

Oktober 2023 - Corbinian Ruckerbauer und Thorsten Wetzling

---

# Zügellose Überwachung?

Defizite der Kontrolle des  
Militärischen Nachrichtenwesens  
der Bundeswehr



Think Tank für die Gesellschaft im technologischen Wandel

## Zusammenfassung

Die Ampelregierung will laut Koalitionsvertrag in der laufenden Legislaturperiode die Kontrolle „aller nachrichtendienstlichen Tätigkeiten des Bundes“ ausbauen und stärken. Eine zentrale Frage ist dabei aber noch gänzlich unbeantwortet: Was genau sind nachrichtendienstliche Tätigkeiten des Bundes und wer übt sie aus? Ist damit ausschließlich das Handeln der drei Nachrichtendienste des Bundes gemeint, also: Bundesnachrichtendienst (BND), Bundesamt für den Verfassungsschutz (BfV) und Bundesamt für den Militärischen Abschirmdienst (BAMAD)? Oder soll, dem Modell anderer Demokratien folgend, der Fokus des Rechtsrahmens und der Kontrolle künftig auch auf nachrichtendienstliche Tätigkeiten des Bundes ausgeweitet werden, die nicht von den Nachrichtendiensten selbst ausgeübt werden? Ein zentrales Beispiel für letzteres sind die Aufklärungsaktivitäten des Militärischen Nachrichtenwesens der Bundeswehr.

Die Ampel hat sich in dieser Frage noch nicht festgelegt, obwohl sie aktuell weitreichende Reformen auf den Weg bringt. Erste Vorschläge der Bundesregierung zur Weiterentwicklung der Rechtskontrolle wurden intern kontrovers diskutiert (Flade, 2023; UK-Rat, 2023; Wetzling & Vieth-Ditlmann, 2023) und letztlich nicht Teil der ersten Reform des Nachrichtendienstrechts (Bundesregierung, 2023b), die Anfang Oktober 2023 in den Bundestag eingebracht wurde (Bundesregierung, 2023b; Bundesregierung, 2023c). In einem zweiten Teil der Reform soll nun bis 2024 „die wertungskonsistente Systematisierung der Regelungen zur Informationsbeschaffung folgen und das Nachrichtendienstrecht insgesamt zukunftsfest ausgestaltet werden“ (Bundesregierung, 2023b). Hierbei wäre es aus unserer Sicht dringend geboten, die nachrichtendienstlichen Tätigkeiten des Militärischen Nachrichtenwesens mit zu berücksichtigen. Sollte eine Reform dieses wachsenden Teils der staatlichen Überwachung erneut ausbleiben, würden folgende rechtsstaatliche Defizite von Regierung und Bundestag weiterhin in Kauf genommen:

**Fehlender Rechtsrahmen.** Es gibt, anders als bei den Nachrichtendiensten oder Strafverfolgungsbehörden, keine ausreichende gesetzliche Grundlage für die Erhebung und Verarbeitung von Daten im Rahmen der militärischen Aufklärung. Das Verfassungsgericht hat eine Reihe von Vorgaben und Verfahren zur rechtsstaatlichen Absicherung und Begrenzung von Grundrechtseingriffen im Rahmen staatlicher Überwachung unmissverständlich formuliert. Im Bereich des Militärischen Nachrichtenwesens werden diese Vorgaben, wenn überhaupt, nur in internen Dienstvorschriften des Bundesministeriums für Verteidigung (BMVg) umgesetzt.

**Unzureichende Kontrolle.** Es fehlen wichtige Vorgaben und Strukturen für eine wirksame unabhängige Kontrolle des Regierungshandelns in diesem Bereich. Bis heute gibt es keine ständige parlamentarische Kontrolle, ganz zu schweigen von einem

unabhängigen Organ der objektiven Rechtskontrolle. Die Prüftätigkeiten des allein auf weiter Flur operierenden Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sind, zumindest soweit öffentlich erkennbar, in der Wirksamkeit begrenzt.

Die Bundesregierung und die Regierungsmehrheit im Bundestag wären schlecht beraten, die Überwachungsbefugnisse des Militärischen Nachrichtenwesens und dessen unabhängige Kontrolle von der für den Sommer 2024 anvisierten Reform auszusparen. Ausgehend von mehreren Fallbeispielen verdeutlicht dieser Impuls, dass Maßnahmen der militärischen Aufklärung tief in Grund- und Menschenrechte eingreifen. Um deren rechtsstaatliche sowie und verfassungskonforme Durchführung und Kontrolle zu gewährleisten, sollte der Bundestag dringend

- die wesentlichen Überwachungstätigkeiten der militärischen Aufklärung in einem Gesetz mandatieren und dabei unmissverständlich anzeigen, wenn diese Aktivitäten in Grundrechte eingreifen;
- dafür Sorge tragen, dass das gesamte Spektrum der militärischen Aufklärung der ständigen parlamentarischen Kontrolle unterliegt und grundrechtsrelevante Tätigkeiten von einem unabhängigen Organ der auf Zulässigkeit und Erforderlichkeit überprüft werden.

Die Bundesregierung und die Regierungsmehrheit im Bundestag könnten dafür ein eigenständiges Bundeswehraufgabengesetz oder ein Gesetz über das Militärische Nachrichtenwesen (MilNWG) erarbeiten. Um jedoch konsistent die gebotenen Standards für Kontrolle und Rechtsrahmen bei staatlicher Überwachung zu gewährleisten, sollte unserer Auffassung nach ein neuer und einheitlicher Rechtsrahmen für alle nachrichtendienstliche Tätigkeiten des Bundes geschaffen werden. Das würde dem Anspruch der Bundesregierung entsprechen, nachrichtendienstliche Methoden der Informationsbeschaffung wertungskonsistent zu regeln. Entscheidend dabei wäre, dass die neue gesetzliche Grundlage legitime Zwecke, Eingriffsschwellen, Anordnungsvoraussetzungen und -verfahren sowie Beanstandungswege auch für die militärische Aufklärung klar benennt, um unverhältnismäßiger Überwachung vorzubeugen und Missstände zu beheben.

## Inhalt

<b>Zusammenfassung</b>	<b>2</b>
<b>1. Einleitung</b>	<b>6</b>
<b>2. Das Militärische Nachrichtenwesen der Bundeswehr</b>	<b>8</b>
2.1. Worum geht es?	8
2.2. Auswahl relevanter Akteure des Militärischen Nachrichtenwesens	8
2.3. Ausgewählte Methoden der Informationsbeschaffung	12
2.3.1. Open Source Intelligence (OSINT)	12
2.3.2. Signals Intelligence (SIGINT)	14
2.3.3. Human Intelligence (HUMINT)	15
<b>3. Grundrechtliche Relevanz des Militärischen Nachrichtenwesens und rechtsstaatliche Herausforderungen</b>	<b>17</b>
3.1. Verfassungsrechtliche Dimensionen und einschlägige Rechtsprechung	17
3.1.1. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung	20
3.1.2. Eingriffe in das Fernmeldegeheimnis	21
3.1.3. Zwischenfazit	21
3.2. Rechtsrahmen des Militärischen Nachrichtenwesens	22
3.3. Unabhängige Kontrolle des Militärischen Nachrichtenwesens	23
3.4. Vergleichbarkeit der Tätigkeiten des Militärischen Nachrichtenwesens mit denen der Nachrichtendienste des Bundes	25
3.4.1. Mögliche Abgrenzungskriterien	25
3.4.2. Enge Verzahnung von Militärischem Nachrichtenwesen und BND	26
3.5. Zwischenfazit	27
<b>4. Wege zur Überwindung rechtsstaatlicher Defizite</b>	<b>29</b>
4.1. Orientierungshilfe aus dem Nachrichtendienstrecht	29
4.1.1. Rechtsrahmen für die Informationsbeschaffung	30
4.1.2. Rechtliche Anforderungen und unabhängige Kontrolle	31
4.1.3. Zwischenfazit	33
4.2. Handlungsoptionen für den Bundestag	34
4.2.1. Bundeswehraufgabengesetz	34
4.2.2. Militärisches Nachrichtenwesen-Gesetz	34
4.2.3. Einheitlicher Rechtsrahmen für alle nachrichtendienstliche Tätigkeiten des Bundes	35
4.3. Weitere Empfehlungen zur Behebung rechtsstaatlicher Defizite	37
<b>5. Fazit</b>	<b>39</b>



<b>Literatur</b>	<b>41</b>
<b>Rechtsprechung</b>	<b>45</b>
<b>Impressum</b>	<b>47</b>

## 1. Einleitung<sup>1</sup>

Angesichts des russischen Angriffskriegs gegen die Ukraine hat die Bundesregierung ein Sondervermögen von 100 Milliarden Euro für die Bundeswehr beschlossen, um „Fähigkeitslücken zu schließen und so die Bündnis- und Verteidigungsfähigkeit zu stärken“ (BMVg, 2023, S. 8). Dieser Ausbau der Fähigkeiten betrifft auch die militärische Aufklärung, also die Erfassung und Auswertung von Signalen und Daten für die verschiedenen Bedarfe der Bundeswehr. Denn wie das aktuelle Kriegsgeschehen in der Ukraine zeigt, ist die militärische Aufklärung ein entscheidender Faktor, der über Erfolg oder Misserfolg von militärischen Operationen entscheiden kann. Vorteile hat die Konfliktpartei, die aus den vielen erhobenen Daten am effektivsten relevante Informationen für den Einsatz extrahieren kann. Dafür müssen die Daten und Analyseprodukte der militärischen Aufklärung nicht nur präzise und umfassend sein, sie müssen auch schnell und in geeigneter Form von den richtigen Stellen verwendet werden können (Joshi, 2023).

Der russische Angriffskrieg in Europa hat das öffentliche Interesse an der Bundeswehr enorm gesteigert. Trotzdem wird über deren Fähigkeiten zur militärischen Aufklärung kaum berichtet. Dabei ist es von großer Bedeutung, offen zu diskutieren, ob die grundrechtsrelevanten Überwachungsaktivitäten von Armeen rechtsstaatlich genügend eingehegt und unabhängig kontrolliert werden – auch um die Praktiken wehrhafter Demokratien von denen autoritärer Staaten abzugrenzen. Dabei geht es nicht darum, den Handlungsspielraum der Exekutive zu beschneiden oder gar die Wehrhaftigkeit der Bundesrepublik einzuschränken. Vielmehr greifen zahlreiche Aufklärungsmaßnahmen der Bundeswehr auch ohne Verteidigungsfall tief in Grund- und Menschenrechte von Personen ein, die nicht fremden Armeen angehören (siehe Kapitel 3). Daher ist dringend geboten, über die gesetzlichen Vorgaben zur Begrenzung der Überwachung und zur Wahrung der Verhältnismäßigkeit zu diskutieren und gegebenenfalls neue Regeln aufzustellen. Eine konstruktive Debatte trägt zur demokratischen Legitimation des Regierungshandelns bei und ist eine Voraussetzung dafür, öffentliches Vertrauen und Rechtssicherheit für die Bundeswehr durch einen umfassenden Rechtsrahmen zu stärken. Ein solcher Rechtsrahmen hilft zudem, Missbrauch vorzubeugen und etwaige Fehler zu ahnden. So werden Resilienz und Glaubhaftigkeit der wehrhaften Demokratie von innen gestärkt.

Um dieser Diskussion einen An Schub zu geben, nimmt dieser Impuls zunächst die Methoden und Fähigkeiten der militärischen Aufklärung in den Blick. Hiervon ausgehend werden dann die grundrechtliche Relevanz und die rechtsstaatlichen Herausforderungen genauer erörtert, die die militärische Aufklärung für unsere Demokratie

<sup>1</sup> Wir danken Hannah-Aeterna Borne, Lilly Goll, Luisa Seeling und Alina Siebert für wertvolle Kommentare, konstruktives Feedback und hervorragende Recherchearbeiten. Die Autoren sind allein verantwortlich für den Inhalt dieses Impulses.



mit sich bringt. Dabei nehmen wir Bezug auf die einschlägige Rechtsprechung des Bundesverfassungsgerichts (BVerfG), die eine grobe Richtschnur für einschlägige Mindeststandards enthält. Daran anschließend beleuchten wir den aktuellen gesetzlichen Rahmen und die bestehende Kontrollarchitektur für die militärische Aufklärung in Deutschland. Abschließend geben wir Empfehlungen für mögliche Wege der Reformen unter Berücksichtigung des Rechtsrahmens und der Kontrolle für ähnlich gelagerte Überwachungstätigkeiten bei den Nachrichtendiensten des Bundes.



