz, etwa zur Erfassung und Auswertung von biometrischen Daten oder für staatliches Hacking. Neue Soft- und Hardware, so hofft man, bieten auch eine geeignete Antwort auf die Herausforderung der Informationsüberflutung.[3]

Im Gegensatz dazu sind die meisten Aufsichtsbehörden eher langsam und häufig auch zurückhaltend darin, sich an den technologischen Fortschritt anzupassen und ihn für ihre Ziele zu nutzen. Kontrollmechanismen wurden von der Forschung und Entwicklung im Sicherheitssektor bislang kaum berücksichtigt und die meisten Aufsichtsbehörden haben es versäumt, auf ihre Schwierigkeiten und technologischen Defizite aufmerksam zu machen. Das ist auch eine Erklärung dafür, dass Nachrichtendienste regelmäßig mit erweiterten Überwachungsbefugnissen ausgestattet werden[4] und auf technologische

1 Babuta, „A New Generation of Intelligence: National Security and Surveillance in the Age of AI,“ 19. Februar 2019, https://rusi.org/commentary/new-generation-intelligence-national-security-and-surveillance-age-ai (eigene Übersetzung).

2 Venedig-Kommission, „Report on the democratic oversight of signals intelligence agencies“, Abschnitt 93., März 2015, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e (eigene Übersetzung).

3 Vgl. Diskussions-Panel über Künstliche Intelligenz im Nachrichtendienstwesen auf about:intel.eu, insb. der Beitrag von Jo Cavan und Paul Killworth (GCHQ) dort, https://aboutintel.eu/artificial-intelligence/.

4 Finnland verabschiedete 2019 ein neues Nachrichtendienstgesetz, während in Österreich, Norwegen, Frankreich und Deutschland Reformen der Gesetzgebung im Gange sind, die den nationalen Sicherheits- und Nachrichtendiensten zusätzliche Überwachungsbefugnisse verleihen.

Innovationen zurückgreifen können, während die Aufsichtsbehörden dagegen häufig ohne zeitgemäße und datenbasierte Instrumente arbeiten.

Die Kosten der Trägheit

Bei den Investitionen in neue Technologien hinkt die Aufsicht dem Rest des Sicherheitssektors weit hinterher. Aktuell geben die meisten europäischen Länder weniger als ein Prozent der Mittel, die sie in ihre Nachrichtendienste investieren, für den Ausbau der Kontrolle aus.[5] Angesichts der rasanten Entwicklung von Überwachungstechnologien kann dieser Sparkurs bei den Ausgaben für die Aufsicht unsere Demokratien teuer zu stehen kommen. Die Legitimität der Exekutivgewalt hängt von einer effektiven, modernen und umfassenden Nachrichtendienstaufsicht ab. Sind Aufsichtsbehörden nicht in der Lage, die Praktiken der Nachrichtendienste vollständig zu überprüfen, führt dies zwangsläufig zu Lücken in der demokratischen Rechenschaftspflicht. Dies wiederum bietet Möglichkeiten für Fehlverhalten und Missbrauch, was angesichts der Intensität und Eingriffstiefe moderner Überwachungsbefugnisse das Vertrauen der Öffentlichkeit in die Gewährleistung von Grund- und Menschenrechten untergräbt.

Eine Reihe von Aufsichtsbehörden in Europa haben kürzlich Budgeterhöhungen erhalten und Mitarbeiter:innen mit technischer Expertise eingestellt. Das ist gut so. Leider haben aber noch immer zu wenige Aufsichtsbehörden damit begonnen, neue Kontrollinstrumente analog zum Innovationstempo der Nachrichtendienste auszubauen und zu nutzen. Stattdessen bleiben viele Kont-

5 Eine genaue Betrachtung des Budget-Verhältnisses zwischen Diensten und Kontrollgremien ist schwierig, da nicht alle Haushaltszahlen öffentlich verfügbar sind. Darüber hinaus müssen die veröffentlichten Zahlen mit Vorsicht behandelt werden, da sie möglicherweise nicht die Gesamtheit nachrichtendienstlicher Tätigkeiten widerspiegeln. Beispielsweise gehen auch verschiedene Abteilungen der Bundeswehr (zum Beispiel das Kommando Cyber und Informationsraum (KdoCIR) und das Kommando Strategische Aufklärung, inklusive der vier Bataillone der elektronischen Kampfführung (EloKa)) nachrichtendienstlichen Tätigkeiten nach, ohne dass die Bundesregierung sich dafür in ähnlicher Form im Rahmen der parlamentarischen und quasi-juristischen Kontrolle zu verantworten hat. Man denke auch an den veröffentlichten Haushalt für die Nachrichtendienste des Bundes im Jahr 2018: rund 1,4 Milliarden Euro. Diese Summe beinhaltet noch nicht weitere 1,4 Milliarden Euro, die für die neue BND-Zentrale in Berlin-Mitte an Steuergeldern ausgegeben wurde. Damit die Ausgaben für die Aufsicht ein Prozent dieses jährlichen Nachrichtendienst-Budgets erreichen, müssten die zusammengefassten Jahresbudgets, die der fragmentierten deutschen Nachrichtendienstaufsicht zur Verfügung stehen (d.h. Parlamentarisches Kontrollgremium, G10-Kommission, Unabhängiges Gremium, Vertrauensgremium, spezielle Referate PK1-PK4 innerhalb der Bundestagsverwaltung, sowie Referate beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sowie beim Bundesrechnungshof), zusammen mindestens 14 Millionen Euro betragen. Auch hier ist es schwierig, dies zu berechnen (aufgrund von Faktoren, wie den Personalkosten für die Mitglieder des Bundestags oder den Personalkosten innerhalb der Exekutive, die zur Beantwortung von Anfragen der Kontrollgremien erforderlich sind). Das Jahresbudget für das PKGr und die G10-Kommission belief sich 2018 auf rund 3 Millionen Euro.

rollgremien weiter abhängig von den Informationen, die sie von den Diensten bekommen. Sie arbeiten teilweise unter strikten Zugangsbeschränkungen, die sie daran hindern, komplexere und eigenständige Prüfungen durchzuführen.[6]

Zusammenfassung: Warum wir Innovationen in der Aufsicht brauchen

Legitimität	Neue Sicherheitsmaßnahmen erfordern neue Formen der Aufsicht. Wenn Aufsichtsbehörden nicht für die Überprüfung der Überwachungsmethoden des 21. Jahrhunderts ausgerüstet werden, so steht die Legitimität demokratischer Nachrichtendienstführung in Frage.
Legalität	Gerichte haben wiederholt eingefordert, dass rechtliche Regelungen besser eingehalten und die Kontrollvorgaben mit Leben gefüllt werden müssen. Im *Big Brother Watch* Urteil vom September 2018 hat der EGMR z. B. festgehalten, dass „erstens die Aufsicht über den gesamten Auswertungsprozess fehlt [...] und zweitens keine Schutzmechanismen für die Auswahl der zu prüfenden zugehörigen Kommunikationsdaten bestehen".[7] Das heißt, dass die massenhafte Kommunikationsüberwachung von der Erhebung bis zur Löschung der Daten einer wirksamen Ende-zu-Ende-Aufsicht unterstellt werden muss.[8]
Wirksamkeit	Die Digitalisierung erzeugt eine Informationsflut (durch größere Datenmengen, immer mehr Datenquellen, kostengünstige Vervielfältigung von Daten), die es zu steuern gilt. Innovative Kontrollinstrumente und -technologien ermöglichen eine proaktivere Aufsicht, machen die Berichterstattung effizienter und verbessern die Erklärbarkeit von Entscheidungen der Kontrollgremien.

Keine neue Forderung

Da moderne nachrichtendienstliche Tätigkeit datenbasiert ist, sollte dies auch für ihre Kontrolle gelten. Es ist an der Zeit, dass denjenigen, denen wir die Aufgabe anvertrauen, dafür zu sorgen, dass die Nachrichtendienste den Rechtsstaat und unsere Grundrechte respektieren, auch die entsprechenden Instrumente gegeben werden. Doch das ist leichter gesagt als getan.

Bei einigen europäischen Aufsichtsbehörden wächst das Bewusstsein, dass ihre aktuelle Ausstattung modernisiert werden muss. Die niederländische

6 Zur Vertiefung der Faktoren, die eine wirksame Aufsicht über verschiedene Rechtsordnungen hinweg behindern, siehe Goldman und Rascoff, „Global Intelligence Oversight: Governing Security in the Twenty-First Century," 2016; und Wetzling, „Options for more effective intelligence supervision," 2017, https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

7 Europäischer Gerichtshof für Menschenrechte, „Case of Big Brother Watch and Others v. The United Kingdom", 13. September 2018, http://hudoc.echr.coe.int/eng?i=001-186048 (eigene Übersetzung).

8 Smith, „What will be in Investigatory Powers Act Version 1.2?", 30. Oktober 2018, https://www.cyberleagle.com/2018/10/what-will-be-in-investigatory-powers.html.

Aufsichtsbehörde CTIVD hat beispielsweise das Projekt „Oversight 3.0“ ins Leben gerufen, in dem sie sich unter anderem den Herausforderungen der Datenlöschung widmet und nach möglichen Innovationen für die Aufsicht sucht. Ebenfalls ist hervorzuheben, dass eine Reihe europäischer Aufsichtsbehörden den internationalen Austausch auf bilateraler und multilateraler Ebene vertieft haben.

Kooperation und Innovation im Bereich der Aufsicht wurden somit als entscheidende Themen anerkannt. Es ist höchste Zeit genau zu bestimmen, was technische Instrumente leisten können, um die aktuellen Herausforderungen der Nachrichtendienstkontrolle zu bewältigen. Andernfalls wird die allgegenwärtige Forderung nach wirksameren Aufsichtsinstrumenten vage und ergebnislos bleiben. Wir nähern uns der Thematik datenbasierter Aufsicht, indem wir einzelne, leichter zugängliche Teilaspekte betrachten.

Ziel dieser Studie

Ganz im Sinne einer Machbarkeitsstudie werden im Folgenden eine Reihe von Instrumenten, die eine datenbasierte Nachrichtendienstkontrolle ermöglichen, vorgestellt und erörtert. Sie können den Aufsichtsbehörden helfen, einen besseren Überblick über das Ausmaß staatlicher Überwachung zu behalten und wirksame Kontrollmechanismen zu gewährleisten. Wir sind uns bewusst, dass die institutionelle Gestaltung der Aufsicht in verschiedenen Ländern jeweils eigenen Pfadabhängigkeiten unterliegt und besondere Anforderungen erfüllen muss. Trotz dieser Faktoren stellt sich nicht die Frage *ob*, sondern *wie* leistungsfähigere datenbasierte Aufsichtsinstrumente eingesetzt werden können. Diese Herausforderung können die Aufsichtsbehörden nicht allein lösen – sie brauchen technische Beratung, etwa aus anderen Politikbereichen oder der Wirtschaft. Und da diese Überlegungen Auswirkungen auf die Beziehungen zwischen Aufsichtsbehörden und Diensten haben, müssen die Nachrichtendienste und ihre Fachaufsicht ebenfalls in diese Diskussion einbezogen werden.

Als zivilgesellschaftliche Beobachter möchten wir dokumentieren, welche datenbasierte Aufsichtsmaßnahmen möglich sind und welche bereits erfolgreich umgesetzt werden, um den Verantwortlichen eine bessere argumentative Grundlage zu geben.

Angesichts der sehr unterschiedlichen Zusammensetzung von parlamentarischen Ausschüssen, justizieller Kontrolle, Expertengremien und Datenschutzbehörden kann es keine Einheitslösung geben. Wir hoffen jedoch, dass sich interessierte Leser:innen aus verschiedenen Bereichen kreativ mit unseren Vorschlägen beschäftigen.

Unser methodisches Vorgehen

Im Rahmen unserer Suche nach Ideen und geeigneten Anwendungen zur Bewältigung häufiger Kontrolldefizite, haben wir sowohl Literatur ausgewertet, als auch eine Reihe von Interviews mit Praktiker:innen aus den Bereichen datenbasierter Polizeiarbeit, Finanzaufsicht und Datenschutz durchgeführt. Viele Ideen in diesem Papier bauen auf dem direkten Zugang zu den IT-Systemen und Datenbanken der Dienste auf, über die eine kleine Gruppe europäischer Aufsichtsbehörden bis dato verfügt. Die Ideen für datenbasierte Kontrollinstrumente wurden in einem Workshop des European Intelligence Oversight Network im Mai 2019 diskutiert und weiterentwickelt.[9]

Gliederung

Im folgenden Kapitel werden sieben Ideen für eine Weiterentwicklung der Nachrichtendienstaufsicht vorgestellt und erläutert. Jedes Instrument wird als mögliche Antwort auf ein verbreitetes Kontrolldefizit vorgestellt. In Kapitel 3 folgt dann eine Diskussion der wichtigsten Aspekte, die bei der Umsetzung dieser Ideen berücksichtigt werden müssen – Fragen der IT-Sicherheit, der exekutiven Eigenverantwortung und sich überschneidender Zuständigkeiten in der Aufsicht. Anschließend arbeiten wir heraus, von welchen Akteuren diese Kontrollinstrumente am besten angewandt werden können, d.h. ob sie von der Exekutive oder von unabhängigen Aufsichtsbehörden genutzt werden. Abschließend geben wir Empfehlungen ab, wie die Umsetzung dieser Ideen politisch und praktisch vorangetrieben werden kann.

Die sieben Ideen variieren in Bezug darauf, wie anspruchsvoll ihre Umsetzung ist. Im Großen und Ganzen werden wir jedoch argumentieren, dass eine datenbasierte Nachrichtendienstaufsicht eine größere Effektivität und Legitimität bei zugleich geringeren Kosten verspricht – vorausgesetzt, die Aufsichtsbehörden erlangen Zugang zu den operativen Systemen der Nachrichtendienste und wissen diesen auch zu nutzen.

9 Stiftung Neue Verantwortung, „Zweiter Workshop des European Intelligence Oversight Network“, 10. Mai 2019, https://www.stiftung-nv.de/de/node/2576.

2. Sieben Ideen zur Modernisierung der Kontrollinstrumente

> *„Die CTIVD untersucht derzeit den Einsatz computergestützter Datenverarbeitung in der Aufsicht, z. B. durch den automatischen Abgleich der von den Diensten verarbeiteten Daten, um so Abweichungen in der Datenverarbeitung erkennen zu können.“*
> (CTIVD-Geschäftsbericht 2018, S. 15)[10]

Nachrichtendienste verarbeiten heutzutage mehr Daten als je zuvor und es gibt keinen Hinweis darauf, dass sich dies in naher Zukunft ändern wird – ganz im Gegenteil. Die europäischen Kontrollbehörden müssen sich daher rasch an den technologischen Wandel und die rasante Entwicklung der Überwachungsmethoden anpassen. In dieser Studie betrachten wir eine Reihe von Instrumenten und mittelfristigen Zielen, die unserer Meinung nach Teil einer Reformagenda für die Nachrichtendienstaufsicht in ganz Europa werden sollten.

Bevor wir weiter auf die Möglichkeiten einer umfassenden und vorausschauenden Kontrolle eingehen, gilt es einige Aspekte zu beachten. Der folgende Abschnitt beginnt mit der kurzen Darlegung unseres Ausgangspunktes. Im Anschluss daran untersuchen wir, ob und wie die von uns vorgestellten datenbasierten Kontrollverfahren für unabhängige Aufsichtsbehörden geeignet sind. Anders gefragt: Gibt es Anwendungen, die sich eher für Institutionen der internen Dienst- und Fachaufsicht eignen? Abschließend werden wir auf klassische analoge Kontrollen eingehen, die neben den neuen technischen Möglichkeiten auch in Zukunft nicht an Bedeutung verlieren werden und sollten.

Unser Ausgangspunkt: Direkter Zugriff auf die technischen Systeme der Nachrichtendienste

Einige europäische Aufsichtsbehörden berichten, dass sie mittlerweile einen besseren Zugang zu den technischen Systemen ihrer nationalen Nachrichtendienste haben. Allerdings haben nur wenige der Behörden detailliert und öffentlich erläutert, wie die Umsetzung eines solchen Zugangs gestaltet ist. Wir stützen unsere Aussagen zum Thema Datenzugriff auf Interviews mit Mitarbeiter:innen verschiedener europäischer Kontrollbehörden, die Teil

10 CTIVD, „Annual Report 2018“, S. 15, https://english.ctivd.nl/binaries/ctivd-eng/documents/annual-reports/2019/06/20/index/CTIVD+annual+report+2018.pdf (eigene Übersetzung).

des European Intelligence Oversight Networks sind, sowie auf die neuesten öffentlich zugänglichen Berichte der Aufsichtsgremien.

Auf Grundlage dieser Quellen können wir sagen, dass die unten aufgeführten Kontrollbehörden, wenn auch in unterschiedlichem Ausmaß, über weiter reichende Zugangsberechtigungen verfügen, als die Mehrheit ihrer europäischen Kolleg:innen. Das bietet eine gute Grundlage für die Einführung und Weiterentwicklung digitaler Kontrollinstrumente.

Im Folgenden bezeichnen wir den verbesserten Zugang als *direkten Zugriff*. Damit meinen wir, dass *die Kontrolleur:innen sich in die technischen Systeme der Nachrichtendienste einloggen und vollkommen unabhängig Daten ihrer Wahl abrufen und auswerten können*. Allerdings sollte der direkte Zugriff nicht mit einem vollständigen Zugriff gleichgesetzt werden. Einige Zugriffsbeschränkungen, welche für die Sicherheit und Geheimhaltung der nachrichtendienstlichen Systeme essentiell sind, werden wahrscheinlich auch weiterhin bestehen bleiben.

Gesetzliche Grundlagen, ihre Auslegungen, die technische Ausstattung und die praktische Umsetzung sind von Land zu Land verschieden. In einigen Ländern werden den Kontrolleur:innen spezielle Computerterminals in den Räumlichkeiten der Nachrichtendienste zur Verfügung gestellt. Diese Art des Zugangs vor Ort wird beispielsweise von den britischen[11], norwegischen und dänischen Aufsichtsbehörden genutzt. In Großbritannien können die Kontrolleur:innen beispielsweise neben ihrer regulären Prüfung, das Personal des Nachrichtendienstes beauftragen, bestimmte Daten zu extrahieren, in ein anderes System zu exportieren (z. B. im Format einer Kalkulationstabelle) und arbeiten dann mit dieser Kopie weiter. Auf diese Weise kann die Kontrollbehörde eine detaillierte Prüfung vornehmen, ohne die Systemintegrität des Dienstes zu beeinflussen. Andere Aufsichtsbehörden können per Fernzugang von ihren eigenen Büros aus auf die technischen Systeme zugreifen. So verfügt beispielsweise die schweizerische Unabhängige Aufsichtsbehörde über

11 Im öffentlichen Jahresbericht 2017 von IPCO an das Parlament heißt es: „Während der Inspektionen haben unsere Kontrolleur:innen Zugang zu dem System, das von den Ermittler:innen und Analyst:innen des MI5 für den Zugriff auf große Mengen von Kommunikationsdaten genutzt wird; wir führen Stichproben und Suchanfragen im System durch. Die Kontrolleur:innen könnten beispielsweise das System nutzen, um uns jede Nennung des Begriffs „Journalist“ anzuzeigen. Dies bedeutet, dass unsere Kontrolleur:innen (i) die Notwendigkeit und Verhältnismäßigkeit der Überlegungen der Analysten und Ermittler beurteilen können; (ii) konkrete Vorgänge untersuchen können und (iii) Anfragen nach sensiblen Datensätzen oder solchen, die Daten über längere Zeiträume benötigen, identifizieren können.“ Siehe IPCO, „Annual Report 2017“, Januar 2019, S. 66, Abschnitt 9.32, https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190131.pdf (eigene Übersetzung).

die nachrichtendienstlichen Tätigkeiten über einen Fernzugriff auf Daten des Schweizer Nachrichtendienstes, was auch besonders geschützte personenbezogene Daten miteinschließt.[12] Zudem unterscheidet sich die Art des Zugriffs darin, ob die Kontrolleur:innen einen permanenten Zugang zu den nachrichtendienstlichen IT-Systemen und Datenbanken haben, oder ob sie von Fall zu Fall für einen begrenzten Zeitraum oder für eine bestimmte Untersuchung Zugang erhalten.

Die folgenden europäischen Aufsichtsbehörden verfügen über einen unserer Definition entsprechenden „direkten Zugriff" auf technische Systeme:

- Dänemark: Nachrichtendienst-Aufsichtsbehörde (TET)[13]
- Frankreich: Nationale Kommission für die Kontrolle von Nachrichtendienst-Technik (CNCTR)[14]
- Niederlande: Kontrollbehörde für die Nachrichten- und Sicherheitsdienste (CTIVD)[15]
- Norwegen: Parlamentarisches Aufsichtsgremium der Nachrichtendienste (EOS)[16]
- Vereinigtes Königreich: Kontrollkommission für nachrichtendienstliche Tätigkeiten (IPCO)[17]
- Schweden: Kontrollbehörde der Nachrichtendienste (SIUN)[18]
- Schweiz: Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND)[19]

Da es oftmals schwierig ist verlässliche Informationen über den Zugang zu Daten zu erhalten, erhebt diese Liste keinen Anspruch auf Vollständigkeit. Wir begrüßen es, wenn weitere Aufsichtsbehörden über die Gestaltung ihrer Zugangsberechtigung berichten.