## 2. Das Militärische Nachrichtenwesen der Bundeswehr

Dieses Kapitel beleuchtet zunächst die wichtigsten uns bekannten Tätigkeiten der militärischen Aufklärung der Bundeswehr. Hierfür benennen wir die wesentlichen Akteure, die diese Tätigkeiten ausführen. Ausgehend von konkreten Beispielen beschreiben wir dann exemplarisch drei Methoden der Informationserhebung.

### 2.1. Worum geht es?

Die wachsende Bedeutung der modernen Aufklärungs- und Überwachungsfähigkeiten von Streitkräften betrifft auch die Bundeswehr. Unter dem Begriff Militärisches Nachrichtenwesen (MilNW) werden alle Tätigkeiten zur Informationsgewinnung und -auswertung gefasst, die der Entscheidungsfindung der politischen Leitung und der militärischen Führung der Streitkräfte dienen. Typische Informationsbedarfe betreffen dabei Erkenntnisse bezüglich Truppen, Waffen und Anlagen anderer Streitkräfte und deren Leistungsfähigkeit, Standort und Verwendung. Zudem werden Informationen hinsichtlich der allgemeinen Lageentwicklung in Einsatzgebieten benötigt. Um die militärische Sicherheit zu gewährleisten, sind Informationen zur Bedrohungslage durch „Spionage, Sabotage, Zersetzung, Extremismus und Terrorismus“ (Binder, 2023, S. 130) von Bedeutung. Auf Grundlage dieser Informationen und der daraus erstellten Analysen sollen politische und militärische Entscheidungsträger:innen informiert werden, um die Einsatzfähigkeit der Streitkräfte zu erhöhen, Bedrohungen zu erkennen und die eigenen Truppen zu schützen.

### 2.2. Auswahl relevanter Akteure des Militärischen Nachrichtenwesens

Die Ausführung der oben beschriebenen Aufgaben ist dabei nicht auf bestimmte Dienststellen innerhalb der Bundeswehr beschränkt. Stattdessen ist das MilNW ein Querschnittsbereich, der sich über die gesamte Organisation hinweg erstreckt. Die Aufnahme und Weitergabe von Informationen, die für die beschriebenen Zwecke relevant sind, wird von allen Soldat:innen erwartet (Bundesregierung, 2021, S. 3). Gleichwohl gibt es Dienststellen, die vorrangig oder ausschließlich für militärische Aufklärung zuständig sind. Im Folgenden beschreiben wir diese Dienststellen und ihren jeweiligen Aufgabenbereich. Diese Aufzählung soll den Lesenden einen groben Überblick über die Breite und Tiefe der Aktivitäten zur Informationsbeschaffung und -verarbeitung der Bundeswehr verschaffen.<sup>2</sup>

<sup>2</sup> Aufgrund der mitunter strikten Geheimhaltung erhebt diese Aufzählung keinen Anspruch auf Vollständigkeit. Es handelt sich um auf Grundlage der öffentlich zugänglichen Informationen geschätzte Zahlen; um deren Genauigkeit zu verbessern, freuen wir uns über Hinweise und Referenzen.



Die Stellen, die mit zentralen Aufgaben des MilNW betraut sind, sind dem seit 2017 neu aufgestellt Organisationsbereich Cyber- und Informationsraum zugeordnet.

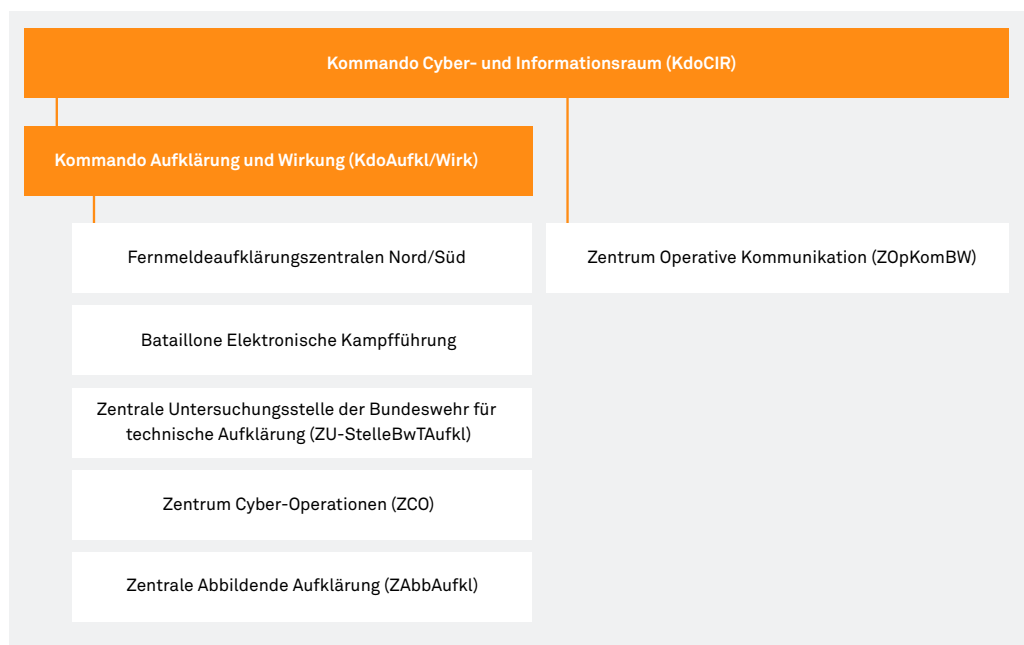
- **Kommando Cyber- und Informationsraum (KdoCIR – ca. 1260 Personen):** Das Kommando führt den gleichnamigen Organisationsbereich und verantwortet dessen Ausrichtung. Darüber hinaus nimmt diese Dienststelle auch Querschnittsaufgaben innerhalb der Bundeswehr wahr. Sie trägt beispielsweise die Gesamtverantwortung für die Informationssicherheit der Bundeswehr (Bundeswehr, 2023a). Dem KdoCIR direkt unterstellt ist das Kommando Aufklärung und Wirkung.
  - ◊ **Kommando Aufklärung und Wirkung (KdoAufkl/Wirk – ca. 540 Personen):** Dem Kommando Aufklärung und Wirkung unterstellte Dienststellen erheben Informationen mit Mitteln der Fernmelde- und elektronischen Aufklärung (SIGINT), der Cyberaufklärung sowie der satellitengestützten abbildenden Aufklärung und durch die Analyse offen zugänglicher Quellen (OSINT). Darüber hinaus umfasst es Fähigkeiten der Elektronischen Kampfführung (EloKa) und Cyberoperationen (cpm, 2022, S. 15). Von den dem Kommando nachgeordneten Dienststellen sind die folgenden von besonderer Bedeutung für das MilNW:
    - **Fernmeldeaufklärungszentralen Nord/Süd (zwei Einheiten mit insgesamt ca. 870 Personen):** Diese im Inland stationierten Einheiten dienen der ortsgebundenen, also stationären, Erfassung elektromagnetischer Kommunikationsvorgänge im Ausland. Diese kontinuierliche Erfassung dient der Erstellung von Lagebildern sowie dem Schutz der Truppe (Bundeswehr, 2023b).
    - **Bataillone Elektronische Kampfführung (vier Einheiten mit insgesamt ca. 2550 Personen):** Diese vier Bataillone bündeln mobile Fähigkeiten der Fernmelde- und elektronischen Aufklärung. Darüber hinaus umfasst sie auch Fähigkeiten zum Schutz der Truppe, wie die Störung gegnerischer Kampfsysteme (Bundeswehr, 2022).
    - **Zentrale Untersuchungsstelle der Bundeswehr für technische Aufklärung (ZU-StelleBwTAufkl – ca. 450 Personen):** Diese Stelle entwickelt neue Mittel zur technischen Aufklärung der Bundeswehr, wobei die Entwicklung sowohl in Deutschland als auch in Einsatzgebieten der Bundeswehr erfolgt. Die Zentrale Untersuchungsstelle begleitet die Entwicklung der technischen Mittel dabei bis zur praktischen Umsetzung (cpm, 2022, S. 66).
    - **Zentrum Cyber-Operationen (ZCO – ca. 100 Personen ):**<sup>3</sup> Das ZCO führt Cyberoperationen einerseits zur Beschaffung von Informationen und andererseits zur Störung gegnerischer Systeme und Infrastruktur durch.

3 Stand von 2020, gemäß Schulze, 2020, S. 35.



Darüber hinaus trägt es zur Stärkung der Informationssicherheit der Bundeswehr bei (cpm, 2022, S. 56).

- **Zentrale Abbildende Aufklärung (ZAbbAufkl – ca. 160 Personen):** Die Einheit trägt mit Erkenntnissen aus satellitengestützten Abbildungen zur Einsatzführung, Lagebeurteilung und Krisenfrüherkennung bei. Dabei kann die ZAbbAufkl auf Aufnahmen eigener Satellitensysteme ebenso zurückgreifen wie auf die kommerzieller Systeme (cpm, 2022, S. 61).
- ◊ **Zentrum Operative Kommunikation (ZOpKomBW – ca. 1000 Personen):** Das Zentrum Operative Kommunikation erstellt Analysen über die lokale Bevölkerung und gegnerische Streitkräfte und unterstützt so die Einsatzvorbereitung und -durchführung. Zudem wirkt die Einheit in Einsatzgebieten der Bundeswehr durch verschiedene Medienprodukte auf die lokale Bevölkerung (Bundesregierung, 2023a; cpm, 2022, S. 13).
- ◊ **Zentrale Fähigkeit OSINT der Streitkräfte (Personenzahl unbekannt):** Diese Einheit leitet den Aufbau der neuen Aufklärungsdisziplin „OSINT“ innerhalb der Dienststellen des BMVg. Ziel ist es die Fähigkeit zu entwickeln, „Informationen aus frei verfügbaren offenen Quellen weltweit“ zu sammeln und „mithilfe entsprechender Analysetools in verwertbare Erkenntnisse“ zu überführen (cpm, 2022, S. 64).



**Abbildung 01:**  
Wesentliche  
Dienststellen des  
Militärischen  
Nachrichten-  
wesens

Bei Betrachtung dieser mit Aufgaben des Militärischen Nachrichtenwesens betrauten Dienststellen der Bundeswehr wird deutlich, dass die Streitkräfte über um-



fassende Fähigkeiten zur Erhebung von Informationen verfügen. Zwar sind in den beschriebenen Organisationseinheiten nicht alle Mitarbeitenden an entsprechenden Aktivitäten beteiligt – gleichzeitig ist die Personalausstattung nicht für alle Stellen öffentlich einsehbar und bei anderen ist von Abweichungen auszugehen. Wir können annehmen, dass ein erheblicher Anteil der hier aufgeführten Personalressourcen direkt oder indirekt der militärischen Aufklärung dient. Wenn wir die vermuteten, hier nicht erfassten Ressourcen in anderen Dienststellen sowie die fehlenden Angaben in unsere Schätzung miteinbeziehen, erscheint uns eine Zahl von 6930 Angehörigen der Bundeswehr, die direkt oder indirekt an Aufklärungsaktivitäten beteiligt sind, realistisch.

Der untenstehende Vergleich mit der personellen Ausstattung der drei Nachrichtendienste des Bundes zeigt, dass die Ressourcen der Bundeswehr im Bereich der militärischen Aufklärung den einzelnen Nachrichtendiensten des Bundes nicht zwingend nachstehen.