Der direkte Zugang zu technischen Systemen birgt enormes Potenzial, denn er ermöglicht den Aufsichtsbehörden die Datenverarbeitung der Nachrich-

12 Schweizer Nachrichtendienstgesetz (NDG), „Aufgaben, Informationsrechte und Empfehlungen der Aufsichtsbehörde", Art. 78 (5)," 25. September 2015, https://www.admin.ch/opc/de/federal-gazette/2015/7211.pdf.

13 https://www.tet.dk/?lang=en

14 https://www.cnctr.fr/

15 https://english.ctivd.nl/

16 https://eos-utvalget.no/en/home/

17 https://www.ipco.org.uk/

18 http://www.siun.se/

19 https://www.ab-nd.admin.ch/de/home.html

tendienste durch Stichproben, unangekündigte Inspektionen und (teil-)automatisierte Kontrollen zu überprüfen. Damit verringert sich die Abhängigkeit der Aufsichtsbehörden (sowohl interner, als auch unabhängiger Behörden) von (Einzel-)Informationen, die die Dienste selbst bereitstellen. Der direkte Zugriff stellt einen zusätzlichen Anreiz dar, Datenschutzvorschriften durchweg umzusetzen und einzuhalten, weil die Beschäftigten der Nachrichtendienste nicht wissen können, ob ein bestimmter Vorgang überprüft wird.

Gewiss bedeutet ein direkter Zugriff auf Daten nicht, dass keinerlei Beschränkungen bestehen bleiben. Denn bereits die Mitarbeiter:innen von Nachrichtendiensten sind in der Regel Zugangsbeschränkungen unterworfen: Sowohl theoretisch als auch praktisch haben sie keinen Zugang zu *allen* Arten von Daten. Auch leitende Angestellte sind an Einstufungen zur Geheimhaltung gebunden und können Informationen nur einsehen, wenn es operativ notwendig ist. Dass Aufsichtsbehörden sich über sämtliche Zugangsbarrieren hinwegsetzen könnten, ist dementsprechend schwierig vorstellbar.

Vor diesem Hintergrund stellt sich die entscheidende Frage, *auf welche Arten von Daten* die Aufsichtsbehörden tatsächlich zugreifen können und wie. Je nach Aufsichtsinstrument oder Kontrollverfahren ist der Zugang zu unterschiedlichen Datentypen erforderlich. Die folgende Tabelle unterscheidet zwischen verschiedenen Zugängen für unterschiedliche Aufsichtsfunktionen. Anstatt die Notwendigkeit und Machbarkeit eines direkten Zugangs grundsätzlich zu bestreiten, sollte der Fokus auf den konkreten Datentypen liegen, die für eine effektive interne und externe Nachrichtendienstkontrolle erforderlich sind.

Art des Datenzugriffs	Beschreibung	Vorteile für die Aufsicht
Zugriff auf Quelldaten	„Rohdaten“, die noch nicht für eine spätere Nutzung weiterverarbeitet wurden. Ihre Eigenschaften hängen von der jeweiligen Quelle der Daten ab, wie z. B. Fernmeldeaufklärung, offene Quellen, Informant:innen, Erwerb von Datensätzen von Unternehmen, Infiltration von Computernetzwerken, Satellitenaufklärung, etc.	(C) Risikoabschätzung (B4) Nachverfolgung von Anordnungen (D) Dialog zwischen Kontrollgremien und Dienstanbietern

Zugriff auf gespeicherte Daten	Strukturierte Datenbanken, die z. B. Daten nach dem Filterprozess enthalten. Dies umfasst sowohl Meta- als auch Inhaltsdaten.	(A) Überprüfung der Datenfilter (C) Risikoabschätzung
Zugriff auf Protokolldaten	Metadaten über die Verwendung von Daten durch die Nachrichtendienste, beinhaltet u.a. die Auswahl, Sichtung, Übermittlung, Löschung und Auswertung von Daten.	(B1) Mustererkennung (B2) Warnhinweis bei Datenaustausch (B3) Lösch-Statistiken (B4) Nachverfolgung von Anordnungen
Zugriff auf Auswertungen	Ergebnisse der nachrichtendienstlichen Informationsgewinnung, die sich oftmals an politische Entscheidungsträger:innen richten. Diese umfassen z. B. Berichte über spezifische Bedrohungen, Länder, militärische Operationen usw.	(B4) Nachverfolgung von Anordnungen (C) Risikoabschätzung

Vor- und Nachteile des direkten Zugriffs

Durch unsere Interviews mit verschiedenen Beschäftigten europäischer Aufsichtsbehörden hat sich gezeigt, dass der direkte Zugriff auf Datenbanken und technische Systeme in Verbindung mit moderner Kontrolltechnik die Arbeit der Kontrollgremien deutlich effizienter gestalten kann.

Doch wie genau sollten diese datenbasierten Kontrollverfahren im Gefüge demokratischer Institutionen gestaltet sein? Die meisten demokratischen Länder sind sich einig, dass die Einhaltung gesetzlicher Vorschriften kontrolliert werden muss, doch ob eine solche Prüfung ausschließlich von der exekutiven Dienst- und Fachaufsicht durchgeführt werden sollte (Position 1) oder ebenfalls von unabhängigen Aufsichtsbehörden (Position 2) führt zu Uneinigkeit. Die unabhängige dänische Aufsichtsbehörde TET genießt beispielsweise einen direkten Zugang zu operativen Systemen, die deutsche G10-Kommission und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hingegen nicht. Wir werden auf diese unterschiedlichen Positionen und ihre praktischen Auswirkungen an mehreren Stellen in diesem Papier zurückkommen.

Wenn Aufsichtsbehörden ein umfangreichere Zugang zu Daten zu gewährt werden soll, müssen zahlreiche Aspekte berücksichtigt werden. Dazu gehören Bedenken im Bereich der IT- und Cybersicherheit, das Prinzip der exekutiven

Eigenverantwortung und praktische Aspekte wie das Risiko von redundanten Kontrollen durch verschiedene Aufsichtsorgane. Darüber hinaus muss der Bedarf an effektiver Kontrolltechnik mit den begrenzten Ressourcen, über die Aufsichtsbehörden typischerweise verfügen, in Einklang gebracht werden. Jeder dieser Punkte verdient gesonderte Aufmerksamkeit. Wir werden im dritten Kapitel auf sie zurückkommen.

Technologie ist keine Antwort, wenn man die Frage nicht versteht

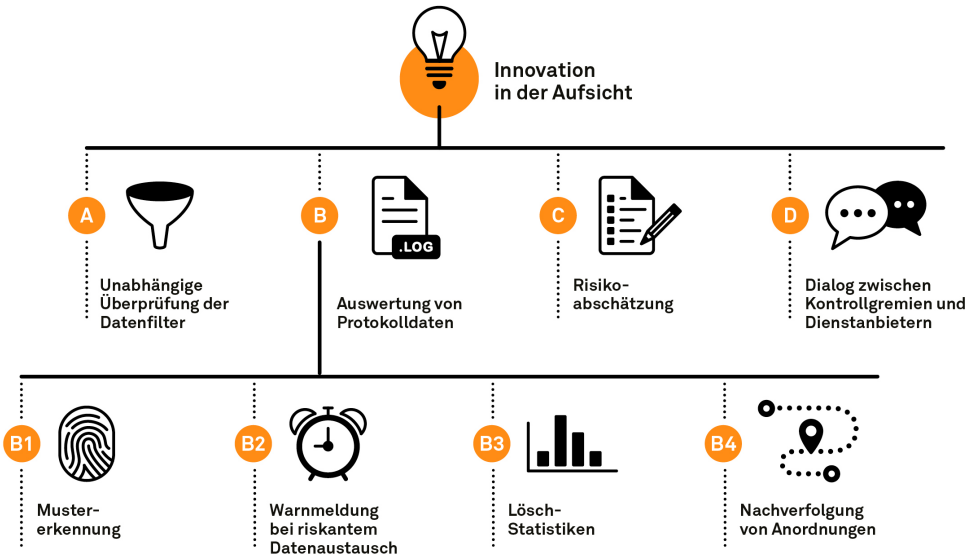
Dieses Plädoyer für eine stärker datenbasierte Nachrichtendienstaufsicht soll nicht die zentrale Rolle gewissenhafter Kontrolleur:innen untergraben, die vor Ort Akten durchsuchen und Beschäftigte der Nachrichtendienste befragen. Wir sind, ganz im Gegenteil, davon überzeugt, dass individueller Einsatz, persönliche Expertise und direkter Austausch nach wie vor entscheidend sind, um eine wirksame Nachrichtendienstaufsicht im 21. Jahrhundert zu garantieren. Die Kombination von technischen Aufsichtsmethoden mit menschlichen Analyse- und Interpretationsfähigkeiten ist notwendig, um echte Innovationen zu erzielen. Dementsprechend möchten wir die Fachleute für Datenschutz und Praktiker:innen der Nachrichtendienstkontrolle auffordern, die datenbasierte Aufsicht stärker zu nutzen und diese als einen wesentlichen Bestandteil ihres wachsenden Instrumentariums zu betrachten.

Gleichwohl möchten wir vor einem allzu dogmatischen Glauben an Algorithmen und Daten als Allheilmittel für aktuelle Herausforderungen warnen. Datenbanken, Überwachungstechnik und Analysewerkzeuge sind von Menschenhand geschaffen; sie können Fehler, Ungenauigkeiten und Verzerrungen enthalten und sogar verschlimmern. Dies kann ohne menschliches Hinterfragen und Korrekturmaßnahmen leicht zu Fehlentscheidungen führen.

Gliederung der Instrumente

Wir werden nun die Instrumente, Anwendungen und Ideen vorstellen, von denen wir glauben, dass sie sowohl seitens verantwortungsvoller Nachrichtendienste als auch von demokratischen Kontrollgremien stärker diskutiert werden sollten. Wir beginnen bei jedem Instrument damit, eine konkrete Herausforderung der modernen Nachrichtendienstkontrolle kurz zu beschreiben, um dann eine Idee oder ein Werkzeug als mögliche Antwort auf diese Herausforderung

vorzustellen. Folgende Abbildung bietet einen Überblick der Methoden und Werkzeuge, die in diesem Abschnitt erläutert werden.



Selbstverständlich sind solche Empfehlungen nur dann von Gehalt, wenn sie die Vor- und Nachteile, sowie Risiken einer Maßnahme beachten. Hierauf werden wir im dritten Kapitel näher eingehen.

A. Durchsuchen gespeicherter Daten auf Filterfehler

Herausforderung

Nicht immer stimmt die Praxis mit dem juristischen Regelwerk überein. Dass gesetzliche Bestimmungen tatsächlich eingehalten und nicht „kreativ“ (oder versehentlich) umgangen werden, stellt für jede Institution, die mit der Kontrolle großer bürokratischer Systeme betraut ist, eine große Herausforderung dar. Ein Beispiel ist das höhere Datenschutzniveau für Inländer (bzw. „Grundrechtsträger“) gegenüber Ausländern im Ausland, wie es viele Nachrichten-

dienstgesetze vorsehen.[20] Einige Gesetze sehen zusätzliche Schutzvorkehrungen für die Erfassung der Kommunikation von Berufsgeheimnisträgern vor (z. B. die Kommunikation zwischen Patient:innen und Ärzt:innen, Kirchgängern und Priester:innen oder zwischen Anwält:innen und ihren Mandant:innen). Diese und andere spezifische Bedingungen müssen erfüllt sein, damit die Nachrichtendienstpraxis im jeweiligen Land rechtmäßig ist. Viele Behörden führen daher komplexe Datenfilterprozesse durch.

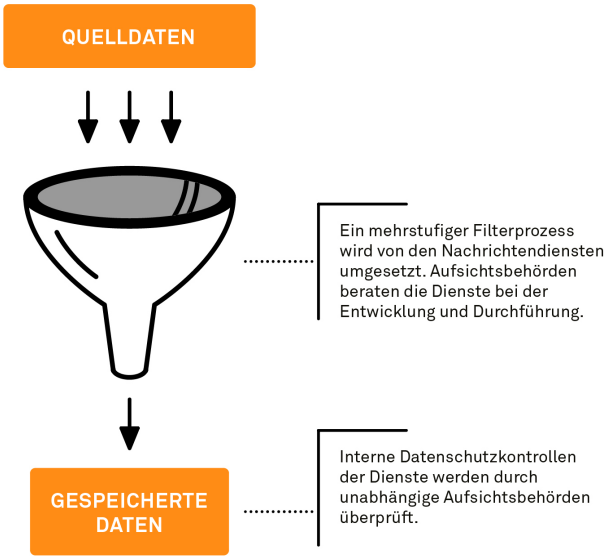
Wenn es um spezifische Informationen über die Genauigkeit von Filterprozessen geht, haben viele Aufsichtsbehörden in Europa oft keine andere Wahl, als sich auf die Angaben der Nachrichtendienste zu verlassen. Ernsthafte Kontrollen der Zuverlässigkeit der Daten-Filter, die Behörden zur Einhaltung der gesetzlichen Vorschriften verwenden, werden selten durchgeführt.[21] Das stellt ein großes Problem dar, schließlich kann ein riesiges Datenvolumen falsch verarbeitet werden, wenn die Filter nicht richtig funktionieren. Darüber hinaus müssen mit Hilfe von Filterverfahren eine Vielzahl von Rechtsvorschriften eingehalten werden; wird keine gründliche Überprüfung vorgenommen, ist es schwierig festzustellen, ob diese Verfahren tatsächlich rechtskonform funktionieren. Daher wären die Aufsichtsbehörden gut beraten, mehr unabhängige Überprüfungen von Filterprozessen anzustreben. Idealerweise sollten Nachrichtendienstgesetze die notwendige Filtergenauigkeit konkret angegeben.[22]

20 Für eine detaillierte Diskussion über die Rolle der Staatsangehörigkeit in der Nachrichtendienstgesetzgebung, siehe den Bericht von Swire, Woo und Desai: „The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance“, Januar 2019, Aegis Series Paper No. 1901, https://www.hoover.org/sites/default/files/research/docs/swire-woo-desai_the-important-justifiable-constrained-role-of-nationality-in-foreign-intelligence-suhttps://writer.zoho.com/writer/open/13b5n0d5c99be9c2b452480e466cf1fa5eb456. In Deutschland steht ein Urteil des Bundesverfassungsgericht über die Rechtmäßigkeit des BND-Gesetzes von 2016 aus, das u.a. unterschiedliche Datenschutzkategorien auf der Grundlage von Staatsangehörigkeit vorsieht.

21 Eine Ausnahme ist der jüngste CTIVD-Bericht über den Einsatz von Filtern durch die niederländischen Geheimdienste AIVD und MIVD. CTIVD, „Progress Report“, 17. Juli 2019 (CTIVD Nr.63), https://www.ctivd.nl/documenten/rapporten/2019/09/03/index.

22 Für weitere Informationen zu Filtern und Kontrollmöglichkeiten, siehe Wetzling und Vieth, „Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich“, November 2018, S. 56ff, https://www.stiftung-nv.de/sites/default/files/massenuberwachung_bandigen_-_web.pdf.

Idee: Unabhängige Überprüfung der Datenfilter



Wenn Kontrollbehörden Zugang zu den gespeicherten Daten der Nachrichtendienste erhalten, können sie Instrumente zur Überprüfung der Genauigkeit von Filterprogrammen entwerfen (oder mit den Nachrichtendiensten zusammenarbeiten, um sie mitzugestalten). So könnten die Kontrolleur:innen beispielsweise Listen mit Suchbegriffen für geschützte Personengruppen erstellen, oder die Namen oder E-Mail-Adressen von deutschen Staatsangehörigen, die für internationale Organisationen arbeiten, auflisten. Auf der Grundlage der nationalen Nachrichtendienstgesetze könnten die Kontrolleur:innen weitere Indikatoren angeben, die auf eine Verletzung einer bestimmten Vorschrift hinweisen. Ein automatisiertes Suchprogramm könnte dann die gesamten gespeicherten Daten nach diesen Merkmalen durchsuchen, die nach der Anwendung eines Filters nicht mehr auffindbar sein sollten.

Wie sollten die Aufsichtsbehörden an den Überprüfungen der Filter beteiligt sein?

Verantwortlich für die Implementierung von Filtersystemen sind in der Regel die Nachrichtendienste. Ob Filter ihren Zweck erfüllen, ist aber auch eine Frage, die unabhängige Aufsichtsbehörden unmittelbar betrifft. Eine mangelhafte Filterung könnte zu weitreichenden Verletzungen der Grundrechte führen, was die Legitimität des Regierungshandelns schwer beeinträchtigen würde. Der direkte Zugriff auf Datenbanken der Nachrichtendienste würde es den Aufsichtsbehörden ermöglichen, selbstständig nach Überresten fehlerhafter Filterung zu suchen, z. B. nach inländischen Daten in ausländischen Datenbanken.

Der Prüfprozess könnte mit Validierungs-Software (teil-)automatisiert werden: Als Standardroutine könnten Computerprogramme die Datenbanken durchsuchen, um sicherzustellen, dass die gespeicherten Daten der Nachrichtendienste mit den geltenden Vorschriften übereinstimmen. Die Überprüfung der Rechtmäßigkeit der gespeicherten Daten kann durch einfache „Merkmaltests" erfolgen. So könnte beispielsweise festgelegt werden, dass eine Telefonnummer in einem ausländischen Datensatz keine inländische Vorwahl enthalten darf. Kontrolleur:innen könnten insbesondere mit Listen von Suchbegriffen arbeiten, die sie für relevant halten, ohne diese vorab an den Nachrichtendienst weiterzugeben. Im Laufe der Zeit könnten Aufsichtsbehörden so Rückschlüsse auf die Gesamtgenauigkeit und Rechtmäßigkeit der Filter ziehen und den Gesetzgeber anschließend beraten, inwieweit rechtliche Rahmenbedingungen für bestimmte Datenkategorien in der Praxis erfolgreich eingehalten werden.

Aufsichtsbehörden die Nutzung von Prüfsoftware für gespeicherte Daten zu erlauben, erfordert Verhandlungen mit der Exekutive, da diese Filter-Kontrollen eine unzulässige Dopplung bedeuten könnten. Angesichts der knappen Ressourcen und des benötigten technischen Fachwissens scheint es zudem unrealistisch zu sein, von den Aufsichtsbehörden zu verlangen, den gesamten Filterprozess zu überprüfen – dies sollte ohnehin von den Nachrichtendiensten selbst durchgeführt werden, damit sie sicherstellen, dass gesetzliche Bestimmungen eingehalten werden. Es wäre jedoch ein Fehler, sich ausschließlich auf die Selbstkontrolle der Nachrichtendienste zu verlassen, ohne die Filtertechnik einer unabhängigen Überprüfung zu unterziehen. Datenfilterung ist eine entscheidende nachrichtendienstliche Praktik, deren große Bedeutung auch die Aufsichtsbehörden anerkennen und sie einer kritischen und unabhängigen Prüfung unterziehen sollten. Entsprechend sollten Kontrollgremien bei der Gestaltung und Umsetzung von Filterverfahren konsultiert werden und darüber hinaus sollten sie befugt sein, unabhängige Prüfungen der Rechtmäßigkeit gespeicherter Daten durchzuführen. Dies würde einer Abwandlung des britischen „double lock"-Systems gleichkommen,[23] wonach dann sowohl das Anordnungsverfahren als auch die Datenfilterung eine Kontrolle unabhängiger Aufsichtsbehörden erfordern. Die Kontrolleur:innen der Aufsichtsgremien könnten dazu zunächst Datensätze auswählen, die relativ einfache binäre Kategorien einhalten müssen – zum Beispiel Tests, die auf simplen numerischen Indikatoren wie Ländervorwahlen in Telefonnummern beruhen, durchführen. Die Analyst:innen könnten dann Schritt für Schritt zu einer komplexeren

23 Durch die im IP Act festgehaltene „Doppelte Absicherung" (sog. „double lock") im Anordnungsverfahren, muss nach der Autorisierung durch ein Mitglied der britischen Regierung, zusätzlich die Genehmigung eines Richters (sog. Investigatory Powers Commissioner) eingeholt werden. Siehe GCHQ, „Investigatory Powers Act", 18. März 2019, https://www.gchq.gov.uk/information/investigatory-powers-act.

Überprüfung übergehen, die mehrere, sich möglicherweise überschneidende Datenschutzkategorien umfasst, wie beispielsweise Staatsangehörige, die im Ausland in geschützten Berufsfeldern (z. B. Presse) arbeiten.