Personal der Nachrichtendienste auf Bundesebene		Personal des Militärischen Nachrichtenwesens der Bundeswehr	
Bundesnachrichtendienst (BND)	ca. 6 500	Kommando Cyber- und Informationsraum (KdoCIR)	ca. 1 260
Bundesamt für Verfassungsschutz (BfV)	ca. 4 300	Kommando Aufklärung und Wirkung (KdoAufkl/Wirk)	ca. 540
Bundesamt für den Militärischen Abschirmdienst (BAMAD)	ca. 1 500	Fernmeldeaufklärungszentralen Nord/Süd	ca. 870
		Bataillone Elektronische Kampfführung	ca. 2 550
		Zentrale Untersuchungsstelle der Bundeswehr für technische Aufklärung (ZU-StelleBwTAufkl)	ca. 450
		Zentrale Abbildende Aufklärung (ZAbbAufkl)	ca. 160
		Zentrum Cyber-Operationen (ZCO)	ca. 100
		Zentrum Operative Kommunikation (ZOpeKomBW)	ca. 1 000
		Zentrale Fähigkeit OSINT der Streitkräfte	unbekannt
Gesamtzahl: ca. 12 300 besetzte Stellen		Gesamtzahl (Schätzung): ca. 6 930 Stellen	

Abbildung 02:  
 Personelle  
 Ausstattung im  
 Vergleich

Der nächste Abschnitt stellt einige Methoden der Informationsbeschaffung genauer vor, welche die hier dargestellten Dienststellen zur Ausführung der Aufgaben des Militärischen Nachrichtenwesens verwenden.

### **2.3. Ausgewählte Methoden der Informationsbeschaffung**

Dem Militärischen Nachrichtenwesen der Bundeswehr steht ein breites Spektrum an Mitteln der Informationsbeschaffung zur Verfügung. Dazu zählen unter anderem die Auswertung offen zugänglicher Informationen (OSINT), die Aufklärung durch menschliche Quellen (HUMINT) und die Fernmeldeaufklärung (SIGINT). Anhand von konkreten Beispielen wollen wir ausgewählte Mittel im Folgenden beleuchten.

#### **2.3.1. Open Source Intelligence (OSINT)**

Eine von der Bundeswehr zunehmend genutzte Methode der Informationserhebung ist die systematische Erfassung und Analyse von offen zugänglichen Quellen (OSINT). Hierunter können verschiedene Beschaffungsmethoden subsumiert werden: von der Erhebung und Analyse individueller Beiträge und Trends in sozialen Medien über das automatisierte Erfassen (Scraping) öffentlich zugänglicher Informationen auf Internetseiten bis hin zum Erwerb und der Verarbeitung von legal oder illegal erhobenen Datensätzen (Wetzling & Dietrich, 2022, S. 34 f.).

Im Januar 2023 wurde beispielsweise durch einen Bericht des *Business Insider* bekannt, dass die Bundeswehr im Rahmen des Pilotprojekts *Propaganda Awareness* automatisiert öffentlich zugängliche Informationen mit Bezug zur Künstler:innenvereinigung *Zentrum für Politische Schönheit* (ZPS) im Internet und Presseprodukten erfasst und verarbeitet hat (Kaleta & Fuchs, 2023). Verwendet wurde dafür eine eigens durch das Rüstungsunternehmen IABG entwickelte Software (Bundesregierung, 2023a). Anlass für diese inländische Überwachungsmaßnahme war eine Aktion im Jahr 2020, in der das ZPS im öffentlichen Raum auf den unklaren Verbleib von Waffen aus den Beständen der Bundeswehr hingewiesen hatte (Heidtmann, 2020).

Die automatisierte Verarbeitung öffentlich zugänglicher Daten durch staatliche Behörden ist kein harmloser Vorgang. Auch wenn die Daten öffentlich abrufbar sind, ist deren Erhebung und insbesondere deren Verarbeitung ein Eingriff in das Recht auf informationelle Selbstbestimmung und bedarf einer Rechtfertigung (Golla, 2022, S. 10). Die Intensität des Grundrechtseingriffs wird dadurch erhöht, dass die Bundeswehr hierbei heimlich und verdeckt vorging (Golla, 2022, S. 11). Außerdem wird das Eingriffsgewicht durch die Tatsache verstärkt, dass durch die automatisierte Datenanalyse neue Informationen generiert und weiterverarbeitet werden. Dies stellt neben der Erhebung der analysierten Daten einen zweiten Grundrechtseingriff dar. Um die Verhältnismäßigkeit solcher Maßnahmen zu gewährleisten, muss der Gesetz-

geber Eingriffsschwellen und Anordnungsvoraussetzungen für die systematische Erhebung auch öffentlich verfügbarer Daten gesetzlich vorgeben (BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, Rn. 103 ff.).

Über die genaue Funktionsweise der Software zur automatisierten Analyse von OSINT-Daten bei der Bundeswehr und die weitere Verknüpfung dieser Daten mit solchen aus anderen Erhebungsmethoden ist wenig bekannt. Eine Vermengung von OSINT-Daten mit Informationen, die beispielsweise gekauft wurden, haben dabei das Potenzial, Erkenntnisse und Personenprofile mit hoher Grundrechtsrelevanz zu ermöglichen. Zugleich erhöht sich das Risiko, dass Beschränkungen bei der Verarbeitung personenbezogener Daten wie die Zweckbindung oder das Kriterium der hypothetischen Neuerhebung unterlaufen werden (Wetzling & Dietrich, 2022). Nach der ersten Datenerhebung entstehen rechtliche Herausforderungen nämlich vor allem auch dann, wenn diese Daten später für andere Zwecke verwendet werden oder wenn sie mit anderen Erkenntnissen verknüpft werden. Das Bundesverfassungsgericht spricht hier von „additiven Grundrechtseingriffen“ und mahnt an, stets die gesamte Überwachungskette und die Wirkung der Gesamtheit der Maßnahmen im Blick zu behalten. Angesichts dieser Herausforderung muss der Gesetzgeber gewährleisten, dass das „Ausmaß der Überwachung insgesamt beschränkt bleibt“ (BVerfG, Urteil des Ersten Senats vom 26. April 2022, Rn. 287).

Zudem stellt sich die Frage, ob eine ausschließlich auf Aktivitäten im Inland gerichtete Aufklärungsmaßnahme der Bundeswehr im vorliegenden Fall überhaupt legitim sein kann. Es ist uns zumindest nicht ersichtlich, wie ein solcher Eingriff mit der engen verfassungsrechtlichen Begrenzung von Einsatz- und Eingriffsbefugnissen der Bundeswehr im Inland auf den Verteidigungs- und Spannungsfall, Inneren Notstand und den Fall der Amtshilfe in Einklang zu bringen ist (Conradi, 2020).

Auch aus der Zusammenarbeit mit einem privaten Unternehmen bei der Entwicklung der Software erwachsen Herausforderungen hinsichtlich des Schutzes der Grundrechte Betroffener (vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, Rn. 100f.). Schon bei der Vergabe des Projekts *Propaganda Awareness*, das mit einem Gesamtbudget von 3,5 Millionen Euro bemessen war (Bundesregierung, 2023a, S. 4), lagen offenbar Unregelmäßigkeiten vor (Kaleta & Fuchs, 2023). Für die Auswirkung auf Grundrechte bedeutender ist hier aber die „Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte“, wenn solche Software von privaten Unternehmen entwickelt und betrieben wird (BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, Rn. 100). Im vorliegenden Fall wurde dieses Risiko wiederum dadurch erhöht, dass die Anwendung auf den Servern der Firma IABG



ausgeführt wurden und so keine unmittelbare Kontrolle für die Bundeswehr vorlag (Bundesregierung, 2023a, S. 5).<sup>4</sup>

Auch wenn die Bundesregierung das konkrete Projekt *Propaganda Awareness* nicht weiter verfolgt (Bundesregierung, 2023a), sieht die Bundeswehr, ähnlich wie andere staatliche Behörden, in „kostenlos, kommerziell, online oder offline“ (cpm, 2022, S. 63) verfügbaren Informationen eine zunehmend wichtige Grundlage für die eigene Arbeit. Daher will sie die Erhebung und Verarbeitung solcher Informationen zukünftig mit deutlich mehr Ressourcen ausstatten (cpm, 2022, S. 63).

### 2.3.2. Signals Intelligence (SIGINT)

Neben der Erhebung und Verarbeitung von öffentlich verfügbaren Quellen nutzt die Bundeswehr auch diverse Techniken der (elektronischen) Fernmeldeaufklärung (SIGINT). Dieser Form der Informationsbeschaffung dienen zum einen die in Deutschland stationierten Einheiten der Fernmeldeaufklärung Nord und Süd, die durch ortsfeste, permanente Aufklärung Kommunikationsvorgänge auf große Entfernungen über die Staatsgrenzen hinaus erfasst. Darüber hinaus verfügt die Bundeswehr auch über mobile Systeme zur Fernmeldeaufklärung, die in Auslandseinsätzen Verwendung finden. Dabei werden Fahrzeuge für den Boden-, Luft- und Wassereinsatz mit Sensoren ausgestattet, die zum Erfassen von elektromagnetischen Signalen geeignet sind (Szandar, 2008). Sowohl im Rahmen der ortsfesten als auch der mobilen Fernmeldeaufklärung werden Funksprüche ebenso erfasst wie mobilfunkgestützte Telefonate (Gebauer & Schmid, 2019). In der Vergangenheit hörten beispielsweise deutsche Soldat:innen „mit Hilfe riesiger Antennen Funksprüche der Russen in Georgien ab, [und] belausch[t]en Telefonate der Taliban“ (Szandar, 2008). Dabei übersteigt die Menge der erhobenen Daten oft die Kapazitäten zur Auswertung (Szandar, 2008).

Wegen der wenigen öffentlichen Informationen hierzu ist indes unklar, ob und wie die Bundeswehr sich bei diesen Tätigkeiten ausschließlich auf die Kommunikation zwischen Angehörigen des Militärs beschränkt. Doch selbst wenn sich die Bundeswehr auf rein militärische Kommunikation beschränkt: Es ist ausgesprochen schwierig, im Kontext asymmetrischer Bedrohungen zwischen militärischen und zivilen Akteuren zu unterscheiden (Brissa, 2011, S. 397) und das Volumen der erfassten Kommunikation insgesamt entsprechend zu filtern und zu minimieren. Wie auch bei den Nachrichtendiensten ist hierbei das Erfassen eines unbeabsichtigten ‚Beifangs‘ – gemeint sind hier rein zivile Kommunikationsdaten – nicht zu verhindern. Mit wach-

<sup>4</sup> Pikanterweise ist eine rückwirkende Prüfung der im Rahmen dieses Pilotprojekts erhobenen und verarbeiteten Daten dadurch unmöglich gemacht worden, dass alle Daten des Projekts einen Tag vor Bekanntwerden dieser Maßnahme durch die öffentliche Berichterstattung gelöscht wurden (Kaleta & Fuchs, 2023).

sendem Einsatz von SIGINT-Maßnahmen bei der Bündnis- und Landesverteidigung wächst auch die Wahrscheinlichkeit unbeabsichtigter Eingriffe in Grund- und Menschenrechte. Betroffen sind davon beispielsweise das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung (siehe Kapitel 3.1).

Hierbei ist wichtig zu erwähnen, dass sich die Bundeswehr nicht nur auf Informationen aus eigens durchgeführten SIGINT-Aufklärungsaktivitäten stützt, sondern auch Daten nutzt und verarbeitet, die beispielsweise der BND erhoben hat. Letzterer darf im Rahmen strukturierter und automatisierter Übermittlungen Daten an die Bundeswehr weitergeben.<sup>5</sup> Öffentliche Details zum Ausmaß dieser Kooperation sind rar. Bereits im NSA-Untersuchungsausschuss wurde 2015 aber bekannt, dass diese Transfers bis zu 400 000 Gespräche und mehrere Millionen Metadaten betreffen können (Biermann, 2015). Die für diese Kooperation vorgesehenen Übermittlungsschwellen sind trotz mehrfacher Novellierungen des BND-Gesetzes noch immer sehr weit gefasst und stellen kaum eine tatsächliche Einschränkung dar (Bäcker, 2022, S. 124; Biermann, 2015).<sup>6</sup> Nach Auffassung der Beschwerdeführer einer aktuell vor dem Bundesverfassungsgericht anhängigen Klage gegen das BND-Gesetz fungiert der BND durch die Automatisierung dieser Übermittlungen hier nicht mehr als Überwachungsbehörde, sondern als bloßer „Datenlieferant der Bundeswehr“ (Bäcker, 2022, S. 125).