B. Auswertung von Protokolldaten

> *„Protokolldaten zu analysieren ist ein wichtiges Werkzeug und es ist schwierig, Aufsicht ohne dieses Werkzeug durchzuführen. Unsere Erfahrung zeigt, dass es notwendig ist Logdateien zu validieren. Mit anderen Worten, Kontrolleur:innen müssen den Vorgang der Protokollierung überprüfen, um sicher zu stellen, dass die Logs vollständig und korrekt sind.“*
> (Emil Bock Greve, Leiter des Sekretariats, Dänische Nachrichtendienst-Aufsichtsbehörde)

Um die riesige Menge der gesammelten Daten zu organisieren und zu verstehen, sind Nachrichtendienste und Sicherheitsbehörden auf leistungsfähige informationstechnische Systeme angewiesen. Sowohl externe Dienstleister als auch interne Abteilungen der Dienste entwickeln Softwarelösungen für die Datenanalyse.[24] Solche IT-Systeme produzieren enorme Mengen an Metadaten (oft standardmäßig), die in Protokolldateien aufgezeichnet werden. Wie wir im Folgenden näher erläutern werden, haben diese Protokolldaten das Potenzial, sowohl die internen Kontrollen als auch die unabhängige Aufsicht der Nachrichtendienste erheblich zu stärken.

Aus operativen Gründen (z. B. Abwehr von Hacker-Angriffen) überprüfen Nachrichtendienste und Sicherheitsbehörden ihre Logdateien laufend und haben daher weitaus mehr Erfahrung und Expertise in der Analyse von Protokolldaten als die Aufsichtsbehörden. Neben offenen Fragen bezüglich der exekutiven Eigenverantwortung für IT-Systeme, birgt die Ausstattung von Aufsichtsbehörden mit verschiedenen Instrumenten der Protokolldatenanalyse das Risiko, dass überlappende Zuständigkeiten zwischen interner und externer Kontrolle entstehen und Aufgaben doppelt anfallen. Wie bereits im vorangegangenen Abschnitt erwähnt, muss dieses Risiko jedoch gegen das einer übermäßigen Abhängigkeit von rein internen Kontrollprozessen der Nachrichtendienste abgewogen werden. Über diese internen Kontrollen wissen wir, dass sie in der Vergangenheit mitunter nur mangelhaft umgesetzt

24 Beispiel für solche Datenanalysesoftware sind Palantirs Gotham, Rolas rsIntCent oder IBMs i2 Analyst‘s Notebook. Einige Regierungen investieren zudem systematisch in die Entwicklung und Bereitstellung von Spitzentechnologien für ihre Nachrichtendienste über Organisationen wie I-Q-Tel (https://www.iqt.org/) und Defense Advanced Research Projects Agency (DARPA, https://www.darpa.mil/) in den Vereinigten Staaten.

oder – noch schlimmer – von den relevanten Entscheidungsträger:innen sogar gänzlich ignoriert wurden.[25]

Protokolldaten: eine kurze Einführung
Logdateien oder auch Protokolldateien (englisch *log file*) zeigen an, wann, auf welche Art, wie lange und von wem ein bestimmtes Computersystem genutzt wurde. Alle Änderungen an einer Datenbank und alle Abfragen einer bestimmten Benutzerin werden automatisch gespeichert und mit Zeitstempeln versehen. Das ermöglicht es Systemadministrator:innen zum Beispiel Dateien und unvollständige Transaktionen wiederherzustellen und die Benutzerfreundlichkeit einer Software (abgeleitet vom Nutzerverhalten) weiterzuentwickeln.

Die folgenden Ereignisse werden typischerweise in Logdateien aufgezeichnet, was sie für Auditzwecke besonders nützlich macht:

- Modifikationen von Datenpunkten und Datensätzen
- Zeitpunkt eines Zugangs und Dauer einer Aktivität
- Benutzeridentifikation (inklusive z. B. Standortdaten)
- Versuchte/fehlgeschlagene Aktionen in bestimmten Datenbanken

Fügt ein Benutzer beispielsweise eine Datei einer Datenbank hinzu, enthält die entsprechende Logdatei die dazugehörigen Metadaten, welche die ID des Benutzers, den Zeitpunkt der Änderung und die Art der geänderten Daten erfassen. Automatisierte Aktionen, wie eine vorprogrammierte Löschung von Daten, werden ebenfalls in Logdateien aufgezeichnet.

Logdateien bilden in der Regel statische Datensätze, die vor allem nachträgliche Überprüfungen ermöglichen. Haben die Aufsichtsbehörden keinen permanenten Zugriff auf Logdaten, besteht die Möglichkeit einer automatisierten Übermittlung. Hierbei werden Logdaten regelmäßig aus dem IT-System des Nachrichtendienstes exportiert und in das der Kontrollbehörde übertragen.

25 So hat beispielsweise das Bundeskanzleramt im Zuge der NSA-Affäre technische und organisatorische Defizite öffentlich angesprochen, was zu einem Untersuchungsausschuss führte, der wiederum Informationen zu diesen Defiziten lieferte. Lohse, „Kanzleramt übt heftige Kritik an BND“, 23. April 2015, https://www.faz.net/aktuell/politik/inland/kanzleramt-uebt-heftige-kritik-an-bnd-13555622.html.

Umgekehrt können Aufsichtsgremien auch eigenständig (ggf. manuell) Daten von einem Nachrichtendienst extrahieren.[26]

Wie können Protokolldaten ausgewertet werden? In der folgenden Tabelle sind die Vorteile der Nutzung der IT-Systeme der Nachrichtendienste und die Vorzüge der Analyse exportierter Kopien von Logdaten gegenübergestellt. Wie Praktiker:innen betonen, nutzt eine effektive Aufsicht idealerweise beide Arten der Datenauswertung.

Vorteile einer Nutzung der IT-Systeme der Nachrichtendienste zur Analyse von Logdaten	**Vorteile einer Verwendung von Kopien der Logdaten zur Analyse auf eigenen Systemen**
Kontrollen laufender Operationen sind möglich, nicht nur nachträgliche Überprüfungen.	Nach dem Export einer Logdatei sind keine nachträglichen Anpassungen oder Manipulationen möglich.
Kontrolleur:innen können schneller auf erkannte Unregelmäßigkeiten reagieren.	Kontrolleur:innen haben mehr Autonomie bei der Verwendung von Protokolldaten, z. B. können sie ihre eigene Analysesoftware wählen.
Logdaten sind potenziell aktueller, vollständiger und übersichtlicher strukturiert.	Die Aufsichtstätigkeit belastet die operativen IT-Systeme der Dienste nicht.

Aufsichtsbehörden, die überwiegend mit Offline-Kopien von Logdateien arbeiten, beklagen mitunter, dass es große Unterschiede in der Qualität der Informationen geben kann, die sie aus Protokolldateien ziehen. Wenn eine Logdatei nur Informationen wie „Datei geändert“ enthält, ohne weitere Informationen über die Art, den Zeitpunkt oder den Auslöser der Änderungen, dann bieten diese Protokolle keine ausreichende Grundlage für eine wirksame Aufsicht.

Interessanterweise haben die jüngsten Gesetzesreformen die Nachrichtendienste oft konkreter dazu verpflichtet ihren Kontrollgremien Zugang zu Protokollen und Registern zu gewähren. Doch noch immer wird die Bedeutung der Qualität einer Logdatei bei der Überprüfung ihrer Rechtmäßigkeit unterschätzt. In Zukunft sollten die von den Nachrichtendiensten verwendeten datenverarbeitenden Systeme so konzipiert sein, dass die Datennutzung so detailliert wie möglich aufgezeichnet wird und dass die Kontrolleur:innen alle durchgeführte Aktionen vollständig nachvollziehen können. Derzeit besteht zwischen den

26 Entsprechend dem Grundsatz der Datensparsamkeit müssen die Aufsichtsbehörden sorgfältig prüfen, welche Daten sie in ihren eigenen Räumlichkeiten oder IT-Systemen aufbewahren, wenn dieselben Aufzeichnungen bereits bei dem Nachrichtendienst oder dem Ministerium gespeichert sind.

Logdaten für die interne Prüfung und den Protokolldaten, die der unabhängigen Aufsicht zugänglich sind, oft eine enorme Informationsasymmetrie.

Je nach praktischer Umsetzung, kann der Zugang zu detaillierten Protokolldateien viel Raum für neue Kontrollinstrumente schaffen. Auf vier Ansätze gehen wir im Folgenden näher ein.

B1: Untersuchung von Mustern im Nutzungsverhalten

Herausforderung
Nachrichtendienste wie der britische GCHQ, der französische DGSE und der deutsche BND sammeln und speichern immer größere Datenmengen. Wirksame Kontrollmechanismen für (massenhafte) Datenverarbeitung liegen daher im Interesse aller Nachrichtendienste, die im Dienste offener, demokratischer Gesellschaften stehen. Datenschutz beginnt mit einer ordentlichen Verwaltung der Zugriffsrechte und der Einrichtung von Kontrollmechanismen, die direkt in die Informationssysteme der Nachrichtendienste integriert sind. Wählt beispielsweise ein:e Nutzer:in Daten für eine unzulässige Analyse aus oder versucht Daten für einen anderen als den ursprünglich genehmigten Zweck zu verwenden, dann sollten die Betriebssysteme der Nachrichtendienste dieses Verhalten automatisch blockieren.

Auch wenn die Notwendigkeit für Datenschutz innerhalb der Nachrichtendienste anerkannt wird, sind alarmierende Fälle unangemessener und gar unrechtmäßiger Zugriffe auf Datenbanken bekannt geworden.[27] Über Fälle, in denen Polizeibeamt:innen Datenbanken mit sensiblen personenbezogenen Daten für private Zwecke abgefragt haben, wird ebenfalls häufiger berichtet.[28]

27 Ein deklassifiziertes FISA-Gerichtsurteil zeigte, wie das FBI die Massenüberwachungsdaten der NSA missbrauchte, indem es nach Online-Kommunikation von US-Bürger:innen, einschließlich FBI-Mitarbeiter:innen und ihrer Familienmitgliedern, suchte. Laut dem FISC-Bericht führte das FBI allein im Jahr 2017 etwa 3,1 Millionen Suchanfragen im Zusammenhang mit US-Personen durch. Nach eigenen Angaben nahm das FBI nur etwa 10.000 Untersuchungen pro Jahr vor. Siehe hierzu: Aaronson, „A Declassified Court Ruling Shows How The FBI Abused NSA Mass Surveillance Data“, 10. Oktober 2019, https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/; Original-FISC-Dokument unter: United States Foreign Intelligence Surveillance Court, „FISC Opinion regarding the Section 702“, 18. Oktober 2018, https://www.documentcloud.org/documents/6464604-2018-FISC-Ruling-Shows-How-FBI-Abused-NSA-Mass.html.

28 Eine Übersicht über Missbrauchsfälle von Polizeidatenbanken in Deutschland gibt Golla: „Neugier und Datenkriminalität“, 16. August 2019, https://www.lto.de/recht/hintergruende/h/polizei-datenbanken-missbrauch-datenkriminalitaet-abfragen-datenschutz/. Für einen aktuellen Fall in Großbritannien, siehe Corfield, „London Cop illegally used police database to monitor investigation into himself“, 11. Juli 2019, https://www.theregister.co.uk/2019/07/11/met_police_sgt_pleads_guilty_computer_misuse_crimes/.

Dabei handelt es sich nicht um isolierte Einzelfälle; es fehlen oft wirksame Schutzmaßnahmen gegen missbräuchliche Datenbankabfragen. Das verdeutlicht die Notwendigkeit, dass unabhängige Aufsichtsbehörden zusätzliche Maßnahmen ergreifen müssen. So könnten sie beispielsweise Logdaten auf ungewöhnliche Zugriffszeiten oder auf ungewöhnlich häufige Datenabfragen für bestimmte Personen überprüfen.

Idee: Mustererkennung

Welche (Verhaltens-)Muster könnten auf Aktivitäten hinweisen, die möglicherweise nicht rechtskonform sind? Beispielsweise können Prüfer:innen nach ungewöhnlichen Häufungen der Aktivität eines einzelnen Nutzers (z. B. eines Nachrichtendienst-Beschäftigten) oder nach außergewöhnlich vielen Transaktionen in einer bestimmten Datei Ausschau zu halten. Die Prüfer:innen können auch potenzielle Probleme im Auge behalten, wie z. B. eine besonders hohe Anzahl von Benutzerkonten, die bestimmte Daten auswerten oder die besonders häufige Nutzung von Datenbanken von ungewöhnlichen Zugriffspunkten aus. Die Möglichkeiten zur Analyse von Logdateien reichen von einfachen deskriptiven Methoden (etwa der Vergleich von Durchschnitts-, Mittel-, Maximal- und Minimalwerten) bis hin zu komplexen Verfahren maschinellen Lernens oder statistischer Analysen. Datenanalyse-Software kann den Kontrolleur:innen helfen, die Nutzung von Datenbanken zu visualisieren sowie statistische Zusammenhänge und Netzwerke in den Protokolldaten zu erkennen und zu veranschaulichen. Gelingt es den Prüfer:innen, z. B. Muster illegaler Datennutzung zu erkennen, können sie sich entscheiden, eine weiterführende Untersuchung des jeweiligen IT-Systems oder der Aktivitäten der verantwortlichen Mitarbeiter:innen einzuleiten. Um falschen Verdächtigungen vorzubeugen, ermöglichen einige Softwaretools auch die exakte Wiederherstellung der zeitlichen Abfolge aller Änderungen an einer Datenbank. Dies ermöglicht es den Prüfer:innen den nachrichtendienstlichen Analyseprozess durch die Augen der Nutzenden wahrzunehmen. Durch eine solche Reproduktion der Handlungsschritte kann ein zunächst als verdächtig wahrgenommenes Nutzungsverhalten unter Umständen wiederum rational und rechtmäßig erscheinen. Wenn Logdateien nur allgemeine Benutzung aufzeichnen (z. B. „Datei wurde gelesen; Datei wurde gespeichert, Datei wurde geändert“) schränkt dies selbstverständlich die Möglichkeiten der Analyse von Logdateien für Aufsichtszwecke erheblich ein.

Welche Methoden der Mustererkennung liefern die besten Ergebnisse für (unabhängige) Prüfverfahren? Die Antwort darauf hängt von den verfügba-

ren Daten und dem Zweck der jeweiligen Untersuchung ab.[29] Audits können aufzeigen, welche Arten von Daten Auswerter:innen typischerweise parallel verwenden, etwa ob Daten aus Funkzellenabfragen, Open Source Intelligence (OSINT) oder Social Media Intelligence (SOCMINT), möglicherweise miteinander in Verbindung gebracht werden. Dies kann oft dazu führen, dass Daten in neuen Datenbanken gespeichert werden und den gesetzlichen Anforderungen nicht mehr ausreichend entsprechen (z. B. in Bezug auf Zweckbestimmungen oder Einschränkungen der Datenweitergabe). Die Analyse von Verwendungsmustern kann den Kontrolleur:innen zudem zu einem besseren, evidenzbasierten Gesamtverständnis der tatsächlichen Arbeitsabläufe der Nachrichtendienstmitarbeiter:innen verhelfen. Verstehen Aufsichtsbehörden die „normale“ Nutzung, können sie besser potenziell verdächtige Aktivitäten davon unterscheiden. Die Mustererkennung in Logdateien kann daher als Mittel zur Verbesserung des Dialogs angesehen werden, denn sie hilft die richtigen Personen und Fälle zu identifizieren, denen die Kontrolleur:innen eine vertiefende Untersuchung widmen sollten.

Die oben beschriebene Durchführung einer Mustererkennung in Protokolldaten erfordert Präzision und technisches Können. Sie birgt einerseits das (große) Risiko, dass zu breit angelegte Suchmuster viele Fehlalarme auslösen könnten, die die Aufsichtsbehörden überfordern und sie von wichtigeren Aufgaben ablenken. Andererseits kann eine zu spezifische Suchroutine überhaupt keine Treffer hervorrufen (obwohl es relevante Muster gäbe), wenn der Suchalgorithmus so konfiguriert ist, dass er zu viele Parameter miteinander kombiniert.

Da parallel hunderte Benutzer in einem bestimmten System arbeiten können und jährlich Millionen Einzelaktionen aufgezeichnet werden, kann sich eine effektive Aufsicht nicht nur auf eine manuelle Analyse verlassen. (Teil-)automatisierte Analysen können es den Kontrolleur:innen ermöglichen, mit großen Mengen an Protokolldaten besser umzugehen. Interessanterweise stehen IT-Sicherheitsabteilungen vor der gleichen Herausforderung, wenn es um die Überprüfung von Logs geht (z. B. bei der Erkennung von Einbruchsversuchen in IT-Systeme). Die bestehende Forschung von Firmen aus dem Bereich der Informationssicherheit und Informatik kann für die Aufsichtsbehörden von großer Hilfe sein und innovative Lösungen dafür bieten, wie man Logs am besten analysiert oder wie man mit dem Problem der Informationsflut durch ständig wachsende Protokolldatenmengen umgeht.

29 So versuchen beispielsweise Wirtschaftsprüfer:innen Insiderhandel oder Geldwäscheaktivitäten aufzudecken. IT-Sicherheitsabteilungen verfolgen vor allem Netzwerkeindringlinge. Für viele Unternehmen die mit großen Datenmengen umgehen, wie Banken und Versicherungen, sind robuste Compliance-Systeme unerlässlich, um einen effizienten Betrieb zu gewährleisten.

B2: Automatisierten Informationsaustausch scannen

Herausforderung

Sowohl auf nationaler als auch internationaler Ebene hat die Nachrichtendienstkooperation in den letzten Jahrzehnten an Bedeutung gewonnen. Zweifelsohne ist es für nationale Sicherheitsbehörden wichtig, belastbare Beziehungen zu ihren internationalen Partnern aufzubauen und zu pflegen. Gleichzeitig ist dieser Bereich der Nachrichtendienstpraxis noch immer der, der am wenigsten kontrolliert wird. Das bietet die Gelegenheit für geheime Absprachen und lädt zur kreativen Umgehung von Vorgaben ein.[30] Das weitere Ausbleiben einer systematischen und fallbezogenen internationalen Zusammenarbeit von Aufsichtsgremien[31] befeuert daher das Kontroll- und damit auch das Demokratiedefizit in diesem Bereich.

Auch wenn die internationale Kooperation der Dienste häufig als eine der schwierigsten Fragen im ohnehin schon komplexen Streben nach demokratischer Nachrichtendienstführung beschrieben wird, sind Verbesserungen des Status quo möglich.[32] Leider fehlt es den meisten Aufsichtsbehörden jedoch an Wissen und Methoden, um sinnvoll nachprüfen zu können, ob und wie nationale Nachrichtendienste Daten mit ausländischen Partnern austauschen.[33] Eines der Hauptprobleme dabei ist, dass Nachrichtendienste, wenn sie Daten an ausländischen Partner weitergeben, zumeist die Kontrolle über die spätere Verwendung dieser Daten verlieren.

Dieser Mangel an Kontrolle ist aus mehreren Gründen problematisch. So können beispielsweise die übermittelten Informationen für einen anderen Zweck als den ursprünglich vorgesehenen verwendet werden. Außerdem können

30 Das Konzept der „Collusive delegation“ beschreibt das Demokratiedefizit der internationalen Zusammenarbeit von Regierungen nicht als reines Nebenprodukt des Macht-Transfers, sondern auch als einen der grundlegenden Zwecke dieser Machtverschiebung. Gemäß dieser These können Staaten kooperieren und ihre Autorität bündeln, um innenpolitische Zwänge in den Gesellschaften zu umgehen. Koenig-Archibugi, „International Governance as New Raison d’état? The Case of the EU Common Foreign and Security Policy“, 2004, European Journal of International Relations 10 (2), 147-188.

31 Wetzling und Vieth, 2018, S. 62f.

32 Eine Sammlung an Argumenten für mehr staatliche Verpflichtungen und angemessene Kontrollsysteme für gemeinsame Nachrichtendienstdatenbanken bieten Ryngaert und van Eijk, „International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees“, 2019, International Data Privacy Law 9 (1), https://academic.oup.com/idpl/article/9/1/61/5427456.