Insgesamt verfügt die Bundeswehr also über erhebliche Fähigkeiten zur direkten oder indirekten Erhebung von Informationen mittels Fernmeldeaufklärung.

### 2.3.3. Human Intelligence (HUMINT)

Für die Aufklärungstätigkeiten der Bundeswehr spielt darüber hinaus auch die Informationserhebung durch menschliche Quellen (HUMINT) eine wichtige Rolle. Der Abschlussbericht des Kundus-Untersuchungsausschusses des Bundestags ist hierfür eine der wenigen öffentlich verfügbaren und erhellenden Quellen. Ziel der Untersuchung war es, die Umstände und Verantwortlichkeiten im Zusammenhang mit einem

5 Seit 2021 gesetzlich geregelt ist in §24 Abs. 7 S. 2 BNDG, dass der BND personenbezogene Daten, die aus Telekommunikationsnetzen zur Eignungsprüfung ausgeleitet werden, automatisiert an die Bundeswehr übermitteln darf, sofern diese den Schutz von Leib, Leben oder Freiheit einer Person betreffen, oder Bezug zu den Aufgaben der Bundeswehr haben. Unter denselben Voraussetzungen dürfen grundsätzlich auch personenbezogene Daten mit dem Zweck der Gefahrenfrüherkennung automatisiert übermittelt werden (§29 Abs. 5 S. 2 BNDG). Mit dem im August 2023 durch das Bundeskabinett beschlossenen Gesetzesentwurf zur Änderung des BND-Gesetzes würde letztere Befugnis sich dann in §11b Abs. 3 wiederfinden. Zudem würden die Gefahrenbereiche, für die eine solche automatisierte Übermittlung möglich ist, deutlich erweitert und diese nun auch für Informationen aus Hacking-Operationen nach §34 BNDG ermöglicht.

6 So ist nach Auffassung der Beschwerdeführer einer beim BVerfG anhängigen Klage zum BNDG das Feld an Sachverhalten, bei denen argumentiert werden kann, dass tatsächliche Anhaltspunkte vorliegen, dass die Übermittlung der Daten vom BND an die Bundeswehr erforderlich ist, um „die Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung und bei Auslandseinsätzen §29 (5) Abs. 1)“ zu schützen, sehr weit gefasst.

Luftangriff der Bundeswehr auf zwei Tanklaster in Afghanistan im Jahr 2009 aufzuklären, bei dem es viele zivile Opfer gab.

Im Vorfeld der militärischen Entscheidung, ob die entführten Tanklaster bombardiert werden sollen, wurden sogenannte HUMINT-Kollektor:innen eingesetzt. Diese sollten das Angriffsziel verifizieren und weitere Informationen dazu einholen (Deutscher Bundestag, 2011, S. 238). Nach Auskunft der Bundeswehr arbeiten deutsche Soldat:innen „grundsätzlich offen und in Uniform“ (Bundeswehr, 2023c), um einen „nachrichtendienstlichen Charakter der Informationsgewinnung“ zu vermeiden (Deutscher Bundestag, 2011, S. 238). Fraglich ist aber, ob allein die Tatsache, dass Angehörige der Bundeswehr sich direkten Kontaktpersonen im Ausland in Uniform zeigen, ausreicht, um dem Erheben und der Verarbeitung von Informationen mittels HUMINT-Kollektor:innen einen nachrichtendienstlichen Charakter abzusprechen. Zum einen gehört die offene Befragung zum Instrumentarium der Quellensteuerung durch Nachrichtendienste, zum anderen werden Geldleistungen an Quellen gelegentlich so bemessen, dass diese noch Subinformanten bezahlen können (Deutscher Bundestag, 2011, S. 238). Bei einer solchen Konstellation lässt sich kaum noch sicherstellen, dass die Informationsbeschaffung keinen verdeckten Charakter hat, da der Auftraggeber dann nur über begrenzten Einfluss auf die Interaktion zwischen Informanten und Subinformanten verfügt. Wenn man hier, wie beispielsweise die SPD-Fraktion in ihrem Sondervotum im Kundus-Untersuchungsbericht, zum Schluss kommt, dass das Führen menschlicher Quellen die Schwelle zur nachrichtendienstlichen Tätigkeit überschreitet, ließe sich auch argumentieren, dass die Bundeswehr gegen geltendes Recht verstoße, da nachrichtendienstliches Handeln im Ausland nur dem BND und in eng begrenzten Fällen dem BAMAD vorbehalten ist (Brissa, 2011, S. 398).

In der Gesamtschau allein dieser drei ausgewählten Methoden der Informationsbeschaffung (OSINT, SIGINT und HUMINT) wird deutlich, dass die militärische Aufklärung eine Vielzahl von grundrechtsrelevanten Aktivitäten umfasst.



### 3. Grundrechtliche Relevanz des Militärischen Nachrichtenwesens und rechtsstaatliche Herausforderungen

Welche Eingriffe in Grund- und Menschenrechte gehen aber mit den oben beschriebenen Methoden der Informationsbeschaffung einher? Dies gilt es nun zu klären, da die Gewichtung von Grundrechtseingriffen maßgeblich über die Notwendigkeit einer einfachgesetzlichen Grundlage und die gebotene Prüftiefe der unabhängigen Kontrolle entscheidet.<sup>7</sup> Dabei sind eine Reihe von verfassungsrechtlichen Vorgaben und Standards zu bedenken, die wir in diesem Kapitel näher erörtern.

Vorab sollten wir aber klar herausstellen, dass die folgende Diskussion die Tätigkeiten der Bundeswehr *abseits* des Bündnis- und Verteidigungsfalles betreffen. Wir sind uns im Klaren darüber, dass viele verfassungsrechtliche Vorgaben bezüglich des Grundrechtsschutzes und der unabhängigen Kontrolle in einem solchen Fall nur eingeschränkt Geltung hätten.

#### 3.1. Verfassungsrechtliche Dimensionen und einschlägige Rechtsprechung

Laut BVerfG müssen grundsätzlich „Eingriffe in alle Grundrechte [...] auf einer gesetzlichen Ermächtigung beruhen, die dem Gebot der Normenklarheit und dem Bestimmtheitsgrundsatz genügt“ (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 137). Betroffene müssen also in der Lage sein, die Rechtslage zu erkennen, Rechtsfolgen abzuschätzen und ihr Verhalten danach auszurichten. Gerichte müssen zudem die Einhaltung dieser Maßstäbe überprüfen können. In Bezug auf die Erhebung und Verarbeitung personenbezogener Daten gilt dies verstärkt, wenn diese von den Betroffenen nicht bemerkt wird.<sup>8</sup> Eine effektive öffentliche Kontrolle der Einhaltung rechtsstaatlicher Standards wird zudem nahezu unmöglich, wenn der rechtliche Rahmen Verschlussache bleibt. Konkret fordert das Bundesverfassungsgericht daher im Urteil zum BND-Gesetz, die einfachgesetzliche Vorgabe der wesentlichen Grundlagen für die Auswertung von im Rahmen der Fernmeldeaufklärung erfassten Daten (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 192). Auch der Europäische Gerichtshof für Menschenrechte (EGMR) gibt in einem Urteil von 2018 vor, dass die verdeckte Ausübung von Überwachungsbefugnissen klarer und detaillierter Re-

7 Gemäß der vom Bundesverfassungsgericht entwickelten *Wesentlichkeitstheorie* ist nämlich der entscheidende Bewertungsmaßstab für die Notwendigkeit einer einfachgesetzlichen, und damit demokratisch legitimierten Grundlage für das Regierungshandeln, „inwieweit eine Maßnahme in Grundrechte des Einzelnen eingreift oder für die Verwirklichung von Grundrechten bedeutsam ist“ (Wissenschaftliche Dienste des Deutschen Bundestages, 2019; Schulze-Fielitz, 2015, Rn. 113 m.w.N.).

8 Denn die Konkretisierung der Befugnis kann in diesem Fall nicht wie sonst durch das Zwischenspiel von behördlichem Handeln und gerichtlicher Kontrolle erfolgen (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 137).

gelungen bedarf. Eine solche klare Regelung wird dabei angesichts der sich schnell entwickelnden Technologien, die zur Verarbeitung der Informationen zur Verfügung stehen, immer wichtiger (EGMR v. 13.09.2018, 58170/13, 62322/14 und 24960/15 (Big Brother Watch u.a. gg. das Vereinigte Königreich), Rn. 308). Der EGMR hat daher Mindestanforderungen für gesetzliche Grundlagen definiert, die das gezielte Abfangen von elektronischen Kommunikationsvorgängen im Rahmen von staatlicher Überwachung regeln sollen. Der zugrundeliegende Rechtsrahmen muss demnach folgende Kriterien vorgeben:

- Anordnungsvoraussetzung für die Grundrechtseingriffe;
- eine Bestimmung der Personengruppen, die von einem Eingriff betroffen sein können;
- eine Begrenzung der Dauer der Maßnahme;
- das Verfahren für die Auswertung, Verwendung und Speicherung der erhaltenen Daten;
- die Sicherheitsmaßnahmen, die bei der Übermittlung der Daten an andere Stellen zu treffen sind;
- und die Umstände, unter denen die ermittelten Daten gelöscht oder vernichtet werden können oder müssen (Big Brother Watch, 2018, Rn. 307).<sup>9</sup>

Wie die vorherigen Ausführungen zur OSINT-, SIGINT- und HUMINT-Praxis im Militärischen Nachrichtenwesen gezeigt haben, werden dort jenseits des Bündnis- und Verteidigungsfalls regelmäßig und systematisch personenbezogene Daten erhoben und verarbeitet. Davon betroffen sind zunächst überwiegend Angehörige fremder Streitkräfte aber auch Personen, bei denen es kaum tatsächliche Anhaltspunkte dafür gibt, dass von ihnen eine Gefahr für die militärischen Interessen der Bundeswehr oder die Sicherheit der Bundesrepublik ausgehen. Im Rahmen der „privilegierten Zusammenarbeit“ (Bundeskanzleramt, 2020, S. 80) der Bundeswehr mit dem BND erhält erstere zudem automatisiert personenbezogene Daten in unbekanntem Umfang zur weiteren Verarbeitung. Die Erhebung dieser Daten beim BND und die Verarbeitung dieser Daten auf Seiten der Bundeswehr unterliegen keinen ausreichenden gesetzlichen Beschränkungen; weder gibt es eine Zweckbindung, noch ist das Volumen begrenzt (Wetzling, 2021, S. 16f.). In diesen Kontexten, aber auch bei der Verwendung der erhobenen Daten in sogenannten *Cross-system-information-analysis-Plattformen*, wo Datenpunkte aus verschiedenen Überwachungstätigkeiten zusammenge-

<sup>9</sup> Für Massenüberwachungsmaßnahmen sind die ersten beiden Anforderungen aufgrund des präventiven Charakters nicht ohne Weiteres anwendbar. Auch in diesem Fall gibt der EGMR aber vor, dass der Gesetzgeber detaillierte Vorgaben zu den Bedingungen festlegt, unter denen diese Maßnahmen angeordnet werden können. Die anderen vier Anforderungen sind hierbei zu erfüllen, wie dies auch für gezielte Maßnahmen gilt (EGMR 25.05.2021, 35252/08 (Centrum För Rättvisa gg Schweden), 2021, Rn. 263).



führt werden,<sup>10</sup> stellt sich die Frage, ob es zu Grundrechtseingriffen kommt und ob diese gerechtfertigt sind.

Das Bundesverfassungsgericht hat sich schon einige Male mit dem Nachrichtendienstrecht beschäftigt und Vorgaben für die staatliche Überwachung gemacht. Ein Beispiel hierfür ist die Vorgabe, dass einige Überwachungsmaßnahmen vor Durchführung angeordnet und von einer unabhängigen Stelle freigegeben werden müssen. Dabei hat das Gericht auch die notwendigen Anordnungsvoraussetzungen konkretisiert: Beispielsweise bedarf es einer schriftlichen und gehaltvollen Begründung, dass eine angeordnete Maßnahme einen legitimen Zweck verfolgt. Zudem muss erörtert werden, ob tatsächliche Anhaltspunkte für eine bestimmte Gefahr bestehen. Das notwendige Anordnungsverfahren hat zudem einer Reihe wichtiger Kriterien und Vorgaben für die unabhängige Prüfung der Notwendigkeit und Zulässigkeit einer Maßnahme zu genügen. Hierbei muss zum Beispiel geklärt werden, ob mit der angeordneten Maßnahme möglicherweise geltende Begrenzungen der Überwachungstätigkeit überschritten werden.