33 Positiv zu vermerken sind die im Rahmen des britischen IP Act eingeführten „examination warrants“: Vor der Auswahl der zu prüfenden Inhalte, muss die Regierung eine unabhängige, gerichtliche Genehmigung eines „Investigatory Powers Commissioner“ (Richter) einholen. Dies gilt auch für die Prüfung von Daten, die von ausländischen Nachrichtendiensten weitergegeben werden. Für eine detaillierte Beschreibung siehe: Smith, 2018.

die Daten in die Hände von Sicherheitsbehörden gelangen, die mit deutlich operativeren Befugnissen ausgestattet sind. Wenn ein Nachrichtendienst die Kontrolle über die Verwendung seiner Daten durch Partnerdienste verliert, heißt das nicht, dass die Bürger:innen ihre Rechte verloren hätten oder dass die Aufsichtsbehörden aufhören sollten, die Exekutive zur Rechenschaft zu ziehen. Das aktuelle Nachrichtendienstrecht und die Aufsichtspraxis in vielen Ländern weisen starke Defizite auf, was die effektive und vollständige Überprüfung der Datenweitergabe betrifft.[34]

Idee: Warnmeldung bei riskantem Datenaustausch
Wie bei anderen automatisierten Benachrichtigungen durch Auditsysteme, ist eine Software denkbar, die Protokolldateien nach Aktivitäten durchsucht, die auf einen problematischen Datenaustausch hinweisen. Dazu wären Logdateien erforderlich, die aussagekräftige Informationen über den Datenaustausch enthalten, so dass Datenübertragungen prüfbar werden. Ein kritischer Datenaustausch könnte zum Beispiel gegeben sein, wenn ein Nachrichtendienst eine Datenbank mit einem anderen Dienst bilateral teilt, oder wenn eine Behörde die Daten an eine gemeinsame internationale Datenbank übermittelt, deren Server im Ausland liegen. Einige Aufsichtsbehörden sind bereits verpflichtet, zu prüfen, ob Informationen, die ihr nationaler Dienst mit ausländischen Behörden teilt, den gesetzlichen Anforderungen entsprechen. Diese Art der Datenweitergabe kann sowohl große Datenmengen als auch sensible personenbezogene Daten umfassen.

Eine gründliche Überprüfung kann ergeben, dass bestimmte Kooperationsdatenbanken relevante Datenschutzanforderungen nicht wirksam umsetzen. In Deutschland müssen einige dieser Anforderungen in einer Dateianordnung schriftlich festgehalten werden. Diese Anordnungen können Kontrollen der Einhaltung bestimmter Richtlinien vorschreiben, wie beispielsweise die Ga-

34 Das Unabhängige Gremium ist beispielsweise ermächtigt, stichprobenartig zu überprüfen, ob Daten die gegen das Verbot der Wirtschaftsspionage verstoßen (§ 6 Abs. 5 BND-Gesetz) und solche, die dem nationalen Interesse Deutschlands zuwiderlaufen könnten, weitergegeben werden (§ 15 Abs. 3 BND-Gesetz). Dem Unabhängigen Gremium fehlt jedoch die technische Ausstattung und der Zugriff auf Selektoren und die Datenfiltersysteme, um eine solche Überprüfung adäquat realisieren zu können.
Auch der Bundesbeauftragte für Datenschutz und Informationsfreiheit, der berechtigt ist Datenbanken des BND und die von anderen deutschen Behörden hierhin übermittelten Daten zu prüfen, steht vor einem ähnlichen Dilemma. Das Gesetz bindet den BfDI an mehrere Einschränkungen. Nach § 28 BND-Gesetz darf der BfDI nur gemeinsame Datenbanken überprüfen, die vom BND betrieben werden (§ 27 BND-Gesetz), und auch diese Prüfungen sind eingeschränkt; geprüft werden darf nur der Anteil der Daten, den deutsche Nachrichtendienste hinzugefügt haben. Damit fällt die Mehrheit der gemeinsamen ausländischen Datenbanken, zu denen deutschen Nachrichtendienste erheblich beitragen, sowie die Datenverarbeitung des BND in gemeinsamen ausländischen Datenbanken, nicht in den Aufgabenbereich des BfDI.

rantie, dass eine Informationsweitergabe nicht stattfindet, wenn anzunehmen ist, dass die Daten für Maßnahmen verwendet werden, die mit der freiheitlich demokratischen Grundordnung nicht zu vereinbaren sind, wie z. B. Folter oder die außergerichtliche Überstellung von Terrorverdächtigen.[35] Aufsichtsbehörden, die mit der Überprüfung der Datenverarbeitung beauftragt sind, können dann systematisch kontrollieren, ob eine Datenbank, die von einem nationalen Nachrichtendienst zum Zwecke des grenzüberschreitenden Nachrichtenaustauschs verwaltet wird, den Anforderungen der Dateianordnung entspricht.[36]

Die Aufsichtsbehörden sollten an der Entwicklung von verbesserten Methoden für das Erkennen von (mitunter sehr umfangreicher) Datenweitergabe beteiligt werden, wozu auch die unabhängige Überprüfung der internen Compliance-Prozesse der Nachrichtendienste und deren Umsetzung in den IT-Systemen der Behörden gehören. Dabei sollten die operativen Systeme, die für den Datenaustausch genutzt werden, vor der Übermittlung standardmäßig eine Bestätigung der zulässigen Verwendungszwecke abfragen. Wenn eine Behörde Informationen ausgetauscht hat, die als besonders schutzbedürftig gelten, muss dies dem Empfänger der Informationen mitgeteilt werden. Routinemäßige Audit-Skripte könnten diese Art von besonders kritischen Fällen für eine eingehende Überprüfung durch die Aufsichtsbehörden kennzeichnen. Im besten Fall, könnten die Aufsichtsgremien des Empfängerstaates und die Aufsichtsgremien des übermittelnden Staates eine gemeinsame Kontrolle durchführen. Dies war zumindest bereits eine Forderung, die von der niederländischen Kontrollbehörde CTIVD aufgegriffen wurde.[37]

Nachrichtendienste arbeiten teilweise mit ausländischen Diensten zusammen, die vor einer Missachtung der Menschenrechte nicht zurückschrecken und spezifische Anforderungen ihrer Kooperationspartner einfach ignorieren.[38] Aus diesem Grund verwenden die Niederlande ein System sogenannter Prüfvermerke („weighting notes“), eine Art Eignungsprüfung bei dem das Risiko

35 Perraudin, „Mordaunt pledges to review internal MoD torture guidance“, 20. Mai 2019, https://www.theguardian.com/uk-news/2019/may/20/mordaunt-pledges-to-review-internal-mod-torture-guidance.

36 Siehe z. B. den Bericht der CTIVD über die Datenaustauschinfrastruktur der Counter-Terrorism Group (CTG) bezüglich personenbezogener Daten mutmaßlicher Dschihadisten. CTIVD, „Review report 56 on the exchange of personal data on (alleged) jihadists by the AIVD“, (CTIVD Nr. 56), https://english.ctivd.nl/investigations/r/review-report-56-on-the-exchange-of-personal-data-on-alleged-jihadists-by-the-aivd.

37 Ebd.

38 Der BND arbeitet beispielsweise mit mehr als 450 verschiedenen Nachrichtendiensten weltweit zusammen. Siehe Becker und Schulz, „Wieviel Geheimdienst braucht Deutschland?“, 16. November 2016, https://www.swr.de/film/bnd-schattenwelt-geheimdienst-doku-nachrichtendienst-swr/-/id=5791128/did=17666664/nid=5791128/1o343xj/index.html.

von ausländischen Nachrichtendiensten nach fünf gesetzlich verankerten Kriterien[39] bewertet wird. Um den Nutzen dieser Prüfvermerke zu erhöhen, könnte das Risiko-Level eines ausländischen Nachrichtendienstes dann in strukturierte Metadaten übertragen werden. Prüfer:innen könnten dadurch die Datenweitergabe an Hoch-Risiko-Partner automatisch erkennen und kennzeichnen. Dies wiederum würde eine solide Grundlage für die Planung weiterer Kontrollen, und die systematische Überprüfung besonders riskanter Datenaustausch-Vereinbarungen, bilden. Außerdem wäre es möglich, die detaillierte Überprüfung des Datenaustauschs mit solchen Partnern zu priorisieren.

B3: Kontinuierliche Analyse der Löschprotokolle

Herausforderung

Europäische Nachrichtendienstgesetze schreiben unterschiedliche Speicherfristen für verschiedene Arten von Daten vor. In Frankreich werden ausgewertete Inhaltsdaten von ausländischen Nachrichtendiensten beispielsweise zwölf Monate aufbewahrt, Metadaten hingegen sechs Jahre.[40]

Doch was passiert nach Ablauf der Speicherfrist? Die Datenlöschung stellt nach wie vor eine enorme Herausforderung für Nachrichtendienste und Aufsichtsbehörden dar.[41] Damit Daten endgültig vernichtet werden, müssen die physischen Datensätze auf einem Speichermedium mehrfach mit anderen Daten überschrieben werden. Eine ordnungsgemäße Löschung kann daher teurer, zeitaufwendiger und komplexer werden als die Datenspeicherung selbst. Dennoch müssen Speicherfristen und Löschbestimmungen im nationalen Nachrichtendienstrecht in der Praxis eingehalten werden. Wenn das nicht möglich ist, dann sollte zumindest offen darüber diskutiert werden, warum dies in der Praxis nicht gewährleistet werden kann und welche Garantien und

39 Dazu gehören die „demokratische Einbettung“ der empfangenden Behörde, ihre Professionalität und Zuverlässigkeit, die rechtlichen Befugnisse und Fähigkeiten des Dienstes sowie das gewährleistete Datenschutzniveau. Die „weighting notes“ unterliegen der Überprüfung durch den CTIVD. Siehe Wetzling und Vieth, 2018, S. 26.

40 Für einen Überblick ausgewählter nationaler Gesetzgebungen und ihre Speicherfristen je nach Datenkategorien, siehe Wetzling und Vieth, 2018, S. 56.

41 Wie der BND in jüngster Zeit gegen gesetzliche Bestimmungen zur Vorratsdatenspeicherung verstoßen hat, zeigt ein geheimer Prüfbericht der Bundesdatenschutzbeauftragten: Meister, “Geheimer Prüfbericht: Der BND bricht dutzendfach Gesetz und Verfassung – allein in Bad Aibling (Updates)“, 01.09.2016, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

gesetzliche Vorgaben stattdessen erforderlich sind, um sicherzustellen, dass die Datenspeicherung den Datenmissbrauch nicht erleichtert.[42]

Endet die Speicherfrist einer Datei, erfolgt die Löschung in der Regel automatisiert und ohne einen manuellen Eingriff. Häufig treten jedoch Probleme bei der Datenspeicherung auf, wenn Daten verschiedener Quellen mit unterschiedlichen Speicherfristen durch die Nachrichtendienste zusammengeführt werden. Außerdem ist es denkbar, dass Daten an Orte verschoben werden, wo keine integrierte automatische Löschung vorgenommen wird und sie so möglicherweise nicht gelöscht werden.

Alles in allem erfordert das Prinzip der Rechtsstaatlichkeit und der Zurechenbarkeit des exekutiven Handelns, dass die Aufsichtsbehörden eine größere Rolle bei der Überprüfung der tatsächlichen Löschung von Daten übernehmen. Derzeit herrschen allzu oft Verwirrung und Unwissen über den Verbleib gesammelter Daten, die rechtlich gesehen, schon längst nicht mehr im Besitz der Nachrichtendienste sein sollten.

Idee: Lösch-Statistiken

Moderne Nachrichtendienstgesetze und Datenschutzbestimmungen verlangen von den Diensten, dass sie erfassen, welche Daten gelöscht oder vernichtet werden und zu welchem Zeitpunkt dies geschieht.[43] Die Protokollierung der Datenlöschung ist ein wesentlicher Bestandteil jeder sinnvollen Datenschutzprüfung. Sie folgt einer simplen, binären Logik: Wurden die Daten rechtzeitig gelöscht oder nicht? Das wiederum ist eine ideale Voraussetzung für einen automatisierten Kontrollmechanismus.

Wenn Löschvorgänge systematisch in gut strukturierten Protokolldateien aufgezeichnet werden, können Kontrolleur:innen Muster und Ausreißer im Laufe der Zeit erkennen. Die schwedische Aufsichtsbehörde hat in einem ihrer Berichte angegeben, dass sie statistische Musteranalysen bezüglich

42 Mögliche Lösungen für das Löschproblem könnten die Einführung zweckorientierter Ansätze der Datenspeicherung sein. So verlangt beispielsweise der USA Freedom Act eine regelmäßige Überprüfung der Notwendigkeit der Datenhaltung. Alternativ könnte die Datenlöschung mehrstufig erfolgen, so dass für den Abruf älterer Daten zusätzliche Zugriffsbeschränkungen gelten. Beispielsweise könnten Datensätze vollständig verschlüsselt werden und die Entschlüsselung nach Ablauf der Gültigkeitsdauer könnte dann eine vorherige Genehmigung erfordern.

43 Frankreich beispielsweise hat Gesetze erlassen, die vorschreiben, dass die Löschung gesammelter Informationen, Transkriptionen und Extraktionen nur von eigens hierfür benannten und autorisierten ND-Mitarbeiter:innen durchgeführt werden kann und aufgezeichnet werden muss (Artikel L. 854-6. des französischen Gesetzes Nr. 2015-1556 über die internationale Überwachung).

des Volumens des gelöschten Materials durchführen.[44] Dies unterstützt die Kontrolleur:innen dabei, ihre Ressourcen für vertiefte Untersuchungen gezielt auf verdächtige Ereignisse bei der Datenlöschung zu richten.

Über einen längeren Zeitraum hinweg können Logdateien beispielsweise besondere Löschaktivitäten an bestimmten Tagen, die nicht dem Ende der Aufbewahrungsfrist entsprechen, aufdecken und darstellen. Erlaubt eine Anordnung die Speicherung eines bestimmten Datensatzes für sechs Monate, so mag sich die Frage stellen, warum er vorzeitig bereits nach vier Monaten manuell gelöscht wurde. Führten eventuell die Ankündigungen der Aufsichtsbehörde über geplante Stichproben zu einer „Bereinigung" von Datenbanken? Es ist zwar nicht möglich, alle gelöschten Daten zu überprüfen, doch eine langfristige Übersicht über Löschaktivitäten kann den Aufsichtsbehörden helfen, gezieltere Untersuchungen durchzuführen.

B4: Verwendung von Überwachungsanordnungen besser nachvollziehen

Herausforderung

In einigen Rechtssystemen fallen jedes Jahr eine hohe Anzahl von Anträgen auf Beschränkungen des Fernmeldegeheimnisses an.[45] Die Beurteilung der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit von staatlichen Anträgen auf Überwachungsmaßnahmen stellt einen zentralen Mechanismus der Rechenschaftspflicht dar. Aufsichtsbehörden wie die niederländische TIB, die deutsche G10-Kommission und das britische IPCO sind für die Genehmigung und Beurteilung einer Menge von Anträgen auf Überwachungsmaßnahmen verantwortlich.

Allerdings fehlt diesen Gremien oft ein ganzheitlicher Blick auf die verschiedenen Interaktionen zwischen Diensten, Regierung und Kontrollorganen bei der Beantragung und Umsetzung einzelner Überwachungsmaßnahmen. Sie können die vielen Entscheidungen und Handlungen, die aufgrund eines Antrages anfallen in der Regel nicht nachverfolgen, obwohl das in digitaler Form durchaus vorstellbar wäre. Es steht daher zu befürchten, dass viele

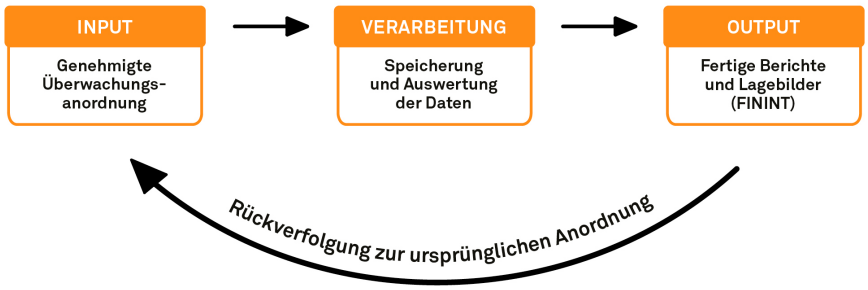
44 Schwedische Kontrollbehörde für die Nachrichtendienste (SIUN), „Årsredovisning för 2017", 22. Februar 2018, Abschnitt 4.1, http://www.siun.se/dokument/Arsredovisning_2017.pdf.

45 So hat die französische Kontrollkommission CNCTR im Jahr 2018 rund 10.000 Rechtsgutachten zu inländischen Abhörbefehlen (basierend auf Nr. I des Artikels L. 852-1 des Codes für innere Sicherheit) sowie über 73.000 Gutachten zu allen Methoden der Nachrichtengewinnung erstellt (siehe: Commission nationale de contrôle des techniques de renseignement, "3. Rapport d'activité 2018," April 2019, S. 62) https://www.cnctr.fr/_downloads/NP_CNCTR_2019_rapport_annuel_2018.pdf)

Aufsichtsbehörden keinen angemessenen Überblick über die zahlreichen bereits bestehenden Überwachungsmaßnahmen haben, wenn sie über die Notwendigkeit einer neuen Maßnahme entscheiden. Ohne eine Systematisierung bestehender Anordnungen und ihrer Umsetzung ist eine Aufsichtbehörde denkbar schlecht aufgestellt, um informiert, und vor allem eigenständig, eine Entscheidung über die Genehmigung weiterer nachrichtendienstlicher Maßnahmen zu treffen.

Darüber hinaus birgt das Genehmigungsverfahren eine weitere große Herausforderung: Einige europäische Nachrichtendienstgesetze verlangen von ihren Regierungen, dass sie eine Begründung für jedes Anordnungsverfahren liefern. Mitglieder der Aufsichtsbehörden haben uns berichtet, dass solche Anordnungen oftmals nur aus einer bestimmten Zahl von Textbausteinen bestehen, Argumente wurden einfach kopiert und eingefügt bzw. sind eher phrasenhaft und ohne inhaltlichen Gehalt formuliert. Sie wiesen daher darauf hin, dass der Fokus der Aufsicht nicht immer auf Abweichungen oder abweichenden Mustern liegen muss. Zumindest wenn es um die Genehmigung von Anordnungen geht, wären die Kontrolleur:innen gut beraten, auch nach übermäßigen Ähnlichkeiten in den Begründungstexten zu suchen. Auch dieser Aspekt der Kontrolle kann durch Automatisierung erleichtert werden.

Idee: Nachverfolgung von Anordnungen



Die digitale Dokumentation von Anträgen und Entscheidungen könnte Aufsichtsgremien in ihren Entscheidungsprozessen unterstützen und dabei helfen, Anträge zu erkennen, die in extremen Ausmaß bestehenden Anordnungen ähneln (mit unklarem Mehrwert) oder dem Mindestmaß an Detailtiefe nicht genügen. Visualisierungen und Statistiken, die diese digitale Dokumentation ergänzen, könnten es den Prüfer:innen ermöglichen, ein genaueres Bild von der Gesamtheit der derzeit laufenden Überwachungsmaßnahmen und den tatsächlichen Prioritäten der Datensammler zu erhalten. Es kann Fälle geben, in denen eine Regierung eine große Anzahl von Maßnahmen beantragt und

nach deren Genehmigung letztlich beschließt, nur wenige davon auch wahrzunehmen. Um diesem Vorgehen entgegenzuwirken, schreibt das französische Nachrichtendienstrecht für einige Überwachungsbefugnisse Quoten vor, die die Anzahl parallel laufender Maßnahmen begrenzen. Auch in diesem Fall scheint eine Nachverfolgung der Genehmigungen notwendig, um überprüfen zu können, ob die französischen Nachrichtendienste diese Quoten auch einhalten.

Eine Möglichkeit Protokolldateien zu analysieren wäre die Einrichtung eines „Genehmigungs-Trackers", der es allen Nutzer:innen (Nachrichtendiensten und Aufsichtsbehörden) ermöglichen würde, Rechtmäßigkeit und Wirksamkeit einer Anordnung anhand eines Vergleichsmaßstabes zu beurteilen. Das einheitliche Kennzeichnen der Datenherkunft ermöglicht es den Aufsichtsbehörden, einen Datensatz auf bestimmte genehmigte oder modifizierte Anordnungen zurückzuverfolgen. Jedes Anordnungsverfahren sollte im System registriert werden, zusammen mit den entsprechenden Metadaten/Kriterien, wie z. B.:

- Verwendungszweck
- an der Umsetzung beteiligte Dritte
- Technische Geräte die zum Einsatz kommen
- Dauer der Anordnung
- Speicherdauer für die erhobenen Daten
- Verwendete Selektoren oder Suchbegriffe
- Arten der Datenverarbeitung, die mit den erhobenen Daten durchgeführt werden sollen
- In- und ausländische Behörden, mit denen die Daten geteilt werden können

Wenn Protokolldateien eine kontinuierliche Kennzeichnung der Datenherkunft beinhalten, können Nachrichtendienste sowie Aufsichtsbehörden die „fertigen Ergebnisse" (FININT) zu konkreten genehmigten Anordnungen zurückverfolgen. Spezifische zusätzliche Bedingungen, z. B. modifizierte Speicherfristen, die im Zuge des Anordnungsverfahrens erlassen wurden, können ebenfalls in Form von Metadaten nachverfolgt werden.

Stärkung der Aufsichtsbehörden durch Rückverfolgung von Anordnungen
Ein Genehmigungs-Tracker könnte zu einem wichtigen Instrument für Aufsichtsgremien werden. Vermutlich besteht innerhalb der Nachrichtendienste bereits ein ähnliches System. Im Idealfall werden die Kriterien einer bestimmten genehmigten Anordnung automatisch als Metadaten in die Informationssysteme der Nachrichtendienste übertragen. Die meisten IT-Systeme folgen

einem standardisierten Metadaten-Katalog oder Metadaten-Handbuch.[46] Bereits das operative Datenmanagement der Nachrichtendienste sollte für Metadaten, die sich aus dem Anordnungsverfahren ergeben, eine Kennzeichnungspflicht schaffen, damit deren Verwendung im Rahmen einer unabhängigen Prüfung sinnvoll nachvollzogen werden kann.