Sollte man aus dieser Rechtsprechung auch Standards für die Aktivitäten des MilNW der Bundeswehr ableiten? Im Wesentlichen ist diese Frage mit ja zu beantworten, da alle staatlichen Behörden an die gleichen verfassungsrechtlichen Grundsätze der Bundesrepublik gebunden sind und die Grundrechte die gesamte deutsche Staatsgewalt auch bei ihren Tätigkeiten im Ausland binden.<sup>11</sup> Es kommt daher vor allem auf die Intensität der Grundrechtseingriffe und den gebotenen Schutz der Betroffenen an und weniger auf das Mandat der staatlichen Behörden, die den Grundrechtseingriff verantworten.

Gleichwohl gelten im Bereich der Verteidigung mitunter andere Handlungsprämissen als im Bereich der nationalen Sicherheit. Vermutlich lassen sich daher nicht alle Kriterien der Verhältnismäßigkeitsprüfung aus dem Nachrichtendienstrecht ohne Weiteres auch auf militärische Kontexte anwenden. Auch abseits des Verteidigungsfalls sind die Angehörigen fremder Armeen hinsichtlich des geltenden Grundrechtsschutzes aber nicht mit unbeteiligten Zivilist:innen gleichzusetzen. So wird beispielsweise die Argumentation angeführt, dass zum einen die im Fokus der militärischen Aufklärung stehenden Informationen zu militärischen Kapazitäten keine

10 Ein Beispiel für eine solche Software ist das vom Unternehmen *rola*. entwickelte Tool *rsIntCent*, das von der Bundeswehr seit 2011 verwendet (Bundesregierung, 2023a, S. 8) und mit folgenden Worten beworben wird: „Mit *rsIntCent* ist es dem Benutzer möglich, alle Daten effizient zu sammeln und vernetzt auszuwerten. Hierfür werden leistungsstarke, aber auch intuitiv zu bedienende Werkzeuge zur Verfügung gestellt, mit denen strukturierte und unstrukturierte Daten aggregiert werden können“ (rola Security Solutions GmbH, o. J.).

11 In seinem Grundsatzurteil zum BND-Gesetz vom Mai 2020 hat Karlsruhe ja nicht allein für den BND entschieden, dass die Grundrechte aus Art. 10 und Art. 5 GG keine „Deutschen-Rechte“, sondern Menschenrechte sind. Diese Argumentation wurde auch vom EGMR aufgegriffen (EGMR v. 12.09.2023, 64371/16 und 64407/16, (Wieder und Guarnieri gg. das Vereinigte Königreich).

Grundrechtsrelevanz haben und zudem gegnerische Streitkräfte als staatliche Hoheitsträger keine Grundrechtsträger sein können (Conradi, 2020, S. 123). Allerdings gilt insbesondere bei der systematischen Erhebung von personenbezogenen Daten im Rahmen von SIGINT- und OSINT- Maßnahmen stets zu bedenken, dass diese Methoden der Informationsbeschaffung in der Regel einen bedeutenden Anteil an Kommunikationsdaten aufgreifen, die eindeutig nicht den gegnerischen Streitkräften zuzuordnen sind.

Um die Diskussion weiter zu konkretisieren, identifizieren wir nun bestimmte Grundrechtseingriffe, die aus den Methoden der Informationsbeschaffung des MilNW erwachsen.<sup>12</sup> Ob es derzeit eine ausreichende Rechtsgrundlage für derartige Eingriffe gibt, erörtern wir im nächsten Kapitel.

### 3.1.1. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung<sup>13</sup>

Kommen wir noch einmal zurück auf den Fall des *Zentrums für Politische Schönheit*: Hier hatte die Bundeswehr im Rahmen des OSINT-Pilotprojekts *Propaganda Awareness* frei zugängliche Daten erhoben und verarbeitet – ein Eingriff, der möglicherweise das Grundrecht auf informationelle Selbstbestimmung verletzt. Dieses Grundrecht gewährleistet, dass einzelne Personen grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen dürfen (BVerfG, Beschluss des Ersten Senats vom 06. November 2019, Rn. 84). Der Schutz entfällt dabei nicht schon deshalb, weil die Informationen öffentlich zugänglich sind. Auch wenn sich eine Person in die Öffentlichkeit begibt, schützt das Recht der informationellen Selbstbestimmung ihr Interesse, dass die damit verbundenen personenbezogenen Informationen nicht automatisiert erhoben und möglicherweise weiterverwertet werden (BVerwG, Urteil vom 22.10.2014).

Im vorliegenden Fall hat die Bundeswehr persönliche Daten erhoben, ohne dass die betroffenen Personen des *Zentrums für Politische Schönheit* davon wussten, geschweige denn in die Datenverwendung einwilligen konnten. Insofern ist anzunehmen, dass die damalige Datenverarbeitung in das Recht auf informationelle Selbstbestimmung der Betroffenen eingriff. Um diesen und ähnliche Eingriffe zu rechtfertigen, bedarf es einer ausreichenden Rechtsgrundlage. Dass die Bundeswehr überhaupt nur sehr eingeschränkt im Inland tätig werden darf, verleiht dem Fallbeispiel besondere Brisanz.

<sup>12</sup> Dieser Impuls kann auch hier nur eine begrenzte Möglichkeit von potenziellen Eingriffsszenarien besprechen.

<sup>13</sup> Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist ein sonstiges Recht i.S.d. § 823 Abs. 1 BGB (BGH, Urteil vom 25. Mai 1954 – I ZR 211/53; BGH, Urteil vom 2. April 1957 – VI ZR 9/56).

Bei der Frage, unter welchen Umständen militärische Aufklärung in das Grundrecht auf informationelle Selbstbestimmung eingreifen darf, ist noch ein weiterer Punkt wichtig: Auch vermeintlich harmlos anmutende Datensätze aus öffentlich verfügbaren Quellen können in Kombination mit Daten, die auf andere Weise gewonnen wurden (z.B. aus SIGINT- oder HUMINT-Datensätzen), bestehende Personenprofile ergänzen und neue Erkenntnisse erzeugen. Datenverarbeitungen im Rahmen sogenannter *Cross-system-information-analysis-Plattformen* stellen eigenständige Grundrechtseingriffe dar. Das hat das Bundesverfassungsgericht im letzten Jahr dazu bewogen, den Gesetzgeber daran zu erinnern, die additive Wirkung der verschiedenen Überwachungsmaßnahmen zu berücksichtigen und auch bei zukünftigen Novellierungen des Rechtsrahmens staatlicher Überwachung zu berücksichtigen (BVerfG, Urteil des Ersten Senats vom 26. April 2022, Rn. 288).

### 3.1.2 Eingriffe in das Fernmeldegeheimnis

Wenn das Kommando Aufklärung und Wirkung der Bundeswehr oder eine der nachgeordneten Dienststellen (siehe Aufzählung in Abschnitt 2.1) Informationen durch Mittel der Fernmelde- und elektronischen Aufklärung (SIGINT) oder durch eine informationstechnische Operation der Cyberaufklärung erhebt, ist es oft nicht möglich, alle erhobenen Daten genau zuzuordnen. Insbesondere in hybriden Konfliktgeschehen gestaltet sich eine präzise Abgrenzung der Kommunikation von Angehörigen fremder Armeen von zivilen Kommunikationsvorgängen technisch, aber auch administrativ schwierig. In der Regel erfordert dies eine Datenminimierung und -filterung auf dem neuesten Stand der Technik. Doch auch wenn solche Technologie zum Einsatz kommt, kann kaum ausgeschlossen werden, dass unbeabsichtigt Daten unbeteiligter Dritter erhoben werden.

Insofern können wir davon ausgehen, dass die militärische Aufklärung der Bundeswehr Eingriffe in das Grundrecht nach Art. 10 Abs. 1 GG nach sich zieht. Hierbei ist es, wie bereits ausgeführt, zunächst unerheblich, ob es sich bei den betroffenen Personen um deutsche oder ausländische Staatsbürger:innen handelt. Abstriche kann es nach einschlägiger Rechtsprechung des Bundesverfassungsgerichts zwar in der Qualität des Grundrechtsschutzes geben; ein Eingriff in die Grundrechte bleibt es dennoch, und dieser erfordert eine einfachgesetzliche Grundlage.

### 3.1.3 Zwischenfazit

Das Militärische Nachrichtenwesen der Bundeswehr greift auf unterschiedliche Weise auch in die Grundrechte von Personen ein, die keiner fremden Streitkraft angehören und bei denen auch keine Anhaltspunkte dafür bestehen, dass von ihnen eine Gefahr für die militärischen Interessen oder die Sicherheit der Bundesrepublik Deutschland ausgehen. Verfassungsrechtlich, aber auch rechtspolitisch ist daher

nach unserer Auffassung eine einfachgesetzliche Grundlage für das Militärische Nachrichtenwesen dringend geboten. Die letzte Bundesregierung hat diese Auffassung explizit nicht geteilt (Bundesregierung, 2021). Auch von der aktuellen Bundesregierung scheint kein Impuls auszugehen, in dieser Legislaturperiode eine einfachgesetzliche Grundlage für das Militärische Nachrichtenwesen auf den Weg zu bringen. Gleichwohl mehren sich mittlerweile gewichtige Stimmen, die mit Verweis auf die Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshof für Menschenrechte eine einfachgesetzliche Grundlage einfordern – und das schon seit geraumer Zeit. So betonte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bereits im Jahr 2019: „Ich habe [...] schon immer vertreten, dass auch hier eine spezialgesetzliche Grundlage erforderlich ist“ (BfDI, 2019). Auch der Vorsitzende der G10-Kommission, Bertold Huber, stellte unlängst fest: „Anders als in Schweden mangelt es in der Bundesrepublik Deutschland an einer näheren einfachgesetzlichen Regelung, unter welchen Voraussetzungen das Militärische Nachrichtenwesen tätig werden kann“ (Huber, 2021). Auch ein Gutachten der Wissenschaftlichen Dienste des Bundestages gibt dieser Forderung viel Raum (Wissenschaftliche Dienste, 2020). Ein entsprechender Entschließungsantrag der Bundestagsfraktion Bündnis 90/Die Grünen fand allerdings keine politische Mehrheit (Deutscher Bundestag, 2021). Und so bleibt es bis auf Weiteres dabei: Eine einfachgesetzliche Grundlage fehlt, obwohl sie verfassungsrechtlich und politisch dringend geboten ist.

In vorangehenden Abschnitten haben wir gezeigt, welcher Rechtsrahmen nötig wäre und welche Defizite es gibt. Doch wie sieht der aktuelle Rechtsrahmen für die Tätigkeiten des MilNW eigentlich aus? Und warum ist er unzureichend? Dieser Frage gehen wir im folgenden Abschnitt nach.

### **3.2. Rechtsrahmen des Militärischen Nachrichtenwesens**

Statt das Militärische Nachrichtenwesen mit einem einfachgesetzlichen Rechtsrahmen auszustatten, der den oben dargestellten verfassungsrechtlichen Anforderungen genügt, wird bislang auf einzelne Normen im Grundgesetz rekuriert. Eingriffe der Bundeswehr in das Recht auf informationelle Selbstbestimmung sowie das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG werden insbesondere mit Art. 87a GG begründet. Dieser Artikel ist eine zentrale Norm für die Bundeswehr, die ihr Bestehen sowie die grundlegenden Fähigkeiten zur Verteidigung Deutschlands bestimmt. Eine weitere verfassungsrechtliche Norm, auf die abgestellt wird, um die Verarbeitung personenbezogener Daten durch die Bundeswehr zu rechtfertigen, ist Art. 24 Abs. 2 GG. Dieser Artikel ermöglicht es dem Bund, sich in Systeme gegenseitiger kollektiver Sicherheit einzuordnen und hierfür Beschränkungen seiner Hoheitsrechte zu akzeptieren. Diese beiden Normen genügen aber in keiner Weise den Anforde-

rungen des Bundesverfassungsgerichts an eine einfachgesetzliche Grundlage für Grundrechtseingriffe.