Die für Aufsichtszwecke wichtigsten Metadaten sind wahrscheinlich die Zweckbindung, Zweckänderungen, sowie die Speicherfrist. Die Verfügbarkeit dieser Metadaten könnte auch hilfreich sein, um die Nutzung und Relevanz einer genehmigten Überwachungsmaßnahme im Zeitverlauf zu verfolgen. Kontrolleur:innen könnten dank der Nachverfolgung von Anordnungen messen, welche Datenquellen am häufigsten in der Auswertungsphase verwendet wurden.

Durch die Gegenüberstellung von (a) der Gesamtheit der Daten, für die eine Erfassung beantragten wurde, (b) den tatsächlich gesammelten Daten und (c) der Teilmenge der schlussendlich ausgewerteten Daten, können Kontrolleur:innen die Relevanz und damit auch die Notwendigkeit bestimmter Maßnahmen der Datenerhebung unabhängig mit Hilfe zuverlässiger Informationen beurteilen. Auf diesem Weg könnten sie feststellen, ob Anordnungen überhaupt genutzt wurden oder ob, obwohl bereits eine große Menge an Daten gesammelt wurde, diese anschließend nicht zur Auswertung herangezogen wurden. Das können wertvolle Erkenntnisse für verschiedene Aufsichtsgremien liefern. Vor allem Kontrollorgane, die explizit mit der Überprüfung der Wirksamkeit nachrichtendienstlicher Informationsgewinnung beauftragt sind, wie das belgische Committee I, könnten von einem solchen Instrument enorm profitieren.

C. Strategische Planung durch risikobasierte Priorisierung

Herausforderung

Die Aufsichtsgremien müssen in der Regel eine Reihe wichtiger und komplexer Aufgaben mit begrenzten Ressourcen ausführen. In Deutschland und im Vereinigten Königreich, um nur zwei Beispiele zu nennen, informieren die Aufsichtsbehörden die Öffentlichkeit jährlich über ihre die geplanten Kontrollaktivitäten. Das ist lobenswert, da es Transparenz über die grobe Planung schafft. Wenn jedoch einzelne Mitglieder des Parlamentarischen Kontrollgremiums des Bundestages über bestimmte Themen und Untersuchungen vor dem Plenum

46 Siehe beispielsweise COBIT (Control Objectives for Information and Related Technologies) ein internationaler Standard für Good Practice in der IT-Governance: https://en.wikipedia.org/wiki/COBIT

Bericht erstatten,[47] ist oft unklar, wonach bestimmte Aufsichtstätigkeiten ausgewählt und priorisiert wurden. Handelt es sich um Bereiche, für die erfahrungsgemäß der größte Kontrollbedarf erwartet wird? Wie kommt es zu einer solchen Prognose? Ist dies auf ein erhöhtes Risiko von Missbrauch oder Regierungsvergehen zurückzuführen oder auf die Notwendigkeit, die Aufsicht auf „bisher unerschlossenes Gebiet" auszudehnen? Gegenwärtig sind die Kriterien, aufgrund derer europäische Aufsichtsbehörden den Einsatz ihrer begrenzten Ressourcen bestimmen, nicht ausreichend erkennbar. Vermutlich gibt es noch deutliches Verbesserungspotential, wie begrenzte Ressourcen zielführend eingesetzt werden können.

Instrument: Risikoabschätzung[48]

Die unabhängige dänische Aufsichtsbehörde TET hat einen systematischen Ansatz für die Festlegung und Abfolge von Aufsichtsaktivitäten entwickelt, den andere Gremien kennen sollten.[49] Welche Aufgabe ist am dringlichsten, und warum ist sie erforderlich? Wenn die Kontrolle der Datenverarbeitung durch die Nachrichtendienste vorrangig geprüft werden soll, wie lässt sich dann bestimmen, welche Datenbank für welche Art von Inspektion ausgewählt werden sollte? Um Antworten auf diese und ähnliche Fragen zu erhalten, verwendet das TET eine eigens entwickelte Risikobewertungsmethode, um seine Arbeit zu strukturieren und zu priorisieren. Kontrolleur:innen berechnen für bestimmte Nachrichtendienstsysteme innerhalb ihres Aufsichtsmandats Risikowerte, die ihnen helfen, Art und Zeitpunkt einer Kontrolle zu bestimmen.

Vor der Bestimmung eines Risikowertes für bestimmte nachrichtendienstliche Tätigkeiten – z. B. die Datenerfassung im Ausland durch informationstechnische Eingriffe in fremde Computer (-netzwerke) – bildet TET alle ihm bekannten Datenverarbeitungssysteme ab. Eine solche Übersicht der verschiedenen Speicherorte, Geräte, IT-Systeme und Software mit denen die Dienste Daten sammeln, aufbewahren oder analysieren, ist entscheidend für eine aussa-

47 Siehe z. B. „Unterrichtung durch das Parlamentarische Kontrollgremium (Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes)", 19. Dezember 2013, https://dip21.bundestag.de/dip21/btd/18/002/1800217.pdf, S.6.

48 Unsere Beschreibung der Risikobeurteilung basiert auf den bisherigen Erfahrungen der Aufsichtsbehörde TET mit diesem Instrument, wovon wir uns während des EION-Workshops am 10. Mai 2019 sowie in bilateralen Interviews mit TET-Mitarbeiter:innen einen Eindruck verschaffen konnten. Diese Methode wurde in Anlehnung an ähnliche Modelle aus dem Bereich der Finanzprüfung entwickelt und angepasst.

49 Das dänische TET ist ein unabhängiges, externes Aufsichtsorgan mit vollem Zugriff auf die von den dänischen Nachrichtendiensten verwendeten operativen Systeme. Es besteht aus fünf Mitgliedern und wird von einem Sekretariat mit neun Personen unterstützt. Näheres hierzu: Danish Intelligence Oversight Board, „The Oversight Board", https://www.tet.dk/om-tilsynet/?lang=en.

gekräftige Risikobewertung. Diese Aufgabe stellt an sich schon eine große Herausforderung dar. Darüber hinaus kann es sein, dass die Aufsichtsbehörde Teile der technischen Infrastruktur oder bestimmte Datenerhebungsmethoden überhaupt nicht kennt. Dementsprechend ist die Identifizierung und Verfolgung bisher unbekannter Komponenten ein kontinuierlicher Teil der Aufsichtsarbeit. Alternativ dazu, wie wir in Kapitel 3 weiter ausführen, kann die Risikobewertung auch von den Nachrichtendiensten initiiert werden, wobei in diesem Fall die Aufsichtsbehörden den Prozess streng und regelmäßig beaufsichtigen müssten.

Das dänische TET wendet nach Abschluss der Kartierung aller ihm bekannten und zugänglichen Systeme und Geräte eine Reihe fester Kategorien an, um das Risiko eines jeden Systems und seiner verschiedenen Teilkomponenten zu bewerten. Die folgende Tabelle zeigt die sieben Kategorien einer typischen Risikobewertung des dänischen TET:

Kategorie der Risikobewertung	Mögliche Werte
Aufsichtsbereich	Datenerhebungsverfahren A, B, C; Datenspeicher D, E, F; Datenverarbeitungssysteme H, I, J, etc.
Spezifisches Untersystem	SIGINT Systeme A1, A2, A3, etc.
Rechtsgrundlage	§4 des Gesetzes XYZ
Beurteilung der Wesentlichkeit[50]	„Hoch“ = 2 „Mittel“ = 1 „Niedrig“ = 0 „Unbekannt“ = 2 „N/A“ = 0
Wird die Einhaltung rechtlicher Vorgaben überprüft? [51]	„Ja, einschließlich relevanter Protokollierung“ = 0 „Ja, aber keine relevante Protokollierung“ = 1 „Nein“ = 3 „Unbekannt“ = 3 „N/A“ = 0

50 Unter Wesentlichkeit werden die grundlegenden bzw. entscheidenden Merkmale eines Aufsichtsbereichs erfasst, wie z. B. Art und Umfang der verarbeiteten Daten, die Anzahl der Mitarbeiter:innen innerhalb des Aufsichtsbereichs und die Frage, ob der betreffende Bereich durch automatisierte oder menschliche Prozesse gesteuert wird.

51 Gibt es beispielsweise eine gesetzliche Genehmigungspflicht für operative Tätigkeiten? Wenn ja, wird diese Genehmigung durch „Stop-and-Go“-Prozesse automatisiert, ohne dass eine Umgehung möglich ist? Gibt es ein angemessenes System zur Rechteverwaltung? Gibt es ein System für die Protokollierung der verschiedenen Aktivitäten in diesem Bereich? Wird das Personal entsprechend seiner Aufgaben regelmäßig geschult?

Werden interne Compliance-Prüfungen durchgeführt?	„Ja, zufriedenstellend“ = 0 „Ja, aber nicht zufriedenstellend“ = 1 „Nein“ = 3 „Unbekannt“ = 3 „N/A“ = 0
Haben die internen Compliance-Prüfungen Fehler ergeben?	„Ja, Nichteinhaltung von Rechtsvorschriften“ = 2 „Ja, kleine Fehler“ = 1 „Nein“ = 0 „N/A“ = 0
Hat die Aufsichtsbehörde bereits zuvor eine Prüfung eines bestimmten Systems durchgeführt?	„Ja“ = 0 „Nein“ = 2 „N/A“ = 0
Haben die vorherigen Kontrollen der Aufsichtsbehörde Fehler ergeben?	„Ja, Nichteinhaltung von Rechtsvorschriften“ = 2 „Ja, kleine Fehler“ = 1 „Nein“ = 0 „N/A“ = 0
Haben diese Kontrollen Vermerke hervorgerufen?[52]	„Ja, wesentliche Vermerke“ = 2 „Ja, kleinere Vermerke“ = 1 „Nein“ = 0 „N/A“ = 0

Die Risikowerte werden in vier Risikokategorien eingeteilt:

Risikowert **0–2,9**	**Geringes Risiko** der Nichteinhaltung von Vorschriften
Risikowert **3,0–5,9**	**Begrenztes Risiko** der Nichteinhaltung von Vorschriften
Risikowert **6,0–8,9**	**Mittleres Risiko** der Nichteinhaltung von Vorschriften
Risikowert **9,0–12**	**Hohes Risiko** der Nichteinhaltung von Vorschriften

Alle Systeme (z. B. ein bestimmtes Programm zur Erfassung von Telefon-Metadaten) werden der gleichen Bewertungsmethode unterzogen. Den einzelnen Kategorien werden Werte zugeordnet und in einer Tabellenkalkulation aufgeführt. Der endgültige Risikowert ist ein Zahlenwert zwischen null und zwölf. Er drückt die allgemeine Wahrscheinlichkeit aus, dass eine bestimmte gesetzliche Bestimmung innerhalb eines Aufsichtsbereichs verletzt wird. Im Anschluss wird dann eine detailliertere Risikoanalyse durchgeführt, die zusätzliche

52 Die Vermerke werden für jedes System systematisch aufgelistet, um eine Vergleichbarkeit im Zeitablauf zu gewährleisten. Als Vermerke werden Faktoren erwähnt, die nicht in den Kriterien der Risikobeurteilung erfasst wurden, z. B. die von den Nachrichtendiensten vorgenommene Beurteilung der Informationssicherheit, eine allgemeine Bewertung der IT-Systeme oder ob Betriebssysteme gegebenenfalls überarbeitet oder aktualisiert werden müssen.

Kriterien wie z. B. Erfahrungen aus früheren Untersuchungen, miteinbezieht. In diesem Schritt wird auch der kritische Aspekt der Datenunvollständigkeit berücksichtigt: Das TET versucht zu bewerten, ob es alle relevanten Systeme erfasst hat. Besteht der Verdacht, dass die Kartierung unvollständig ist, wird eine zusätzliche Prüfung veranlasst, um mögliche Ungereimtheiten zu klären.[53]

Die Ergebnisse dienen als Grundlage für die Erstellung des jährlichen Aufsichtsplans, in dem Prioritäten festgelegt werden und der einen Überblick über alle Kontrollprozesse ermöglicht. Die Kontrolleur:innen des TET können daher fundiertere Entscheidungen darüber treffen, in welche Bereiche sie ihre begrenzten Mittel investieren sollen, als viele ihrer europäischen Kolleg:innen.

Risk assessment model - Danish Intelligence Oversight Board				
Area of oversight/process	System	Legislation	Risk score per section 0-2,9 = Low risk 3,0-5,9 = Limited risk 6,0-8,9 = Medium risk 9,0-12 = High risk	Combined risk score 0-2,9 = Low risk 3,0-5,9 = Limited risk 6,0-8,9 = Medium risk 9,0-12 = High risk
Gathering discipline A	SIGINT system A	§ 3 (gathering)	12,0	7,8
		§§ 4-5 (processing)	10,0	
		§ 6 (deletion)	7,0	
		§ 7 (disclosure)	2,0	
		~~§ 8 (legal political activities)~~	N/A	
	SIGINT system B	§ 3 (gathering)	7,0	7,0
		§§ 4-5 (processing)	5,0	
		§ 6 (deletion)	9,0	
		§ 7 (disclosure)	7,0	
		~~§ 8 (legal political activities)~~	N/A	
Gathering discipline B	Collection system A	§ 3 (gathering)	7,0	7,3
		§§ 4-5 (processing)	6,0	
		§ 6 (deletion)	7,0	
		§ 7 (disclosure)	9,0	
		~~§ 8 (legal political activities)~~	N/A	
	Collection system B	§ 3 (gathering)	3,0	3,0
		§§ 4-5 (processing)	2,0	
		§ 6 (deletion)	4,0	
		~~§ 7 (disclosure)~~	N/A	
		~~§ 8 (legal political activities)~~	N/A	

Auszug aus der vom TET verwendeten Kalkulationstabelle zur Bestimmung individueller Risikowerte spezifischer Datenverarbeitungssysteme und kombinierter Risikowerte für nachrichtendienstliche Erfassungstechniken.

53 So können beispielsweise auf sogenannten ‘Altsystemen’ relevante Daten gespeichert sein, die noch nicht auf dem Radar der Aufsicht sind.

Diskussion

Auf Grundlage seiner risikobasierten Einschätzung der eigenen Ressourcen und Kapazitäten kommt das TET zu einer gut informierten und reproduzierbaren Entscheidung darüber, welche nachrichtendienstlichen Aktivitäten innerhalb eines bestimmten Zeitraums überprüft werden sollen.

Von der dänischen Methode profitieren die Aufsicht, die Nachrichtendienste und die breite Öffentlichkeit. Erstens schafft sie einen strukturierten Überblick darüber, was kontrolliert werden könnte und was bereits der Aufsicht unterliegt. Das ist eine wichtige Leistung. Kontrolleur:innen (und, je nach Einstufung, auch die Öffentlichkeit) erhalten ein umfassenderes und präziseres Verständnis für rechtliche Graubereiche von nachrichtendienstlichen Tätigkeiten.

Zweitens liegt in der Bestimmung von Risikowerten bereits eine Chance für die Kontrolleur:innen, sich ein detailliertes und praxisnahes Wissen über die komplexen Sicherheitsbehörden zu verschaffen, die sie beaufsichtigen. Dies wiederum macht sie auf Systeme, Prozesse oder Herausforderungen aufmerksam, von denen sie möglicherweise noch nichts wussten. Drittens trägt dieser Ansatz dazu bei, begrenzte Aufsichtsressourcen effizienter zu nutzen und sowohl die bestehenden Aufsichtslücken, aber auch die geleistete Aufsichtsarbeit transparent und besser nachvollziehbar zu machen.

Viertens ermöglicht die Risikoabschätzung routinemäßige und spezifische Feedbackschleifen, die den Kontrolleur:innen helfen, die Wirksamkeit früherer Inspektionen und Untersuchungen systematisch zu bewerten. Das Modell der Risikobewertung wird ständig angepasst und um neue Informationen ergänzt. Beispielsweise könnten die Kontrolleur:innen die verdachtsunabhängige Überwachung ausländischer Kommunikation dauerhaft als einen Bereich mit hohem Risiko einstufen, der dementsprechend für eine strenge und regelmäßige Überprüfung vorgemerkt wird. Dies kann über einen längeren Zeitraum hinweg dann spezifische Risiken schmälern oder in ein anderes Licht rücken. Ein kontinuierliches Interagieren mit den Diensten und der Fachaufsicht in diesem Bereich ermöglicht den Aufsichtsgremien die Risikowerte zu aktualisieren und zukünftige Untersuchungen auf die aus den Feedbackschleifen gewonnenen Informationen abzustimmen.

Fünftens, je nachdem, wie ein Aufsichtsorgan über seine Aufsichtsinstrumente und -methoden berichtet, könnte sich zudem das Vertrauen der Öffentlichkeit und der Nachrichtendienste in den Einsatz dieser Instrumente verändern. Die Risikobewertung ermöglicht es den Aufsichtsbehörden zu dokumentieren und zu begründen, wie und warum sie bestimmte Aspekte nachrichtendienstlicher

Informationsgewinnung ins Visier nehmen. Die Dienste profitieren auch von dieser Vereinheitlichung und Professionalisierung der Kontrolle, da sie sich auf besser vorbereitete Inspektionen einstellen können. Zudem wird der Öffentlichkeit geholfen besser zu verstehen, welche Kontrollen das Aufsichtsorgan in der Praxis durchführen kann.

Allerdings birgt das dänische Modell auch gewisse Risiken und Nachteile. Zum einen stellt die Berechnung des Risikowertes lediglich eine Annäherung dar und kann noch immer subjektiv ausfallen. Eine verbindliche und nachvollziehbare Dokumentationspflicht sowie Peer-Reviews unter den Kontrolleur:innen könnten dazu beitragen, dieses Problem zu entschärfen.

Zum anderen ermöglicht ein kombinierter Risikowert für sich genommen noch keine allgemeine Schlussfolgerung und kann auch kein vollständiges Bild abgeben. Kontrolleur:innen, die diese Methode anwenden, sollten stets etwaige „blinde Flecken" mitbedenken. Der Risikowert darf nicht die einzige Entscheidungsgrundlage zur Festlegung der Aufsichtsprioritäten sein. Er muss im Kontext betrachtet, mit zusätzlichen Informationen angereichert und von den Aufsichtsbehörden in Frage gestellt werden. Wird beispielsweise der Kategorie „Haben die internen Compliance-Prüfungen Fehler ergeben?" der Wert 0 (keine Fehler) zugewiesen, muss das nicht zwangsläufig bedeuten, dass auch keine Fehler gemacht wurden. Es könnte z. B. auch daran liegen, dass die interne Aufsicht in einer bestimmten Angelegenheit nachlässig oder oberflächlich vorgegangen ist. Ständige Feedback- und Anpassungsschleifen müssen daher in die Risikobewertung einbezogen werden, damit sie als solide und zuverlässige Grundlage für die Erstellung von Arbeitsplänen dienen kann.

Zudem darf die Transparenz der Risikobewertungsmethode die Aufsichtsinspektionen nicht allzu berechenbar machen. Es müssen weiterhin Kapazitäten für unangekündigte Kontrollen bestehen, da sich die Nachrichtendienste sonst möglicherweise an die risikobasierte Planung der Aufsichtsbehörden anpassen. Das würde deren Wirksamkeit beeinträchtigen. Andererseits sind die Aufsichtsgremien aber auch auf die Kooperationsbereitschaft der Nachrichtendienste angewiesen. Eine klare Kommunikation über Kontrollmethoden und -präferenzen ist hier von Vorteil, um das offene und zielführende Interagieren zwischen Kontrollierenden und Kontrollierten zu befördern. In Anbetracht dessen sollten sich vorhersehbare und unvorhersehbare Aufsichtsaktivitäten die Waage halten. Ein risikobasierter Arbeitsplan könnte mit spontanen, unangekündigten Prüfungen und Inspektionen kombiniert werden.

Insgesamt steckt in der dänischen Methode ein probates Mittel, um die Effizienz und die Wissensbasis der Aufsichtsbehörden deutlich zu verbessern.