Die Verarbeitung personenbezogener Daten durch die Bundeswehr wird durch die anwendbaren Normen von Teil 1 und 2 und §85 Abs. 1 BDSG sowie durch die DSGVO geregelt (Bundesregierung, 2021, 2023). Genauere Bestimmungen stehen darüber hinaus in der zentralen Dienstvorschrift A-1100/8 zur Verarbeitung personenbezogener Daten im Militärischen Nachrichtenwesen (Bundesregierung, 2021) – diese ist uns als Verschlussache allerdings nicht zugänglich. Anders als andere öffentliche staatliche Stellen, die zur Erfüllung ihrer Aufgaben in Grundrechte eingreifen, wie die Bundespolizei oder die Nachrichtendienste des Bundes, legt der Bundestag hier also keinen einfachgesetzlichen Rechtsrahmen fest.

Teile der Literatur argumentieren, dass mit den Bundestagsbeschlüssen, die der Bundeswehr das jeweilige Einsatzmandat erteilen, eine solche einfachgesetzliche Grundlage vorliege und die Aktivitäten des Militärischen Nachrichtenwesens dadurch begrenzt würden (Conradi, 2020, S. 124; Löffelmann & Zöller, 2022, S. 21). Den Bestimmtheitsanforderungen für die gesetzliche Grundlage für Grundrechtseingriffe dieser Art können diese Beschlüsse aber keineswegs genügen, da diese Mandate schon nicht zwischen den genauen Tätigkeiten des Militärischen Nachrichtenwesens unterscheiden und darüber hinaus auch keine substantielle Begrenzung vornehmen.

Die angeführten Rechtsnormen werden so den Mindestanforderungen der nationalen und europäischen Rechtsprechung an den gesetzlichen Rahmen für staatliche Eingriffe in Grundrechte durch das verdeckte Erheben und Verarbeiten elektronischer Kommunikationsdaten nicht annähernd gerecht. Sie bilden daher keinen angemessenen Rechtsrahmen für die zahlreichen Grundrechtseingriffe durch das Militärische Nachrichtenwesen.

### **3.3. Unabhängige Kontrolle des Militärischen Nachrichtenwesens**

In der Praxis kann der Rechtsrahmen seine Wirkung nur dann entfalten, wenn kontinuierlich und unabhängig kontrolliert wird, ob Anordnungsvoraussetzungen erfüllt werden und die staatliche Überwachung verhältnismäßig ist. Die Bundesregierung der vergangenen Legislaturperiode war der Auffassung, dass das Militärische Nachrichtenwesen ausreichend dicht kontrolliert werde. Sie verwies darauf, dass die Kontrolle durch Gerichte, die Fachaufsicht durch das BMVg, den administrativen Datenschutzbeauftragten und den Beauftragten für den Datenschutz der Bundeswehr gewährleistet sei. Zudem würden der Verteidigungsausschuss des Bundestages sowie der BfDI als unabhängige Kontrollmechanismen eingebunden (Bundesregierung, 2021, S. 3).



Diese Auffassung hält einer kritischen Betrachtung jedoch nicht stand. Während die Fachaufsicht durch das BMVg und die Zuständigkeit der Datenschutzbeauftragten innerhalb des BMVg und der Bundeswehr nicht die Anforderungen einer *unabhängigen* Kontrolle erfüllen können, ist auch die Zuständigkeit der ordentlichen Gerichtsbarkeit ein schwaches Argument. Zwar gibt es hier einen hypothetischen individuellen Rechtsschutz; in der Praxis kann dieser aber nicht wirklich greifen, da die betroffenen Individuen wegen des verdeckten Vorgehens des Militärischen Nachrichtenwesens von den Maßnahmen in der Regel nichts erfahren. Ein unabhängiges Organ, das eine durchgängige effektive objektiv-rechtliche Kontrolle ausüben könnte, gibt es hier nicht.

Auch die Kontrolle durch den Verteidigungsausschuss, unterstützt durch die Wehrbeauftragte, genügt nicht den Anforderungen an eine unabhängige und effektive Kontrolle. Deren Mandat für das Militärische Nachrichtenwesen erwächst lediglich aus der allgemeinen Zuständigkeit für die Belange der Bundeswehr. Dies umfasst jedoch ein sehr weites Feld und führt dazu, dass eine Befassung in der gebotenen Tiefe kaum möglich ist. Im Gegensatz zur Kontrolle der Nachrichtendienste durch das PKGr erfolgt hier also keine ständige Kontrolle der Steuerung und Fachaufsicht der Bundesregierung hinsichtlich der Tätigkeiten des Militärischen Nachrichtenwesens.

Der BfDI prüft die Erhebung und Verarbeitung personenbezogener Daten im Rahmen des Militärischen Nachrichtenwesens (Sosna, 2022). In der Ausübung seiner Kontrolltätigkeit verfügt er jedoch über keinerlei Sanktionsbefugnisse. Dies bemängelt der BfDI in seinem Tätigkeitsbericht 2019 insbesondere vor dem Hintergrund der „eingeschränkten Rechtsschutzmöglichkeiten der Betroffenen“ (BfDI, 2019, S. 31). Bis zur Veröffentlichung des vorliegenden Impulses lag noch kein ausführlicher Bericht des BfDIs zum Militärischen Nachrichtenwesen vor.

Für die strategische Fernmeldeaufklärung des BND im Ausland und die damit verbundenen Grundrechtseingriffe betont das BVerfG die Notwendigkeit einer umfassenden, unabhängigen und kontinuierlichen Kontrolle. Auch das BVerfG und der EGMR stellen dabei wie der BfDI heraus, dass diese dort von elementarer Bedeutung ist, wo der Zugang zu gerichtlichem Rechtsschutz der betroffenen Individuen durch das verdeckte Vorgehen verhindert wird und deshalb kompensiert werden muss (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 272; EGMR, 04.12.2015, Roman Zakharov v. Russland, Rn. 233). In Widerspruch zu Art. 19 Abs. 4 GG und Art. 13 EMRK wird Betroffenen der militärischen Aufklärung hier kein effektiver Rechtsschutz gegen die staatlichen Maßnahmen zuteil.



Wie schon bei der fehlenden einfachgesetzlichen Grundlage werden auch die Kontrollmechanismen, welche die Bundesregierung für das Militärische Nachrichtenwesen vorsieht, den verfassungsgerichtlichen Anforderungen nicht gerecht.

### **3.4. Vergleichbarkeit der Tätigkeiten des Militärischen Nachrichtenwesens mit denen der Nachrichtendienste des Bundes**

Im Januar 2021 forderte die Bundestagsfraktion von Bündnis 90 / Die Grünen die Bundesregierung auf, eine der Rechtsprechung des BVerfG vom 19. Mai 2020 entsprechende einfachgesetzliche Grundlage für das Militärische Nachrichtenwesen zu erarbeiten und effektive Kontrollstrukturen anzulegen. Die Bundesregierung erwiderte, dass dieses Urteil sich nicht auf das Militärische Nachrichtenwesen auswirke. Ein zentrales Argument dabei lautete, dass diese Tätigkeiten nicht mit der Aufgabenwahrnehmung von Nachrichtendiensten des Bundes vergleichbar seien (Bundesregierung, 2021, S. 2).

Was ist von diesem Argument der Bundesregierung zu halten? Darum soll es im folgenden Abschnitt gehen.

#### **3.4.1. Mögliche Abgrenzungskriterien**

Als wesentliches Unterscheidungsmerkmal des Militärischen Nachrichtenwesens von den Tätigkeiten der Nachrichtendienste führt die Bundesregierung an, dass ersteres ausschließlich zur „Vorbereitung oder Durchführung von Auslandseinsätzen und der Landes- oder Bündnisverteidigung [...] in einem eng begrenzten Aufgabenbereich tätig“ sei (Bundesregierung, 2021, S. 2). Auch Löffelmann und Zöllner sehen hierin einen wesentlichen Unterschied zum BND, dessen Aufgabenradius mit dem „Sammeln und Auswerten von Information über Vorgänge von außen- und sicherheitspolitischer Bedeutung“ weiter gefasst sei (Löffelmann & Zöllner, 2022, S. 206). Die Fallbeispiele dieses Impulses zeigen allerdings, dass die Abgrenzung in der Praxis oft weniger klar ist. So hat das Militärische Nachrichtenwesen mit der Beobachtung des *Zentrums für Politische Schönheit* in die Grundrechte der Beteiligten eingegriffen, obwohl hier keine Verbindung zu bewaffneten Konflikten oder Einsatzmandaten besteht.

In der Literatur wird zudem eine Abgrenzung anhand der zur Verfügung stehenden Fähigkeiten als nicht zielführend eingeordnet, da das Militärische Nachrichtenwesen „über Methoden und Mittel verfügt, die für traditionelles nachrichtendienstliches Handeln wesensbestimmend sind“ (Brissa, 2011, S. 396; Deutscher Bundestag, 2011, S. 238; vgl. Löffelmann & Zöllner, 2022, S. 206). Wo – wie von uns in Kapitel 2 dargestellt – nachrichtendienstliche Methoden verwendet werden, sollten diese

Aktivitäten auch als nachrichtendienstliche Tätigkeiten eingeordnet werden (Singer, 2016, Rn. 125).

Diskutiert wird auch eine Unterscheidung anhand der Betroffenen der Überwachungsmaßnahmen. Löffelmann und Zöller argumentieren, dass beim Militärischen Nachrichtenwesen die Betroffenen hauptsächlich Kombattant:innen seien, während die Aktivitäten des BND grundsätzlich jede Person betreffen können (Löffelmann & Zöller, 2022, S. 206). Dass diese Feststellung nicht pauschal zutrifft, zeigt uns allerdings schon das bereits diskutierte Beispiel der Beobachtung des *Zentrums für Politische Schönheit*.

Es ist in der Praxis ohnehin schwierig, zwischen Angehörigen der Zivilbevölkerung und legitimen Zielen wie Kombattant:innen zu unterscheiden – insbesondere in hybriden Bedrohungslagen (Siemsen, 2018, S. 93). Auch technisch scheint eine Lösung, die den Anforderungen des BVerfG an wirksame Filterprozesse für abgefangene Kommunikationsdaten von Zivilist:innen genügt, nicht realisierbar (vgl. BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 173). Zum einen ist also fraglich, ob eine solche Begrenzung auf rein militärische Ziele überhaupt möglich ist. Siemsen argumentiert, zudem dass das Grundgesetz keinen unbegrenzten Eingriff in das Recht auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG erlaubt, selbst wenn der Einsatz einen militärischen Charakter hat (Siemsen, 2018, S. 78 f.). Auch die früher geläufige Begründung, dass deutsche Grundrechte nicht auf Kommunikationsvorgänge zwischen nicht-deutschen Staatsbürger:innen im Ausland anwendbar seien, ist seit dem Urteil des BVerfG zur strategischen Fernmeldeaufklärung des BND endgültig überholt (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020).

#### 3.4.2. Enge Verzahnung von Militärischem Nachrichtenwesen und BND

Außerdem besteht zwischen dem Militärischen Nachrichtenwesen und dem BND eine enge funktionale und organisatorische Verbindung. Dies liegt einerseits an den sich häufig ergebenden Überschneidungen der Zuständigkeitsbereiche (Binder, 2023, S. 134), andererseits an der institutionellen Aufgabenteilung. So nimmt der BND beispielsweise seit 2007 die zentrale Lagebeurteilung vor und führt damit eine essenzielle Aufgabe des Militärischen Nachrichtenwesens aus (Löffelmann & Zöller, 2022, S. 207). Bemerkenswert ist auch, dass der BND im Rahmen von Auslandseinsätzen der Bundeswehr sogenannte „Unterstützungselemente Militärisches Nachrichtenwesen“ führt, die ohne Dienstposten dem Einsatzkontingent angehören, und hier nachrichtendienstliche Aufgaben ausführen, „die in Zusammenhang mit der militärischen Auslandsaufklärung stehen“ (BVerwG, Urteil vom 30.06.2011, Rn. 20–21).