Stärkung der Aufsichtsorgane durch strategische Ressourcenzuweisung
Um diesen Ansatz in die Praxis umzusetzen, müssen die Aufsichtsbehörden einen kontinuierlichen Dialog mit den Nachrichtendiensten und den Ministerien führen, um die Datenverarbeitungssysteme so genau wie möglich erfassen und kartieren zu können. Nachrichtendienste führen wahrscheinlich zudem parallel ihre eigenen Risikobewertungen durch. Beide Maßnahmen können nebeneinander bestehen und/oder ineinander übergreifen: Die Aufsichtsbehörden können eine Art „Sorgfalts-Prüfung" der internen Risikobewertungen der Nachrichtendienste durchführen. Jedoch sollten sich die Aufsichtsbehörden nicht auf eine rein passive Nachprüfung beschränken. Selbst wenn der Prüfungsumfang anfangs noch begrenzt sein mag, sind Aufsichtsbehörden, die ihre eigene Risikobewertung durchführen, im Vorteil. Je genauer die anfängliche Kartierung vorgenommen wird, desto effektiver können die begrenzten Ressourcen zum Einsatz kommen. Die Aufsichtsbehörden müssen sich dafür einsetzen, dass Risikobewertungen und Feedbackschleifen Standardverfahren werden. Mindestens eine (idealerweise mehrere) Personen mit Führungsverantwortung sollten für deren Durchführung verantwortlich sein.

D. Regelmäßiger Austausch mit den Telekommunikationsanbietern

Herausforderung
Die Interaktion zwischen Nachrichtendiensten, Regierungen und privaten Dienstleistern ist für die Durchführung moderner Überwachung von zentraler Bedeutung. Für die meisten Aufsichtsbehörden ist diese Interaktion nicht, oder nur unzureichend, einsehbar. Dass Nachrichtendienste eigene technische Ausrüstung bei den Dienstleistern installieren und manchmal eigene, separate Räume und Einrichtungen auf dem Gelände eines Internetanbieters unterhalten, sollte Kontrolleur:innen regelmäßig Anlass geben, diesen Betrieb kritisch zu überprüfen. Kontrollbehörden sollten ein fundiertes Verständnis für das Risiko kreativer Rechtsauslegungen und fehlerhaft oder unzulässig installierter technischer Ausrüstung entwickeln und laufend erneuern. Allein schon ein besserer Überblick über das technische Missbrauchspotenzial kann dazu beitragen, dass Kontrolleur:innen aktiv die Einhaltung der gesetzlichen Vorgaben befördern können.

In der Privatwirtschaft spricht man von „Maverick-Buying" („wilder Einkauf"), wenn ein Angestellter eigenmächtig und außerhalb des Beschaffungsprozesses Waren einkauft. Das ist zum Beispiel der Fall, wenn ein Mitarbeiter ohne (oder mit zu später) Einbeziehung der für den Einkauf zuständigen Abteilung Produkte bestellt. Diese Aktivitäten gelten meist nicht als illegales Verhalten

und es kann gute Gründe geben, bestimmte Schritte des offiziellen Beschaffungsprozesses im Ausnahmefall zu umgehen. Tritt „Maverick-Buying" jedoch wiederholt oder systematisch auf, kann dies schwerwiegende Auswirkungen auf die finanzielle Stabilität eines Unternehmens haben. Aus diesem Grund ist die Rückverfolgung eigenmächtiger Einkäufe eine Standard-Kontrollaktivität in der Finanzprüfung.

Überträgt man das Konzept des „Maverick-Buying" auf den Bereich der Datenerfassung von Nachrichtendiensten, könnte zum Beispiel eine unbefugte Sammlung von Kommunikationsdaten über einen Mobilfunkanbieter oder die unsachgemäße Installation von Überwachungstechnik zur Ausleitung von Daten aus dem Backbone-Glasfasernetz als ein solches Verhalten gelten. Wie können Aufsichtsbehörden diese Art der unzulässigen Datenbeschaffung erkennen und stoppen?

Idee: Dialog zwischen Kontrollgremien und Dienstanbietern
Ein verbesserter und regelmäßiger Austausch zwischen Aufsichtsbehörden und Kommunikationsdienstleistern, die relevante Daten weiterleiten oder speichern, könnte dazu beitragen, die Wissensbasis zu erhöhen und etwaiges Fehlverhalten zu erkennen. Vor allem für große Internetdienstanbieter, die zahlreiche Übermittlungsanordnungen erhalten, wären derartige bilaterale Treffen wahrscheinlich ein effizienter Ansatz. Zusätzlich zu diesen Treffen könnte ein breiteres, multilaterales Forum für Aufsichtsbehörden eingerichtet werden, das auch kleinere Unternehmen einschließt, die nur gelegentlich von Anordnungsverfahren der Regierung betroffen sind.[54]

Diskussion
Um wirksame Kontrollen durchführen zu können, müssen die Aufsichtsbehörden genau über den Prozess der Datenerhebung informiert sein. Dies gilt sowohl für Aufsichtsbehörden, die die juristische Kontrolle von Anordnungen durchführen als auch für Gremien, die eine nachsorgende Datenschutzkontrolle durchführen. Einige Aufsichtsbehörden haben bereits direkte Beziehungen zu Internetdienstanbietern (oder Postbetreibern, Mobilfunkbetrei-

54 In Großbritannien fungiert das Technical Advisory Board (TAB) als Plattform für den Austausch zwischen Nachrichtendiensten und Unternehmen. Das TAB besteht aus sechs Vertreter:innen der Kommunikationsbranche (O2, British Telecom, Vodafone usw.), sechs Vertreter:innen der überwachenden Behörden und Diensten, sowie einem Vorsitzenden, der direkt an das Innenministerium berichtet. Siehe www.gov.uk/government/organisations/technical-advisory-board. Es sind jedoch keine (unabhängigen) Vertreter:innen der Aufsicht direkt beteiligt. In Frankreich hat die Regulierungsbehörde für elektronische Kommunikation (ARCEP) das Recht, eines der neun Mitglieder des Kontrollgremiums CNCTR zu benennen, welches über „umfangreiche technische Kenntnisse der elektronischen Kommunikation" verfügt. Diese Person ist derzeit ein Vertreter der Telekommunikationsindustrie und könnte auch die Verbindung zwischen Aufsicht und Industrie stärken.

bern, Kommunikationsdienstanbietern usw.) etabliert. Als Ergänzung zu den eingangs beschriebenen technischen Möglichkeiten zur Optimierung der Kontrolle, sollten auch der regelmäßige und strukturierte Austausch zwischen Aufsichtsgremien und Telekommunikationsanbietern europaweit ausgebaut werden.

Einige Dienstleister haben Ungereimtheiten bei der Umsetzung von Überwachungsanordnungen angemahnt. Auch sie haben Bedarf an Rechtssicherheit und Rechtsstaatlichkeit. So hat beispielsweise der deutsche Internet-Exchange-Provider DE-CIX vor dem Bundesverwaltungsgericht einige Übermittlungsanordnungen im Rahmen der strategischen Fernmeldeaufklärung angefochten.[55] Das Gericht entschied, dass die Vorwürfe des Unternehmens formal unzulässig waren. Die Bundesrichter:innen erklärten aber auch, dass die fraglichen Anordnungen zu viel Spielraum in ihrer Umsetzung lassen.[56] Auch das britische Nachrichtendienstrecht lässt einen sehr großen Ermessensspielraum bei der Umsetzung von Übermittlungsanordnungen: Anordnungen können dort alle Handlungen autorisieren, die erforderlich sind, um dem Antrag genüge zu tun, einschließlich „dem Abhören von Kommunikation, die nicht explizit in der Anordnung genannt wird“ oder „das Extrahieren von Sekundärdaten aus solcher Kommunikation“.[57] Nach britischem Recht sind die Betreiber verpflichtet, Missstände, wie z. B. ein fehlerhaftes Abfangen oder einen Fehler bei der Datenweitergabe, an IPCO und die betreffende Sicherheitsbehörde zu melden.[58]

Ein konstruktiver Dialog zwischen Aufsichtsbehörden und privaten Anbietern wäre für beide Seiten von großem Nutzen: Die Aufsichtsbehörden könnten dank

55 Pressemitteilung des Bundesverwaltungsgerichts, „Klage der DE-CIX Management GmbH erfolglos“, 31. Mai 2018 (38/2018), https://www.bverwg.de/pm/2018/38.

56 Die mündliche Verhandlung vor dem Bundesverwaltungsgericht hat zum Beispiel gezeigt, dass die nach dem G10-Gesetz erlassenen Anordnungen nicht eindeutig bestimmen, welche Glasfaserkabel mit welcher Methode abgefangen werden müssen. Stattdessen sendet der BND separate E-Mails an den Internetanbieter mit der Angabe der konkreten Ports, die abgehört werden sollen, und den Geräten zur Ausleitung des Datenstroms.

57 Gezielte Abhöranordnungen werden in Abschnitt 15(5) des IP Act geregelt http://www.legislation.gov.uk/ukpga/2016/25/section/15/enacted (eigene Übersetzung); siehe außerdem Investigatory Powers Act 2016: „Explanatory Notes“, § 67, http://www.legislation.gov.uk/ukpga/2016/25/section/67/enacted.

58 In § 235 (6) des IP Acts heißt es, dass eine Behörde, ein Telekommunikations- oder Postbetreiber dem Investigatory Powers Commissioner alle relevanten Fehler melden muss (im Sinne des § 231 Abs. 9). Ein „relevanter Fehler“ gemäß § 231 (9) bedeutet einen Fehler (a) einer Behörde bei der Einhaltung von Anforderungen, die ihr durch dieses Gesetz oder einen anderen Erlass auferlegt werden und die der Überprüfung durch einen Judicial Commissioner unterliegen und (b) einer Beschreibung für diesen Zweck in den Praxisrichtlinien nach Anhang 7 unterliegen, Investigatory Powers Act 2016, www.legislation.gov.uk/ukpga/2016/25/section/235/enacted, (eigene Übersetzung).

der Informationen, die sie im Rahmen des Austausches erhalten vermutlich besser nachvollziehen und überprüfen, wie die Datenerhebung in der Praxis umgesetzt wird. Die Kommunikationsdienstleister hätten den Vorteil bei unklaren Rechtsfragen nicht allein mit der Exekutive im Austausch zu stehen und könnten etwaige Missstände auf direktem Weg gegenüber den Kontrolleur:innen zur Sprache bringen. Auch die Nachrichtendienste würden davon profitieren, wenn Aufsichtsbehörden ein klareres Bild vom Geschehen haben und sich die Fragen der Kontrolleur:innen auch mit Blick auf die Interaktion zwischen Nachrichtendiensten und Internetanbietern professionalisieren.

3. Reformagenda für datenbasierte Aufsicht

Das vorherige Kapitel stellte sieben Kontrollinnovationen vor, die unserer Meinung nach größere Aufmerksamkeit verdienen. Sie sollten Teil einer ambitionierten Reformagenda für eine wirksamere Nachrichtendienstkontrolle werden. Die von uns diskutierten Instrumente bauen auf bekannten Ideen auf: Häufig haben wir uns von bereits bestehenden Praktiken in anderen Politikbereichen und von Ergebnissen des kollaborativen Arbeitsprozesses im European Intelligence Oversight Network (EION) inspirieren lassen.[59]

Einige Kontrolleur:innen haben das wegweisende Potenzial der datenbasierten Aufsicht erkannt. Dennoch kratzen die meisten europäischen Aufsichtsgremien beim Ausschöpfen der damit verbundenen Möglichkeiten zumeist immer noch nur an der Oberfläche. Unterstützung verdient der Vorstoß einer Gruppe von sechs Aufsichtsbehörden, die gemeinsam ein neues Projekt initiiert haben, das sich auf „(1) die Entwicklung von Aufsichts- und Prüfstandards und (2) Innovationen im Aufsichtsbereich konzentrieren wird".[60]

Wie bereits erwähnt, gibt es noch eine Reihe potenzieller Fallstricke bei der Konzeption und auch bei der Implementierung datenbasierter Kontrolltechniken. Diese sollten von den Praktiker:innen der Nachrichtendienstkontrolle, den Abgeordneten, der unabhängigen Zivilgesellschaft und natürlich auch von den Vertreter:innen der Regierungen gründlich eruiert werden, bevor Veränderungen im Nachrichtendienstrecht beziehungsweise in der Kontrollpraxis vorgenommen werden. Hierfür möchte dieses Kapitel eine Diskussionsgrundlage schaffen.

3.1 Mögliche Einwände aus Sicht der Exekutive

Kernbereich der exekutiven Eigenverantwortung
Vorgebracht wird mitunter, dass der direkte Zugang und neue Ideen für Kontrolltechniken zwar grundsätzlich willkommen sind, diese aber den Kontrollinstitutionen innerhalb der Dienste oder der Fachaufsicht vorbehalten sein sollten, sprich dem Bundeskanzleramt für den Bundesnachrichtendienst, dem Bundesministerium des Innern, für Bau und Heimat für das Bundesamt

59 European Intelligence Oversight Network (Europäisches Netzwerk Nachrichtendienstkontrolle), „Workshop on control tools", Stiftung Neue Verantwortung 10. Mai 2019, https://www.stiftung-nv.de/sites/default/files/agenda_second_eion_workshop_10052019.pdf.

60 De Ridder, „A simple yet existential demand: let oversight bodies work together", November 2019, https://aboutintel.eu/simple-oversight-demands/, (eigene Übersetzung).

für Verfassungsschutz und dem Bundesministerium der Verteidigung für den Militärischen Abschirmdienst. Dieser Position liegt die Sorge zugrunde, dass der direkte Zugriff auf operative Systeme und der Einsatz leistungsstarker Kontrollinstrumente durch unabhängige Aufsichtsbehörden den grundsätzlich nicht ausforschbaren Initiativ-, Beratungs- und Handlungsbereich der Exekutive zu stark begrenzt. Vertreter:innen dieser Position verweisen auf das vom Bundesverfassungsgericht begründete Prinzip des Kernbereichs exekutiver Eigenverantwortung um einen umfassenden Zugriff unabhängiger Kontrolleur:innen auf Datenbanken und IT-Systeme zu verneinen. Einige der in diesem Papier vorgestellten Ideen (wie z. B. Warnmeldungen bei riskantem Datenaustausch und eine konsequente Nachverfolgung der Überwachungsanordnungen) mögen diesem Prinzip entgegenstehen. Demnach würde der Kernbereich besonders in sensiblen Bereichen der Sicherheitspolitik benötigt, um Gefahren für die äußere und innere Sicherheit zu begegnen oder die Handlungsfähigkeit der Bundesrepublik zu wahren. Da es den Kontrollgremien nicht obliegt, die Sicherheit der Bundesrepublik zu gewährleisten, sollten sie auch an Entscheidungsprozessen beteiligt werden.

Um diesen Punkt weiter zu veranschaulichen, verweisen einige Beobachter:innen auf die Stellung der Bundeswehr als *Parlamentsarmee*. Hier übt der Bundestag eine direkte Haushalts- *und* Einsatzkontrolle über die Bundeswehr aus. Für die Steuerung der Nachrichtendienste sei dieser Ansatz aber unpraktikabel. Wollte der Souverän dies ändern, müsste er zunächst einen *Parlamentsnachrichtendienst* schaffen, was Änderungen der Bundes- und Landesverfassungen voraussetzen würde. Zudem hat das Bundesverfassungsgericht den Grundsatz der exekutiven Eigenverantwortung in seiner Rechtsprechung zwar im Einzelfall eingeschränkt, aber es hat gleichwohl wiederholt betont, dass der Regierung grundsätzlich ein unausforschbarer Raum für Beratungen eingeräumt werden muss. Dieses Argument sollte aber in seinem Kontext betrachtet werden. Wie der wissenschaftliche Dienst des Bundestages ausgeführt hat „existiert (...) kein absoluter Kernbereich der Exekutive, wie auch kein allumfassender Informationsanspruch des Parlaments."[61] Vielmehr gelte der Grundsatz, dass das parlamentarische Informationsinteresse gewichtiger sein müsse, je weiter das Begehren in den Kernbereich der Regierung vordringe. Weiter halten die Gutachter:innen fest: „Das Informationsinteresse ist besonders

61 Wissenschaftliche Dienste des Deutschen Bundestages, „Der Kernbereich exekutiver Eigenverantwortung", 10.11.2006, S. 3, https://www.bundestag.de/resource/blob/412760/1e98af44462dee55fd1ee3925501dbf4/wd-3-383-06-pdf-data.pdf.

gesteigert, soweit es der Aufklärung von Missständen und Rechtsverstößen innerhalb der Regierung dient."[62]

Das sogenannte Privileg der Exekutive wird in Europa aufgrund vielfältiger konstitutioneller und soziokultureller Unterschiede in Theorie und Praxis unterschiedlich ausgelegt. In Deutschland ist gegenwärtig mit starkem Widerstand zu rechnen, wenn es um die Weiterentwicklung der Kontrolle durch umfassenderen Zugang und moderne, datenbasierte Kontrollinstrumente für unabhängige Kontrollgremien geht. In anderen europäischen Ländern scheint dieses Argument weniger Einfluss zu haben. Betrachten wir zum Beispiel das dänische Aufsichtsgremium TET: Trotz seines Status als unabhängige Institution haben die Mitglieder und Mitarbeiter:innen direkten Zugriff auf Protokolldateien und operative Systeme der dänischen Dienste. Darüber hinaus verfügt es über deutlich modernere Kontrollinstrumente als die deutschen Kolleg:innen.[63]

Gefahr für die Unabhängigkeit?

Andererseits besteht auch weiterhin die Gefahr der Befangenheit, die durch zu große Nähe zwischen den Kontrolleur:innen und den Kontrollierten entstehen kann. Verwaltungswissenschaftler:innen bezeichnen dieses Phänomen als *regulatory capture*. Die Kontrollgremien müssen daher stets darauf achten, ihre Eigenständigkeit und ihre Rolle als externes Korrektiv gegenüber den Regierungen und Nachrichtendiensten zu wahren, die über ein Vielfaches an Ressourcen verfügen. Aufsichtsbehörden sollten daher stets einen Moment

62 Ebd., S. 11.

63 Die institutionelle Ausgestaltung und Mandate der Aufsichtsbehörden variieren von Land zu Land. Einige Länder, wie das Vereinigte Königreich und Dänemark, haben ihren Nachrichtendiensten weitaus größere Überwachungsbefugnisse eingeräumt als andere. Dementsprechend ist das Bedürfnis einer leistungsfähigen Kontrolle in diesen Ländern möglicherweise ebenso erhöht. Auch ist denkbar, dass Aufsichtsbehörden umfassendere Kontrollmandate und Zugangsrechte erhalten haben, weil ihre Einrichtung als Expertengremien eine größere faktische Nähe zur Exekutive bedeutet. Interessanterweise scheint diese Argumentation nicht für das Unabhängige Gremium und die G10-Kommission zu gelten. Diese unterliegen stärkeren Zugangsbeschränkungen als die fünf europäischen Aufsichtsbehörden, die die Gemeinsame Erklärung von Bern unterzeichnet haben, siehe „Strengthening oversight of international data exchange between intelligence and security services", https://eos-utvalget.no/wp-content/uploads/2019/05/joint_statement_for_publication_20181114_final_endelig.pdf. Und das obwohl das Unabhängige Gremium eher einem administrativen Aufsichtsgremium entspricht und auch als solches in der Literatur und Rechtsprechung diskutiert wird. Siehe z. B. Graulich, „Reform des Gesetzes über den Bundesnachrichtendienst, https://kripoz.de/2017/01/15/reform-des-gesetzes-ueber-den-bundesnachrichtendienst-ausland-ausland-fernmeldeaufklaerung-und-internationale-Datenkooperation/, oder auch: Bundesverfassungsgericht, „G 10-Kommission ist im Organstreitverfahren nicht parteifähig und scheitert daher mit dem Antrag auf Herausgabe der NSA-Selektorenliste" 14. Oktober 2016 (72/2016), https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/bvg16-072.html;jsessionid=7E07882B3FF5229720E12BEF0CB9498E.1_cid370.

der Zufälligkeit und der Unvorhersehbarkeit im Kontrollbetrieb einsetzen und eigenständig über den Verlauf von Kontrollen und die für die Untersuchungen nötige Ausrüstung bestimmen können. Nicht nur in der Theorie sondern auch in der Praxis muss allen Beteiligten klar sein, dass es eine Grenze zwischen Kooperation und Komplizenschaft gibt, die nicht überschritten werden darf. Deshalb sollten die Kontrolleur:innen zwar eine kooperative Beziehung zu den Kontrollierten pflegen, dabei aber auch im eigenen Interesse die kritische Distanz zu den Nachrichtendiensten und den zuständigen Regierungsstellen wahren. Das schirmt sie dann gegebenenfalls auch vor dem Risiko ab, für Missstände oder die Nichteinhaltung gesetzlicher Vorgaben mitverantwortlich gemacht zu werden. Aufsichtsgremien können und sollen die Arbeit der Verwaltungsleitung, der Grundsatzreferate, der internen Datenschutzkontrolleur:innen und der internen Abteilungen der Dienst- und Fachaufsicht nicht ersetzen. Vielmehr müssen die Aufsichtsbehörden dafür streiten, dass die Nachrichtendienste neue Systeme so gestalten, dass sie überprüfbar bleiben. Dies wird nicht möglich sein, wenn die Kontrolleur:innen davor zurückschrecken, während der Planungsphase mit Regierungsmitarbeiter:innen zusammenzuarbeiten, weil sie befürchten, dass ihnen bei Skandalen oder Unregelmäßigkeiten im Nachhinein die Hände gebunden wären. Die Erfahrungen aus Ländern wie Dänemark und den Niederlanden zeigen, dass es sehr wohl möglich ist, die Exekutive bei Bedarf zu beraten, ohne die Unabhängigkeit der Aufsicht zu beeinträchtigen. Hier stehen viele mögliche Modelle im Raum, wie zum Beispiel die Ausweitung des BfDI-Mandats auf den G10-Bereich und eine strikte behördliche Trennung zwischen nachsorgenden Datenschutzkontrollen durch den BfDI und das Antragsverfahren im Vorfeld einer Überwachungsmaßnahme durch die G10-Kommission und ggf. das Unabhängige Gremium.