Über diese Einheiten hinaus sind mehr als zehn Prozent der BND-Angestellten Soldat:innen im Abordnungsverhältnis (Löffelmann & Zöller, 2022, S. 207). Die enge Verzahnung zwischen Militärischem Nachrichtenwesen und BND wird nicht zuletzt auch anhand der oben dargestellten automatisierten Datentransfers zwischen den Institutionen deutlich.

Dies zeigt, dass eine eindeutige und überzeugende Abgrenzung nachrichtendienstlicher Tätigkeiten von den Tätigkeiten des Militärischen Nachrichtenwesens kaum möglich ist – und zwar unabhängig davon, ob man die genutzten Methoden und Mittel, die Einsatzgebiete der Bundeswehr oder den Betroffenenkreis als Kriterium heranzieht. Darüber hinaus wirft auch die enge Verschmelzung der beiden Organisationen die Frage auf, ob für beide Bereiche nicht ähnliche Regelungen bestehen sollten. Aufgrund der zahlreichen funktionellen und organisationalen Überschneidungen erschließt sich nicht, warum für vergleichbare Grundrechtseingriffe unterschiedliche Standards gelten sollten. Und ein weiteres Problem kommt noch hinzu: Die Unterschiede bei Rechtsgrundlage und Kontrolldichte schaffen im schlechtesten Fall Anreize, die Asymmetrien auszunutzen und bestehende Einschränkungen zu umgehen.

### **3.5. Zwischenfazit**

Die Aufklärungsfähigkeiten der Bundeswehr sind eine wichtige Voraussetzung dafür, dass sie ihre Aufgaben effektiv ausüben kann. Das kann unter Umständen, auch außerhalb des Verteidigungsfalles, bedeuten, dass Grundrechtseingriffe gerechtfertigt sind. Allerdings müssen diese Überwachungsbefugnisse in einem Rechtsstaat begrenzt und kontrolliert werden. Der aktuelle, spärliche Rechtsrahmen und die rudimentären Kontrollmechanismen reichen nicht aus, um den verfassungs- und europarechtlichen Vorgaben zu genügen. Das Ergebnis sind nicht nur Probleme für die Rechtsstaatlichkeit und den Schutz von Grundrechten. Vielmehr führt der Ist-Zustand auch zu mangelnder Rechtssicherheit für die Angehörigen der Bundeswehr, die innerhalb des Militärischen Nachrichtenwesens für Überwachungsmaßnahmen zuständig sind.

Die Bundesregierung der vergangenen Legislaturperiode argumentierte, dass die vom BVerfG entwickelten Anforderungen an Gesetzgebung und Kontrollstrukturen für Grundrechtseingriffe bei staatlichen Überwachungstätigkeiten nicht auf das Militärische Nachrichtenwesen anwendbar seien. Diese Argumentation ist aber aus unserer Sicht nicht haltbar. Zum einen beschränkt das Verfassungsgericht diese Anforderungen nicht allein auf nachrichtendienstliches Handeln, weshalb grundsätzlich alle staatlichen Stellen an diese verfassungsrechtlichen Grundsätze gebunden sind. Insbesondere betrifft dies auch die Wirkung von Grundrechten im Ausland. Der vorausgehende Abschnitt zeigt überdies, dass die ehemalige Bundesregierung es sich mit der Behauptung zu leicht machte, wenn sie behauptet, die Tätigkeiten des



Militärischen Nachrichtenwesens seien nicht mit denen der Nachrichtendienste des Bundes vergleichbar. Im Gegenteil: Wir sehen kaum substanzielle Unterschiede, die begründen würden, dass die verfassungsrechtlichen Anforderungen für erstere nicht gelten müssen. Stattdessen müssen unserer Auffassung nach viele Aktivitäten des Militärischen Nachrichtenwesens als nachrichtendienstliche Tätigkeiten eingeordnet werden. Daraus folgt nach Art. 45d GG, dass der Bundestag die Zuständigkeit des PKGr auf das MilNW ausweiten müsste. Das bringt uns zum letzten Kapitel, in dem wir unterschiedliche Vorgehen zur Beseitigung dieser Defizite diskutieren.

## 4. Wege zur Überwindung rechtsstaatlicher Defizite

Angesichts der Defizite kann kaum noch bezweifelt werden, dass es für militärische Aufklärung einen einfachgesetzlichen Rechtsrahmen und eine umfassendere unabhängige Kontrolle braucht. Will die Ampelregierung ihrem eigenen Anspruch, eine „Fortschrittskoalition“ zu sein, gerecht werden, sollte sie eine Reform nicht länger aufschieben. Welcher aber ist der vielversprechendste Weg, diese rechtsstaatlichen Defizite zu beheben? Welche Form soll der einfachgesetzliche Rechtsrahmen für die militärische Aufklärung genau annehmen? Wo genau sollte dieser im bestehenden Sicherheits- bzw. Wehrrecht aufgehängt werden? Der Bundestag könnte hier zwischen verschiedenen Alternativen wählen: Ist es sinnvoller, ein eigenes Gesetz über das Militärische Nachrichtenwesen der Bundeswehr (MilNWG) zu errichten? Oder wäre es besser, die nachrichtendienstlichen Tätigkeiten der Bundeswehr in das bestehende Nachrichtendienstrecht einzupflegen? Denkbar wäre auch, ein umfassendes Bundeswehraufgabengesetz auf den Weg zu bringen. Zudem muss der Bundestag entscheiden, ob es für die unabhängige parlamentarische Kontrolle sowie die mögliche Rechtskontrolle der nachrichtendienstlichen Tätigkeiten der Bundeswehr eigenständiger Aufsichtsgremien bedarf. Möglich wäre auch, die bestehenden Mandate des parlamentarischen Kontrollgremiums, der G10-Kommission und des Unabhängigen Kontrollrats entsprechend auf diesen Bereich auszudehnen.

Bevor wir näher auf die konkreten Handlungsoptionen des Bundestages eingehen, lohnt sich zunächst der direkte Vergleich mit dem Nachrichtendienstrecht und der Nachrichtendienstkontrolle auf Bundesebene.

### 4.1. Orientierungshilfe aus dem Nachrichtendienstrecht

Trotz der unterschiedlichen Begebenheiten und Handlungsprämissen im militärischen und nachrichtendienstlichen Bereich kommen bei der Aufklärung durch die Bundeswehr gängige Methoden der nachrichtendienstlichen Informationsbeschaffung zum Einsatz. Die damit verbundenen Grundrechtseingriffe unterscheiden sich nicht wesentlich voneinander. Aufgrund der Vielzahl an Gerichtsurteilen und Gesetzesnovellierungen hat sich das Nachrichtendienstrecht in den letzten Jahren dynamisch weiterentwickelt. Es berücksichtigt heute deutlich mehr zentrale verfassungsrechtliche Vorgaben als früher. Weitere Schutznormen kommen aktuell noch



dazu.<sup>14</sup> Im Nachrichtendienstrecht sind zahlreiche, auch für die Bundeswehr einschlägige verfassungsrechtliche Vorgaben umgesetzt worden. Sie bieten eine gute Orientierungshilfe auf dem Weg zu einem einfachgesetzlichen Rechtsrahmen und einer höheren Kontrolldichte für die militärische Aufklärung.

#### 4.1.1. Rechtsrahmen für die Informationsbeschaffung

Wie im vorangehenden Kapitel beschrieben, kann die Bundesregierung derzeit nur auf wenige Artikel im Grundgesetz und pauschal auf das Bundesdatenschutzgesetz und die DSGVO verweisen, um den öffentlich einsehbaren Rechtsrahmen für die nachrichtendienstlichen Tätigkeiten der Bundeswehr zu beschreiben. Im direkten Vergleich mit dem Nachrichtendienstrecht bestehen starke Unterschiede: Allein das BND-Gesetz beinhaltet derzeit 69 Einzelvorschriften. Diese werden um weitere Gesetze zu Beschränkungsmaßnahmen des Grundrechts aus Art. 10 GG (Art. 10-Gesetz) und zur ständigen parlamentarischen Kontrolle nachrichtendienstlicher Tätigkeiten (PKGrG) ergänzt. Aktuell ist auch ein eigenständiges Gesetz zur Rechtskontrolle durch den Unabhängigen Kontrollrat (UKRat-G) Thema der Ressortabstimmung innerhalb der Bundesregierung (Unabhängiger Kontrollrat, 2023).



**Abbildung 03:** Überwachungsbefugnisse mit einfachgesetzlicher Grundlage im Nachrichtendienstrecht

Wichtiger als die Anzahl der Vorschriften oder Gesetze ist natürlich, welche Überwachungstätigkeiten Gegenstand einer einfachgesetzlichen Regelung sind. Einen groben Überblick darüber gibt die Abbildung 03. Sie stellt eine Auswahl an Über-

<sup>14</sup> Das betrifft beispielsweise auch klarere Vorgaben bezüglich der Übermittlung von personenbezogenen Daten an Behörden der öffentlichen Sicherheit und Verteidigung im In- und Ausland. Diese hatte das Bundesverfassungsgericht im Nachrichtendienstrecht bis zum 31.12.2023 gefordert. Das Bundeskabinett hat im September entsprechende Veränderungen im BND-Gesetz und im BVerfSch-Gesetz beschlossen, mit denen sich der Bundestag nun befassen wird. Bis zum Sommer 2024 will die Regierung eine umfangreichere Reform des Nachrichtendienstrechts beschließen.



wachungsbefugnissen dar, die im Nachrichtendienstrecht des Bundes mit eigenen Vorgaben zur rechtsstaatlichen Durchführung und Begrenzung versehen sind.

Das Militärische Nachrichtenwesen übt ganz ähnlich gelagerte Überwachungstätigkeiten aus, (siehe Kapitel 3.2.), ohne dass sie in ähnlicher Weise gesetzlich mandatiert und demokratisch legitimiert sind.

#### 4.1.2. Rechtliche Anforderungen und unabhängige Kontrolle

Ein ähnliches Bild ergibt sich, wenn man auf die Akteure und die konkreten Befugnisse der unabhängigen Kontrolle blickt. Auch hier sind die gesetzlichen Regelungen und die Kontrollmechanismen bei BND und MiNW sehr unterschiedlich gestaltet. Das illustrieren die folgenden Grafiken. Am Beispiel der technischen Aufklärung werden für BND und MiNW die jeweiligen rechtlichen Anforderungen und Kontrollbefugnisse vergleichend dargestellt.