Direkter Zugang – ein Alptraum für die IT-Sicherheit?

Ein weiterer Punkt in der Debatte sollte sein, dass ein besserer Zugang mehr Verantwortung nach sich zieht. IT-Sicherheit stellt in diesem Zusammenhang eine Herausforderung dar, wenn es darum geht, Kontrolleur:innen einen besseren elektronischen Zugriff auf Betriebssysteme und Datenbanken zu gewähren.[64] Die Verwaltung einer elektronischen Schnittstelle würde, so argumentieren einige Kritiker:innen, einen zusätzlichen Angriffspunkt für Ausforschung, Cyberkriminalität oder Sabotage liefern. Derzeit seien Aufsichtsbehörden bei weitem nicht ausreichend ausgestattet und ausgebildet, um einen eigenen

64 Die kürzlich durchgeführte Sicherheitsbewertung des österreichischen Inlands-Nachrichtendienstes BVT veranschaulicht einige gemeinsame Sicherheitsbedenken, wie die physische Sicherheit von Einrichtungen und die Risiken einer digitalen Infiltration (durch vernetzte Systeme). Siehe hierzu Schmitt, „Alarm: Verfassungsschutz BVT steht total blamiert da“, 11. November 2019, https://m.oe24.at/oesterreich/politik/Alarm-Verfassungsschutz-BVT-steht-total-blamiert-da/405465583.

Zugang zu diesen sicherheitsrelevanten Daten in angemessener Weise vor solchen Risiken zu schützen. Dies würde zusätzliche Investitionen erfordern.

Die Praxis in den Niederlanden, der Schweiz und in Norwegen zeigt, dass Aufsichtsbehörden derartige Schnittstellen durchaus gegen Angriffe und Spionage härten können. Das Personal, das direkt operative Systeme nutzt, muss ebenso gut ausgebildet sein und die gleichen Sicherheitsstandards einhalten wie Regierungsmitarbeiter:innen. Wenn ein vergleichbar hohes Schutzniveau gegen Missbrauch oder Datenverlust vorhanden ist, sind Kontrolleur:innen nicht anfälliger für Hackerangriffe als Regierungsstellen. Angesichts der enormen Summen, die für moderne Überwachungs- und Aufklärungstechnik ausgegeben werden, sollten Demokratien deutlich mehr Mittel zur Verfügung stellen, um Aufsichtsbehörden im Bereich der IT-Sicherheit auf den aktuellen Stand zu bringen.

Unnötige Redundanz

Ein überzeugenderes Argument, zumindest unserer Auffassung nach, liefern diejenigen, die vor dem unnötigen Verwaltungsaufwand warnen, wenn die gleichen Prüfungen auf dem gleichen Datensatz doppelt stattfinden. Moderne Nachrichtendienste und die Fachaufsicht-Referate in den Ministerien führen ihrerseits eine Reihe von Audit-Aufgaben durch. Dort wird die Datenerfassung und -verarbeitung unter anderem auch auf ihre Effektivität und Legalität hin untersucht. Sollten unabhängige Aufsichtsbehörden ihrerseits Kontrollinstrumente von Grund auf neu entwickeln, würde dies viele der ohnehin schon knappen Ressourcen in Anspruch nehmen, und unter Umständen Zeit und Geld vergeuden. Da andere Institutionen innerhalb der Exekutive schon über datenbasierte Aufsichtsinstrumente verfügen, lautet ein Vorschlag, dass die externen Kontrollorgane vielmehr dazu beitragen sollten, diese zu optimieren und den sorgfältigen und akkuraten Einsatz dieser Instrumente zu kontrollieren. In Anbetracht dessen, sollte eine Reform der Kontrollstrukturen den spezifischen Mehrwert der Maßnahmen beachten und unnötigen zusätzlichen Arbeitsaufwand vermeiden.

Es gibt stichhaltige Punkte für dieses Argument. Wir sind uns bewusst, dass einige der von uns vorgeschlagenen Instrumente leichter umgesetzt werden können als andere (siehe Abschnitt unten). Generell ist eine engere Zusammenarbeit zwischen unabhängigen Kontrollorganen und der Exekutive erforderlich. Eine Reform der Kontrollaufsicht sollte versuchen, Synergien zu nutzen und Ressourcen so gut wie möglich zu kumulieren. Dies erfordert, dass die Regierungen bereit sind, mit einer unabhängigen datenbasierten Nachrichtendienstkontrolle zusammenzuarbeiten. Es wäre ein Trugschluss, alle Arten des modernen Auditing ausschließlich der Exekutive zu überlassen. Uns ist indes

nicht ganz klar, ob im Bereich der Fachaufsicht überhaupt schon ausreichend mit datengesteuerter und automatisierter Kontrolltechnik gearbeitet wird.

Die Kontrollgremien sollten von Seiten der Zivilgesellschaft jedenfalls ermutigt werden, die Daten, die sie von den Diensten erhalten, unabhängig zu untersuchen und mit eigenen Mitteln zu testen – auch wenn dies mitunter darauf hinausläuft, dass bestimmte Tätigkeiten einer doppelten oder ähnlich gelagerten Kontrolle unterliegen. Das bleibt unverzichtbar, um ein Überraschungsmoment aufrechtzuerhalten und *regulatory capture* zu vermeiden. Die bloße Teilnahme an reaktiver Nachsorge würde bedeuten, dass viele praktische Erkenntnisse, die die Kontrolleur:innen durch proaktives Prüfen gewinnen, ungenutzt verloren gingen.

Unabhängige Aufsichtsbehörden seien nicht vertrauenswürdig
Mancherorts wird die Integrität und die Zuverlässigkeit der Kontrollgremien in Frage gestellt. Weitergehende Zugangsmöglichkeiten und effektivere Werkzeuge für die Aufsichtsbehörden würden, so die Befürchtung, das Risiko erhöhen, dass eingestuftes Material in den öffentlichen Raum gelange. In dieser allgemeinen Form können wir diese Sorge nicht teilen. Vielmehr sollte man das Risiko natürlich mitbedenken und gegebenenfalls einzelne Fallkonstellationen prüfen. Theoretisch könnten natürlich eingestufte Informationen durch Mitglieder parlamentarischer Aufsichtsgremien weitergegeben werden. Häufig konnte man jedoch in Untersuchungen vermeintlicher Lecks im Nachgang aber keinen Schuldigen ausmachen. Zudem sind Exekutivorgane im Übrigen auch in der Lage, den Medien gezielte Informationen durchzustechen. Besonders hervorzuheben ist hierbei, dass keine Fälle bekannt sind, wo seitens der Gremien der juristischen Kontrolle eingestufte Informationen unerlaubterweise an Dritte weitergegeben wurden.

Diese verschiedenen Bedenken und Anliegen verdienen mehr Aufmerksamkeit und sollten in Zukunft noch eingehender erörtert werden. Die vorangegangene Diskussion zeigt, dass den Argumente, die gegen eine technologiegestützte Kontrollinnovation sprechen, mindestens so viele Argumenten gegenüberstehen, die dafür sprechen und aus unserer Sicht überzeugender sind. Gerade mit Blick auf die bereits begonnenen Schritte in einzelnen Ländern lässt sich die praktische Machbarkeit und der Mehrwert von datengesteuerten Kontrollinstrumente für unabhängige Aufsichtsbehörden kaum in Abrede stellen.

Länder, die ihren Aufsichtsbehörden direkten Zugang zu den Informationssystemen gewähren und datengestützte Kontrollinstrumente einsetzen, sind auf dem richtigen Weg. Wir brauchen jetzt eine breitere öffentliche Diskussion, um sie auf Ihrem Weg zu unterstützen und Nachzügler zu motivieren.

Angesichts der Vielzahl von Optionen für eine verbesserte Kontrolle, die wir in diesem Papier diskutiert haben, können wir uns nur schwer vorstellen, wie ein effektives Kontrollmandat für unabhängige Aufsichtsgremien zukünftig gerechtfertigt sein soll, wenn es ohne den direkten Zugang zu den Systemen und Datenbanken der Nachrichtendienste auskommen muss.

Die zunehmende Diskrepanz zwischen High-Tech-Aufklärung und Low-Tech-Aufsicht stellt eine große Gefahr für unsere Demokratien dar. Es braucht daher dringend mehr Anstrengungen, um die Kontrolle zu modernisieren und zu professionalisieren.

Wer sollte die Instrumente einsetzen?

Die Ideen, die wir im vorherigen Kapitel vorgestellt haben, erfordern unterschiedliche Formen der Zusammenarbeit und Vernetzung zwischen Kontrollgremien und Nachrichtendiensten. Einige Ideen können vermutlich nur realisiert werden, wenn die Dienste die notwendige Infrastruktur und Daten dafür bereitstellen. Es liegt nahe, dass einige Instrumente bereits von Nachrichtendiensten eingesetzt werden, da dies zur Einhaltung grundlegender Rechtsvorschriften erforderlich scheint. Wichtig wäre es daher, diese Instrumente (z. B. die Suche nach Missbrauchs-Mustern in Protokolldaten) dann direkt in die operativen Prozesse und die Informationsinfrastruktur der Dienste zu integrieren. Andererseits dürfen unabhängige Aufsichtsbehörden, wie eingangs ausgeführt, nicht Gefahr laufen, die kritische Distanz zu den Nachrichtendiensten zu verlieren oder gar von diesen in ungebührlicher Weise abhängig zu werden. Die folgende Grafik zeigt, wie die im dritten Kapitel vorgestellten Instrumente aus unserer Sicht in der Praxis mit mehr oder weniger Eigenverantwortung und Regierungsnähe eingesetzt werden sollten.

Wir schlagen beispielsweise vor, dass die Tools B2 (Warnmeldungen bei riskantem Datenaustausch) und A (Unabhängige Überprüfung der Datenfilter) am besten eingesetzt werden, wenn Kontrollorgane ihre eigenen Prozesse auf Grundlage der technischen Infrastruktur betreiben, die von den Nachrichtendiensten betrieben und gewartet wird. Die ordnungsgemäße Datenfilterung ist ein grundlegender Baustein für gesetzeskonformes Handeln und sollte in erster Linie in der Verantwortung der Dienste liegen. Im Gegensatz dazu sehen wir für die Kontrolleur:innen deutlich mehr Spielraum, die Risikoabschätzung (C) oder Lösch-Statistiken (B3) eigenständig auszuführen. Bei einigen der hier vorgestellten Ideen ist Widerstand von den Nachrichtendiensten und der Fachaufsicht zu erwarten. Vor diesem Hintergrund könnte es sinnvoll sein, sich zunächst auf diejenigen Ideen zu konzentrieren, die mit weniger Widerstand seitens der Regierung umzusetzen sind, wie zum Beispiel die Auswertung von Lösch-Statistiken. Die ordnungsgemäße Löschung von Daten stellt eine enorme Herausforderung dar und die Einführung dieser Statistiken könnte viele Befürworter:innen haben. Sowohl Regierungen als auch Aufsichtsbehörden haben ein Interesse an einer effektiven Datenlöschung: Die Einhaltung von Aufbewahrungsfristen ist aus Gründen des Datenschutzes erforderlich, sie ergibt aber auch mit Blick auf Datensicherheit und Datengenauigkeit Sinn.

Was andere Werkzeuge und Konzepte betrifft, so schafft die Bereitstellung von Protokolldaten (B) eine Win-Win-Situation. Aufsichtsbehörden, die Zugang zu aussagekräftigen Audit-Trails haben, bräuchten von den Diensten nicht mehr ausführlich unterrichtet zu werden. Damit würde außerdem viel Missbrauchspotenzial entfallen, das dem Prozess und der Politisierung der Unterrichtungen innewohnt. Eine verbesserte Transparenz gegenüber den Aufsichtsbehörden hätte zudem noch weitere positive Auswirkungen: Wenn die Kontrolleur:innen relevante Protokolldaten erhalten, können sie ihre Untersuchungen auf besonders missbrauchsanfällige Bereiche des nachrichtendienstlichen Handels konzentrieren (siehe die Kategorien zur verbesserten Risikoabschätzung (C), das Risiko reduziert sich, u.a. wenn relevante Protokollierung erfolgt). Die Bereitstellung von Protokolldaten wiederum befreit Regierungsstellen von der Notwendigkeit, sich mit Antworten auf detaillierte Anfragen von Kontrollgremien zu bemühen, sodass die dadurch freigewordenen Kräfte an anderer Stelle zur Verfügung stünden.

3.2 Handlungsempfehlungen

Der Wunsch nach mehr Kontrollinnovation steht seit längerer Zeit im Raum. Leider werden wichtige Veränderungen aber noch immer vertagt. Hier scheint der politische Willen zu fehlen. Mancherorts fehlt es den Kontrolleur:innen vielleicht auch an eigenen Ideen, um eine technikgestützte, teil-automatisierte Kontrolltätigkeit Wirklichkeit werden könnte. Mit folgenden Punkten und Empfehlungen hoffen wir eine politische Debatte zu befeuern, die den Weg ebnet für eine moderne und wirksame Nachrichtendienstkontrolle.

Allgemeine Empfehlungen

- **Oversight-By-Design fördern:** Nachrichtendienste sollten ihre Prozesse und Informationssystem so konzipieren, dass sie jederzeit effizient kontrolliert werden können. Es liegt in der Verantwortung der Dienste, die Nachvollziehbarkeit in allen Phasen der Informationsgewinnung sicherzustellen. Vor Einführung neuer Datenverarbeitungssysteme sollten standardmäßig Konsultationen zwischen den Diensten und den Kontrolleur:innen stattfinden. Nachrichtendienste sollten in den jeweiligen Gesetzen dazu verpflichtet werden, die Kontrollgremien in den Prozess mit einzubinden und deren Anforderungen an neue Überwachungstechnologien bereits in der Planungsphase abzubilden.[65]

- **Direkter elektronischer Zugriff auf die Betriebssysteme:** Kontrollbehörden, denen ein umfassender digitaler Zugang zu den von den Nachrichtendiensten verwendeten Daten und Betriebssystemen fehlt, können nur beschränkt effektive Aufsicht gewährleisten. Dafür ist sowohl der direkte Zugriff auf Informationssysteme, als auch die Möglichkeit, Datensätze für eigenständige Offline-Analysen zu exportieren, nötig.

- **Bewertung der Kontrollkapazität:** Die Aufsichtsbehörden sollten Lücken und Defizite in ihren bestehenden Mandaten aufzeigen, bewerten und diese den politischen Entscheidungsträger:innen vorlegen. Diese Auseinander-

65 Der französische Gesetzgeber hat dieses Prinzip in Form verbindlicher Ex-ante-Gutachten der Aufsicht für Datenkennzeichnungsregeln gesetzlich verankert; siehe Wetzling und Vieth, 2018, S. 61f. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist unterdessen verpflichtet, die Rechtmäßigkeit und Funktion neuer Nachrichtendienstdatenbanken für personenbezogene Daten vor deren Umsetzung zu prüfen; siehe § 14 Abs. 1 Bundesverfassungsschutzgesetz, https://www.gesetze-im-internet.de/bverfschg/__14.html.

setzung ermöglicht es, kontextspezifische Strategien für datenbasierte Innovationen zu entwickeln.

- **Raum und Bereitschaft für Experimente eröffnen:** Jeder von uns vorgestellte Ansatz setzt ein hohes Maß an Vorbereitung und Experimentierfreudigkeit voraus. Damit die Kontrolltechnik richtig funktioniert, muss sie laufend evaluiert und angepasst werden. Dies erfordert Klarheit im Bezug auf Ziele und Motive, Personalressourcen, Kenntnisse des geltenden Rechts und der Nachrichtendienstpraxis sowie der benötigten Fähigkeiten zur Datenanalyse. Die Kontrollorgane sollten erfahrene Datenanalyst:innen einstellen, um spezielle technische Aufsichtsfunktionen aufzubauen und zu gewährleisten.

- **Austausch mit der Privatwirtschaft:** Die Aufsichtsbehörden sollten von den Erfahrungen profitieren, die im Bereich der Kontrolltechnik bereits in anderen Politikfeldern, wie der Informationssicherheit und der Finanzaufsicht, gesammelt wurden. Sie sollten über bestehende Partnerschaften hinaus den direkten Kontakt mit weiteren Akteuren der Privatwirtschaft und der Wissenschaft suchen. Die Kontrolleur:innen können auch von der Sichtung bestehender Lösungen für ähnliche Herausforderungen beim Aufbau und bei der Umsetzung von Kontrollkapazitäten und -technik profitieren. Es gibt beispielsweise eine breite Palette von Standardlösungen aus anderen Bereichen, die zumindest herangezogen werden könnte, um zu sehen, welche Art von Kontrolltechnik bereits zum Einsatz kommt. Personen, die Regierung und Sicherheitsdienste regelmäßig beim Aufbau von Datenanalyse-Tools beraten, sollten konsultiert werden, um ihre Expertise für die Entwicklung und Modernisierung der datenbasierten Kontrollinstrumente zu gewinnen.

Empfehlungen zur Verbesserung der unabhängigen Überprüfung der Datenfilter

Wie bereits erwähnt, wird die Implementierung der Filtertechnologie wahrscheinlich weiterhin eine Frage der internen Kontrolle bei den Nachrichtendiensten bleiben. Dennoch fällt den unabhängigen Kontrollgremien aber die entscheidende Aufgabe zu, die Ergebnisse der Datenfilterung kritisch zu prüfen. Die Aufsichtsbehörden sollten dafür in regelmäßigen Abständen unangekündigte Tests durchführen.

- **Sorgfalts-Prüfungen von gespeicherten Daten:** Dies erfordert einen ungehinderten Zugriff auf die Daten, die nach dem Filterprozess gespeichert werden. Die Ergebnisse dieser Tests sollten über einen längeren Zeitraum hinaus dokumentiert und verglichen werden, damit die Aufsichtsbehörden

eine allgemeine Fehlerquote der Filter ermitteln können. Dies würde es dann der Regierung und dem Gesetzgeber ermöglichen, evidenzbasierte Entscheidungen über die Effektivität und Umsetzbarkeit bestimmter rechtlicher Datenschutzvorgaben zu treffen.

- **Präzise und realistische Filterziele vorgeben:** Auf der Grundlage unabhängiger Kontrollen und der technischen Machbarkeit sollte der Gesetzgeber klare Anforderungen formulieren, was den Einsatz der Filtertechnik und die zulässige Fehlerquote betrifft.

Empfehlungen zur besseren Nutzung von Protokolldateien
Sowohl die Dienste als auch die Aufsichtsbehörden sollten die Vorteile der Bereitstellung von Protokolldaten für (halb-)automatische Auswertung erkennen. Die Protokollierungspflichten müssen im Gesetz detailliert vorgegeben werden, um eine wirksame Aufsicht zu ermöglichen. Da Protokolldateien bereits für andere Zwecke im Nachrichtendienstwesen aufgezeichnet und genutzt werden, sollte zukünftig bedacht werden, dass bereits beim Aufbau neuer Logging-Systeme die Bedürfnisse der Kontrolleur:innen berücksichtigt werden.

- **Einführung einer Audit-Trails-Pflicht:** Protokolldateien und andere relevante Daten sollten bei den Diensten so geführt und gepflegt werden, dass sie den Bedürfnissen der Kontrollgremien entsprechen. Dazu gehört die gesetzliche Verpflichtung zur Aufzeichnung und Bereitstellung aussagekräftiger Protokolldateien sowie eine umfassende Datenkennzeichnungspflicht. Diese sind bereits von vielen Datenschutzgesetzen vorgesehen und sind entscheidende Voraussetzungen für die oben beschriebenen Formen der Protokolldatenanalyse.

- **Kontrollinnovationen durch Hackathons und Beteiligung an Sicherheitsforschung:** Da Aufsichtsbehörden üblicherweise relativ kleine Institutionen mit begrenzten Ressourcen sind, sind deren Möglichkeiten in Eigenregie technische Innovationen auf die Beine zu stellen in der Regel nicht vorhanden. Die moderne Nachrichtendienstkontrolle stellt allerdings besondere Anforderungen an technische Lösungen. Die Vorbereitung und Leitung von Hackathons für die Nachrichtendienstkontrolle könnte externes Fachwissen zusammenbringen und es auf die spezifischen Bedürfnisse der Kontrollgremien ausrichten. Um Methoden und Datenquellen vor den Teilnehmer:innen geheim zu halten, könnte ein öffentlich zugänglicher Hackathon auf einem abstrakten Problem basieren, das mit synthetischen Daten dargestellt wird. Es könnte auch ein offener Aufruf zur Ideenfindung für Ansätze der Mustererkennung ausgeschrieben werden. Ebenso sollten Möglichkeiten in Erwägung gezogen werden, sich an nationalen oder euro-

päischen Forschungsprojekten zu beteiligen, um den Einsatz sogenannter supervisory technology auch für die Aufsicht von Sicherheitsbehörden zu prüfen und zu testen.

- **Gemeinsame Berichtsstandards für Datenweitergabe:** Europaweit sollten die Kontrollbehörden mit ihren nationalen Regierungen intensiver zusammenarbeiten, um gemeinsame Mindestanforderungen für Meldepflichten festzulegen, die Datensätze betreffen, die getauscht oder gemeinsam geführt werden. Allgemein sollte gelten, dass Daten, die an einen ausländischen Dienst weitergegeben werden, auch von den Aufsichtsgremien der beiden betreffenden Länder eingesehen werden dürfen.

- **Zusammenarbeit der Aufsichtsgremien zur Professionalisierung der Protokolldatenanalyse:** Angesichts der Komplexität, die mit der Entwicklung von Kontroll-Programmen verbunden ist, sollten die Aufsichtsbehörden im Rahmen ihrer internationalen Zusammenarbeit Erfahrungen austauschen und bewährte Verfahren ermitteln. Durch gegenseitige Wissensvermittlung, gemeinsames Experimentieren mit und Bewerten von Lösungsansätzen wie Lösch-Statistiken, Datenvisualisierungen und Mustererkennungstools, können sie so den Herausforderungen ihrer Arbeit besser gerecht werden und ihre Kapazitäten erweitern.

Empfehlungen für eine effektive Risikoabschätzung
Ein systematischer Ansatz bei der Priorisierung von Kontrollaktivitäten liegt im Interesse aller Beteiligten. Er sollte sowohl transparent als auch anpassungsfähig sein.

- **Ständige Abbildung aller den Kontrolleur:innen bekannten nachrichtendienstlichen Tätigkeiten:** Auf der Grundlage einer ersten Bestandsaufnahme der Datenerfassungsprogramme und Speichersysteme sollten die Aufsichtsbehörden die zuständigen Ministerien oder Behörden anfragen, ob dieses Verzeichnis vollständig ist oder ob es andere Elemente gibt, die einbezogen werden sollten. Die regelmäßige Wiederholung dieses Vorgangs ermöglicht es, die Ergebnisse im Laufe der Zeit zu vergleichen.

- **Öffentliche Dokumentation:** Um einen Bias zu minimieren und blinde Flecken bei der Risikobewertung möglichst auszuschließen, sind klare Dokumentationen sowie Handbücher bereitzustellen und routinemäßige Peer-Reviews unter den Risikobewerter:innen einzurichten. Diese transpa-

rente Darstellung hilft der Öffentlichkeit, den Wert und die Durchschlagskraft der unabhängigen nachrichtendienstlichen Kontrolle zu verstehen.

- **Fortwährende Evaluierung:** Es bedarf zudem regelmäßiger Tests und Anpassungen der Risikobewertungsmethode.

Empfehlungen für den Dialog zwischen Dienstanbietern und Kontrolleur:innen

Technologiegestützte Innovationen sollten mit prozessorientierten Verfahren und Schutzmaßnahmen einhergehen. Die datengesteuerten Tools sollten daher unbedingt durch eine Verpflichtung der Dienstleister Fehler zu melden und regelmäßige Austauschformate mit Kontrolleur:innen ergänzt werden.

- **Fehlermeldung an die Aufsichtsgremien einführen:** Um einen strukturierten Austausch zwischen Aufsichtsbehörden und Dienstanbieter einzuleiten, sollte eine Meldepflicht bei Fehlern oder Ungereimtheiten in der Ausführungen von Übermittlungsanordnungen eingeführt werden. Eine Meldung an die Aufsichtsgremien sollte sowohl bei technischen Fehlern als auch bei Fällen von Rechtsunsicherheit sowie bei Verdacht auf eine kreative Umgehung von Rechtsvorschriften erfolgen.

- **Transparenz:** Form und Häufigkeit des Austausches zwischen Kontrolleur:innen und Dienstanbietern sollten auch in den Jahresberichten der Gremien Eingang finden, um das Vertrauen der Öffentlichkeit in ihre Arbeit zu stärken.

4. Fazit

In Zukunft wird es nicht ausreichen, der Nachrichtendienstkontrolle nur einen sporadischen Zugriff auf einen Bruchteil der nachrichtendienstlichen Informationssysteme zu gewähren. Länder, in denen unabhängige Aufsichtsbehörden noch immer mit stark fragmentierten und papier-basierten Kontrollen vorlieb nehmen müssen, vereiteln das enorme Potenzial der datenbasierten Aufsicht. Mehr noch: Zur Wahrung der Rechtsstaatlichkeit und weiterer demokratischer Grundprinzipien ist ein Wandel dringend erforderlich – und möglich.

Angesichts der schieren Menge an Daten, die von Nachrichtendiensten gesammelt werden, muss eine wirksame Aufsicht ebenfalls datenbasiert arbeiten. Um dies zu erleichtern, müssen die Aufsichtsbehörden sicherstellen, dass ihre spezifischen Bedürfnisse beim Bau von IT-Systemen berücksichtigt werden. Allein dies erfordert einen entscheidenden Planungs- und Mehraufwand in den kommenden Jahren. Es ist wichtig, dass datengesteuerte Aufsichtsinstrumente nicht als Ersatz für die bisherige Arbeit, sondern als leistungsfähige Ergänzung eingesetzt werden, um effizienter zu arbeiten. Wie bei der softwaregestützten Diagnostik in der Medizin werden datengesteuerte Werkzeuge vermutlich nur dann erfolgreich genutzt werden, wenn sie in der subjektiven Wahrnehmung der Kontrollierenden als operative Bereicherung gesehen werden. Die Akzeptanz der Nutzer:innen erfordert wiederum einen Schulungs- und Sozialisierungsprozess, der Zeit in Anspruch nimmt. Damit dieser Prozess erfolgreich ist, muss zusätzliches Fachwissen in die Aufsichtsbehörden getragen werden, um es ihnen zu ermöglichen, eine größere praktische Unabhängigkeit von Regierungsstellen und Nachrichtendiensten zu erlangen.

Überzogene Erwartungen und Mandate stellen ebenso ein Problem dar: Die Aufsichtsbehörden benötigen offensichtlich mehr Personal, Ressourcen und Fachwissen, um viele der im zweiten Kapitel diskutierten Herausforderungen bewältigen zu können. Diese Stellen müssen die Gelegenheit nutzen, mit Nachrichtendiensten und politischen Entscheidungsträgern sowie ausländischen Kontrollgremien zusammenzuarbeiten und Strategien für Kontrollinnovationen zu entwickeln, die für bestimmte nationale Gegebenheiten angepasst werden müssen. Natürlich sollten dabei auch bewährte Maßnahmen ausgetauscht werden, weshalb wir das neue Projekt über Innovations- und Auditstandards für die Aufsicht begrüßen, das kürzlich von sechs europäischen Kontrollbehörden aufgenommen wurde.

Damit die datengesteuerte Nachrichtendienstkontrolle Fahrt aufnimmt, benötigen Aufsichtsbehörden mehr Hilfe und Verbündete. Warum sollten nur die Nachrichtendienste, aber nicht die Aufsichtsbehörden Zugang zu beträchtlichen Ressourcen für Forschung und Entwicklung haben? Politische Entscheidungsträger:innen und Planer:innen von Horizon Europe in der Europäischen Kommission sollten die Zuweisung von Finanzmitteln für Forschung und Entwicklung in Betracht ziehen, die sich ausdrücklich auf die Förderung datenbasierter Aufsichtslösungen in der Justiz und in der Verwaltung konzentrieren.

Sollten Aufsichtsbehörden diese Innovationen und Modernisierung weiter versäumen, steht zu befürchten, dass nationale und internationale Gerichte schwerwiegende Kontrolldefizite rügen und leistungsfähigere Aufsichtssysteme fordern. Auch hier zeigt sich: Legitimität ist ein Gut, das sich fortlaufend neu erarbeitet werden muss. Es ist an der Zeit, endlich wegweisende Maßnahmen für effektivere Nachrichtendienstkontrolle zu ergreifen.

5. Anhang

5.1 Liste der Interview- und Fokusgruppenteilnehmer:innen

Wir bedanken uns für die Hilfe, die wir bei der Erstellung dieses Berichts von verschiedenen Stellen erhalten haben. Wir wissen es sehr zu schätzen, dass Expert:innen aus verschiedenen Sektoren uns mit ihrem Wissen und ihrer Zeit unterstützt haben. Nicht alle wollten namentlich genannt werden, aber unser Dank gilt ihnen allen. Die folgenden Personen lieferten uns während des Workshops Europäischen Netzwerk Nachrichtendienstkontrolle (EION)[66] am 10. Mai 2019 und/oder in bilateralen Gesprächen wertvolle Hinweise:

- Dr. Julia Thorsøe Ballaschk, Datenschutzabteilung der Nationalen Polizei, Dänemark
- Wouter de Ridder, Generalsekretär des Ständigen Kontrollausschuss für Nachrichten- und Sicherheitsdienste, Belgien
- Arild Færaas, Kommunikationsberater im Sekretariat des EOS-Gremiums, Norwegen
- Christian Flisek, stellvertretendes Mitglied der G10-Kommission, Deutschland
- Dr. Luka Glušac, Berater im Büro des Ombudsmanns, Serbien
- Dr. Emil Bock Greve, Sekretariatsleiter der Nachrichtendienst-Aufsichtsbehörde TET, Dänemark
- Giles Herdale, Associate Fellow am Royal United Services Institute (RUSI), Vereinigtes Königreich
- Dr. Bertold Huber, stellvertretender Vorsitzender der G10-Kommission, Deutschland
- Rune Odgaard Jensen, Nachrichtendienst-Aufsichtsbehörde TET, Dänemark
- Thomas Kugelmeier, Arbeitsgruppe Nachrichtendienste beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Deutschland
- Klaus Landefeld, stellvertretender Vorstandsvorsitzender, Vorstand Infrastruktur und Netze eco-Verband der Internetwirtschaft e. V. und Mitglied des Aufsichtsrats bei DE-CIX International, Deutschland
- Stuart Macleod, Prüfungsleiter, Investigatory Powers Commissioner's Office (IPCO), Vereinigtes Königreich

66 https://www.stiftung-nv.de/de/unterprojekt/europaeisches-netzwerk-nachrichtendienstkontrolle-eion

- Charles Miller, Prüfungsleiter, Investigatory Powers Commissioner's Office (IPCO), Vereinigtes Königreich
- Adam Steen Petersen, Datenschutzabteilung der Nationalen Polizei, Dänemark
- Dr. Jörg Pohle, PostDoc, Leiter des Forschungsprogramms „Daten, Akteure, Infrastrukturen" sowie des Programms „Global Privacy Governance", Alexander von Humboldt-Institut für Internet und Gesellschaft, Deutschland
- Kjetil Otter Olsen, Technischer Direktor im Sekretariat des EOS-Gremiums, Norwegen
- Sir Bernard Silverman FRS, emeritierter Professor an den Universitäten Bristol und Oxford und Vorsitzender des Technologie-Beirats des Investigatory Powers Commissioner's Office (IPCO), Vereinigtes Königreich
- Dr. Sabine Sosna, Leiterin Arbeitsgruppe Nachrichtendienste beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Deutschland
- Dr. Félix Tréguer, PostDoc an der Sciences Po Paris und Gründungsmitglied von La Quadrature du Net, Frankreich
- Dominic Volken, stellvertretender Leiter der Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten, Schweiz

5.2 Literatur

Aaronson, Trevor. 2019. „A Declassified Court Ruling Shows How The FBI Abused NSA Mass Surveillance Data“. The Intercept. 10. Oktober 2019. https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/.

Babuta, Alexander. 2019. „A New Generation of Intelligence: National Security and Surveillance in the Age of AI“. RUSI.org. 19. Februar 2019. https://rusi.org/commentary/new-generation-intelligence-national-security-and-surveillance-age-ai.

Becker, Rainer, und Christian Schulz. 2016. „Wieviel Geheimdienst braucht Deutschland?“ 16. November 2016. https://www.swr.de/film/bnd-schattenwelt-geheimdienst-doku-nachrichtendienst-swr/-/id=5791128/did=17666664/nid=5791128/1o343xj/index.html.

Bundesgesetz über den Nachrichtendienst. 2015. (Schweizer NDG).

Bundestag. 2013. „Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes“. 18/217. Berlin. https://dip21.bundestag.de/dip21/btd/18/002/1800217.pdf.

Bundesverfassungsgericht. 2016. „G 10-Kommission ist im Organstreitverfahren nicht parteifähig und scheitert daher mit dem Antrag auf Herausgabe der NSA-Selektorenlisten (Pressemitteilung Nr. 72/2016)“. 14. Oktober 2016. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/bvg16-072.html;jsessionid=7E07882B3FF5229720E12BEF0CB9498E.1_cid370.

Bundesverwaltungsgericht. 2018. „Klage der DE-CIX Management GmbH erfolglos (Pressemitteilung Nr. 38/2018)“. 31. Mai 2018. https://www.bverwg.de/pm/2018/38.

Cavan, Jo, und Paul Killworth. 2019. „GCHQ embraces AI, but not as a blackbox“. about:intel. 8. Oktober 2019. https://aboutintel.eu/author/jo-cavan-paul-killworth/.

Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD). 2018. „Review report: The multilateral exchange of data on (alleged) jihadists by the AIVD (CTIVD Review Report no. 56)“. https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2018/04/24/index/CTIVD+Review+report+NO56.pdf.

———. 2019a. „Annual Report CTIVD 2018“. https://english.ctivd.nl/binaries/ctivd-eng/documents/annual-reports/2019/06/20/index/CTIVD+annual+report+2018.pdf.

———. 2019b. „Progress Report“. CTIVD nr. 63. https://www.ctivd.nl/documenten/rapporten/2019/09/03/index.

Commission national de contrôle des techniques de renseignement (CNCTR). 2019. „3. Rapport d’activité 2018.“. https://www.cnctr.fr/_downloads/NP_CNCTR_2019_rapport_annuel_2018.pdf.

Corfield, Gareth. 2019. „London cop illegally used police database to monitor investigation into himself.“ The Register. 11. Juli 2019. https://www.theregister.co.uk/2019/07/11/met_police_sgt_pleads_guilty_computer_misuse_crimes/.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. 2019. „27. Tätigkeitsbericht 2017-2018“. https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/27TB_17_18.pdf?__blob=publicationFile&v=4.

EOS-utvalget Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-Gremium). 2019. „EOS Committee Annual Report 2018“. Annual Report. https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf.

———. 2018. „Strengthening oversight of international data exchange between intelligence and security services," October 22, 2018, https://eos-utvalget.no/wp-content/uploads/2019/05/joint_statement_for_publication_20181114_final_endelig-2.pdf.

Europäischer Gerichtshof für Menschenrechte (EGMR). 2018. „Case of Big Brother Watch and Others v. The United Kingdom". http://hudoc.echr.coe.int/eng?i=001-186048.

Foreign Intelligence Surveillance Court. 2018. „FISC Opinion regarding the Section 702". Washington D.C. https://www.documentcloud.org/documents/6464604-2018-FISC-Ruling-Shows-How-FBI-Abused-NSA-Mass.html.

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10-Gesetz). 2001. https://www.gesetze-im-internet.de/g10_2001/.

Goldman, Zachary K., und Samuel J. Rascoff, Hrsg. 2016. Global Intelligence Oversight. Governing Security in the Twenty-First Century. Oxford: Oxford University Press.

Golla, Sebastian. 2019. „Neugier und Datenkriminalität". Legal Tribune Online. 16. August 2019. https://www.lto.de/recht/hintergruende/h/polizei-datenbanken-missbrauch-datenkriminalitaet-abfragen-daten-schutz/.

Government Communications Headquarter. 2019. „Investigatory Powers Act". 19. März 2019. https://www.gchq.gov.uk/information/investigatory-powers-act.

Graulich, Kurt. 2017. „Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation", Kriminalpolitische Zeitschrift (KriPoZ), Nr. 1/2017: 43–52.

Investigatory Powers Act. 2016. http://www.legislation.gov.uk/ukpga/2016/25/section/67/enacted?view=interweave.

Koenig-Archibugi, Mathias. 2004. „International Governance as New Raison d'état? The Case of the EU Common Foreign and Security Policy", European Journal of International Relations, Nr. 10 (2). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.893.1837&rep=rep1&type=pdf.

Lohse, Eckart. 2015. „Kanzleramt übt heftige Kritik an BND", 23. April 2015. https://www.faz.net/aktuell/politik/inland/kanzleramt-uebt-heftige-kritik-an-bnd-13555622.html.

Meister, Andre. 2016. „Geheimer Prüfbericht: Der BND bricht dutzendfach Gesetz und Verfassung – allein in Bad Aibling (Updates)". Netzpolitik.org. 1. September 2016. https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

Perraudin, Frances. 2019. „Mordaunt pledges to review internal MoD torture guidance", 20. Mai 2019. https://www.theguardian.com/uk-news/2019/may/20/mordaunt-pledges-to-review-internal-mod-torture-guidance.

Ridder, Wouter de. 2019. „A simple yet existential demand: Let oversight bodies work together". about:intel. November 2019. https://aboutintel.eu/simple-oversight-demands/.

Ryngaert, Cedric, und Nico van Eijk. 2019. „International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees", International Data Privacy Law, Nr. 9 (1) (April). https://academic.oup.com/idpl/article/9/1/61/5427456.

Schmitt, Richard. 2019. „Alarm: Verfassungsschutz BVT steht total blamiert da (Alarming: Austria's Intelligence Service BVT disgraces itself to European partners)", 11. November 2019. https://www.oe24.at/oesterreich/politik/Alarm-Verfassungsschutz-BVT-steht-total-blamiert-da/405465583.

Smith, Graham. 2019. „What will be in Investigatory Powers Act Version 1.2?" 30. Oktober 2019. https://www.cyberleagle.com/2018/10/what-will-be-in-investigatory-powers.html.

Statens inspektion för försvarsunderrättelseverksamheten (SIUN). 2018. „Årsredovisning för 2017“. http://www.siun.se/dokument/Arsredovisning_2017.pdf.

Swire, Peter, Jesse Woo, und Deven R. Desai. 2019. „The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance“, A Hoover Institution Essay, 19. Januar 2019.

Venedig Kommission. 2015. „Report on the democratic oversight of signals intelligence agencies“. CDL-AD (2015) 011 Adopted by the Venice Commission at its 102nd Plenary Session. Strasbourg. http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

Wetzling, Thorsten. 2017. „Options for More Effective Intelligence Oversight“. Discussion Paper. https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

Wetzling, Thorsten, und Kilian Vieth. 2019. Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich. Schriften zur Demokratie 50. Berlin: Heinrich-Böll-Stiftung. https://www.stiftung-nv.de/sites/default/files/massenuberwachung_bandigen_-_web.pdf.

Wissenschaftliche Dienste des Deutschen Bundestages. 2006. Der Kernbereich exekutiver Eigenverantwortung. 10.11.2006. https://www.bundestag.de/resource/blob/412760/1e98af44462dee55fd1ee3925501dbf4/wd-3-383-06-pdf-data.pdf.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autoren

Kilian Vieth

Kilian Vieth koordiniert den Themenbereich Grundrechte, Überwachung und Demokratie bei der Stiftung Neue Verantwortung. Er forscht im europäischen GUARDINT-Projekt zu den Potenzialen und Grenzen der Kontrolle von Überwachung. Als Projektmanager für das Europäische Netzwerk Nachrichtendienstkontrolle (EION) erarbeitet er Reformansätze für eine demokratischere und effizientere Überwachungs- und Nachrichtendienstpolitik in Europa. Er studierte Politikwissenschaft unter anderem am Otto-Suhr-Institut der Freien Universität Berlin und an der Sciences Po Paris.

So erreichen Sie den Autor
kvieth@stiftung-nv.de
+49 (0)30 81 45 03 78 88
@newsvieth

Dr. Thorsten Wetzling

Thorsten Wetzling leitet die Arbeit der Stiftung Neue Verantwortung im Themenfeld Grundrechte, Überwachung und Demokratie. Er führt das Europäische Netzwerk Nachrichtendienstkontrolle (EION) und ist Principal Investigator im Verbundprojekt GUARDINT, das von der DFG finanziert wird. Zudem ist Thorsten Editor in Chief des englischsprachigen Blogs aboutintel.eu. Er hat am Genfer Hochschulinstitut für internationale Studien und Entwicklung mit einer vergleichenden Studie zur Performanz und Reform der Nachrichtendienstkontrolle in Europa promoviert.

So erreichen Sie den Autor
twetzling@stiftung-nv.de
+49 (0)30 81 45 03 78 93
@twetzling

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Klöthe

Grafikdesign:
Anne-Sophie Stelke
www.annesophiestelke.com