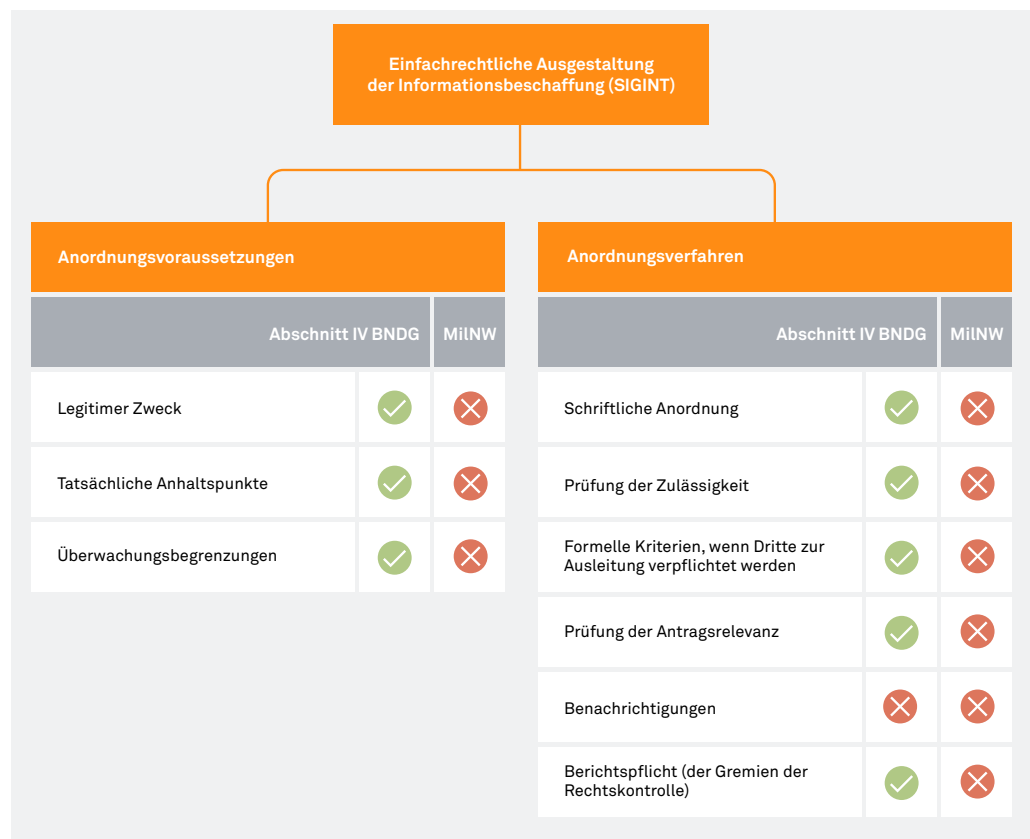


Abbildung 04:  
 Vergleich der rechtlichen Anforderungen der technischen Aufklärung



Unabhängige Kontrolle	Rechtskontrolle		
		BND (PKGr) Abschnitt IV BNDG	MiINW
	Genehmigungsverfahren (ex ante)	✓	✗
	Administrative Rechtskontrolle (ex post)	✓	✗
	Ständige parlamentarische Kontrolle		
		BND (PKGr) Abschnitt IV BNDG	MiINW (Verteidigungsausschuss)
	Steuerung und Fachaufsicht der Bundesregierung	✓	⊗
	Informations- und Sachaufklärungsrechte	✓	⊗
	Berichtspflicht	✓	⊗
	Personal	✓	⊗
Billigung der Wirtschaftspläne, Bauangelegenheiten und Mittelverwendung	✓	✗	
Kontrolle der Datenverarbeitung und Datenschutzkontrolle			
	BND (BfDI) Abschnitt IV BNDG	MiINW	
Verpflichtende Anhörung des BfDI vor Einrichtung von gemeinsamen Dateien	✓	⊗	
Anordnungsbefugnisse	✗	⊗	
Prüfbericht öffentlich	✓	⊗	

Abbildung 05: Vergleich der Kontrollbefugnisse im Bereich der technischen Aufklärung

Das Symbol ⊗ bedeutet, dass die jeweiligen Kontrolldimensionen zwar als Teil des gesetzlichen Kontrollauftrags des zuständigen Kontrollorgans gesehen werden könnten, in der Praxis aber nicht in der gebotenen Tiefe und Kontinuität zur Geltung kommen.



#### 4.1.3. Zwischenfazit

Aus der vergleichenden Betrachtung des Rechtsrahmens und der unabhängigen Kontrolle für ähnliche Überwachungsbefugnisse ergibt sich ein erhebliches Ungleichgewicht. Anders als bei den Nachrichtendiensten des Bundes sind die einzelnen Überwachungstätigkeiten des MilNW weder gesetzlich festgeschrieben, noch wird ihre Durchführung mit verfassungsrechtlich gebotenen Schutznormen und Verfahren zur unabhängigen Überprüfung der Rechtmäßigkeit flankiert.

Es mag sein, dass ein Teil der Vorgaben in internen und für die Öffentlichkeit nicht einsehbare Dienstvorschriften geregelt ist. Dabei darf es aber nicht bleiben. Bei der Abwägung, welche Regelungen formell-rechtlich festgelegt werden müssen und wo Vorgaben im Binnenrecht der Exekutive ausreichen, hat das Bundesverfassungsgericht eine wichtige Richtschnur vorgegeben: In Anlehnung an das Grundsatzurteil zum BND-Gesetz vom Mai 2020 sollten die „wesentlichen Grundlagen“ der Aufklärungstätigkeiten von Dienststellen im Geschäftsbereich des BMVg gesetzlich normiert werden. Konkrete Beispiele für Bestimmungen, die nicht länger ausschließlich in internen Dienstvorschriften der Exekutive geregelt werden dürfen, sind, beispielsweise, das „Gebot einer unverzüglichen Auswertung der erfassten Daten [...], die Geltung des Verhältnismäßigkeitsgrundsatzes bei der Auswahl der Suchbegriffe [...] Regelungen zum Einsatz von eingriffsintensiven Methoden der Datenauswertung, insbesondere komplexe Formen des Datenabgleichs [...] sowie die Beachtung der grundgesetzlichen Diskriminierungsverbote [...]. Zu regeln ist gegebenenfalls auch der Einsatz von Algorithmen, insbesondere die Sicherstellung ihrer grundsätzlichen Nachvollziehbarkeit in Blick auf eine unabhängige Kontrolle“ (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 192). Zudem sei der Einsatz von Algorithmen zu regeln und deren Nachvollziehbarkeit für die Kontrolle sicherzustellen. Wichtig ist darüber hinaus, dass die Einzelheiten, die weiterhin lediglich in einer eingestufteten Dienstvorschrift aufgeführt werden dürfen, „freilich einer unabhängigen objektivrechtlichen Kontrolle unterliegen“ sollten (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, Rn. 192).

Die Rechtmäßigkeit der Überwachungspraxis sollte also ständig unabhängig überprüft werden. Das kann aber nicht wie bisher allein vom BfDI geschultert werden. Zudem ist auch die parlamentarische Kontrolle unzureichend, wie Enrico Brissa bereits 2011 bemängelte: „Eine demokratische Kontrolle findet nur im Rahmen der allgemeinen parlamentarischen und den speziell für die Bundeswehr geschaffenen Kontrollmechanismen statt (Brissa, 2011, S. 398). Zwar lässt sich der Verteidigungsausschuss im Bundestag als parlamentarischer Untersuchungsausschuss nutzen, aber das entspricht bei weitem nicht einer funktionalen und ständigen parlamentarischen Kontrolle, wie sie beispielsweise das Parlamentarische Kontrollgremium für die Nachrichtendienste des Bundes ausübt. Eine demokratische Kontrolle des

Militärischen Nachrichtenwesens findet aufgrund dieser schwerwiegenden Defizite nur in einem unzureichenden Maße statt.

#### **4.2. Handlungsoptionen für den Bundestag**

Wir haben in diesem Impuls erläutert, dass die zahlreichen Grundrechtseingriffe des Militärischen Nachrichtenwesens völlig unzureichend gesetzlich legitimiert sind und dass die gebotene unabhängige Kontrolle nicht gegeben ist. Nun stellt sich die Frage, wie die notwendige Gesetzesgrundlage und die umfassendere Kontrolle am besten gestaltet werden könnten. Im Folgenden schauen wir uns die oben angedeuteten Optionen genauer an und diskutieren, warum ein einheitlicher Rechtsrahmen für alle nachrichtendienstlichen Tätigkeiten des Bundes der geeignetste Weg ist, die bestehenden Defizite zu überwinden.

##### **4.2.1. Bundeswehraufgabengesetz**

Anders als für die Nachrichtendienste oder auch für die Strafverfolgungsbehörden auf Bundes- und Landesebene gibt es für die Bundeswehr ganz allgemein keine eigenständige Gesetzesgrundlage. Denkbar wäre, nicht nur das Militärische Nachrichtenwesen, sondern das gesamte Handlungsspektrum der Exekutive im Bereich der Verteidigung in einem Bundeswehraufgabengesetz demokratisch zu legitimieren. Ein solches Vorgehen könnte das Regierungshandeln transparenter und nachvollziehbarer machen.

Es scheint aber nicht realistisch, dass ein solches Gesetz in der laufenden Legislaturperiode noch umgesetzt werden kann. Die Ampelkoalition hat diesbezüglich keine Vorgaben im Koalitionsvertrag gemacht; die zahlreichen Tätigkeiten der Bundeswehr, ihr komplexes Beschaffungswesen und ihre internationalen Kooperations-tätigkeiten im Rahmen der NATO und der EU würden ein komplexes und langwieriges Gesetzgebungsverfahren erforderlich machen. Mit Blick auf die unmittelbar drängende Notwendigkeit einer einfachgesetzlichen Grundlage für das Militärische Nachrichtenwesen würden wir einen anderen Weg vorschlagen.

##### **4.2.2. Militärisches Nachrichtenwesen-Gesetz**

Bei den Tätigkeiten der militärischen Aufklärung handelt es sich häufig um Methoden der Informationsbeschaffung, die von der Art her nachrichtendienstlichen Tätigkeiten entsprechen oder ihnen zumindest stark ähneln. Auch hinsichtlich der allgemeinen Grundrechtsrelevanz lassen sich keine großen Unterschiede feststellen. Analog zum Nachrichtendienstrecht auf Bundesebene könnte der Gesetzgeber daher ein eigenes Gesetz nur für das Militärische Nachrichtenwesen schaffen. Darin sollten in den jeweiligen Unterabschnitten das Mandat des MilNW und die einzelnen Tätigkei-

ten normenklar aufgeführt werden. In Anlehnung an das BND-Gesetz wäre in einem MilNW-Gesetz ein Großteil der verfassungsrechtlichen Vorgaben in ähnlicher Weise zu beachten, sofern sie nicht den Verteidigungsfall betreffen. Insbesondere die Befugnisse, die stark in Grundrechte eingreifen und nicht ausschließlich Angehörige fremder Armeen betreffen, wären so zu regeln, dass die gesetzliche Grundlage zulässige Anlassgefahren benennt und ein Anordnungs- und Genehmigungsverfahren für diese Tätigkeiten etabliert, sofern sie nicht den Verteidigungsfall betreffen. Dafür muss das Gesetz die wesentlichen Eingriffsschwellen, Anordnungsvoraussetzungen und Begrenzungen der Überwachungstätigkeit festschreiben. Zusätzlich sollte das Gesetz Vorgaben hinsichtlich der Verarbeitung, Kennzeichnung, Übermittlung und Löschung von Daten beinhalten.

Anders als bei einem deutlich komplexeren Bundeswehr-Aufgabengesetz wäre ein MilNW-Gesetz vermutlich noch in dieser Legislaturperiode realisierbar. Das setzt aber voraus, dass auch die unabhängige parlamentarische Kontrolle sowie die notwendige Rechtskontrolle auf diesen Bereich ausgeweitet werden und es dafür auch eigene Rechtsgrundlagen gibt. Angesichts der fehlenden Strukturen der unabhängigen Kontrolle im Bereich der Bundeswehr könnte der Gesetzgeber ein eigenes Gremium der ständigen parlamentarischen Kontrolle und ein neues Organ der Rechtskontrolle in Erwägung ziehen. Unserer Auffassung nach wäre es jedoch deutlich besser, das gesetzliche Mandat des bestehenden Parlamentarischen Kontrollgremiums sowie des Unabhängigen Kontrollrats auf das Militärische Nachrichtenwesen auszuweiten. Aus Sicht der Steuerzahlenden wäre es kaum nachvollziehbar, warum für sehr ähnlich gelagerte Prüfvorgänge gänzlich neue Aufsichtsgremien geschaffen werden sollten. Effizienter wäre es, bestehende Ressourcen und Expertise zu bündeln.

Jenseits der Frage der unabhängigen Kontrolle wäre es aber aufgrund der engen Verflechtung des MilNW mit dem BND (siehe Kapitel 3.4) vermutlich auch für die einzelnen Mitarbeiter:innen der beiden Institutionen schwierig, auf Grundlage unterschiedlicher Gesetze tätig zu werden.

#### 4.2.3. Einheitlicher Rechtsrahmen für alle nachrichtendienstliche Tätigkeiten des Bundes

Geeigneter und insbesondere langfristig am sinnvollsten erscheint uns daher, wenn Deutschland dem Modell anderer Demokratien wie Großbritannien und Kanada folgen und einen einheitlichen Rechtsrahmen für alle nachrichtendienstlichen Tätig-

keiten des Bundes schaffen würde.<sup>15</sup> Darunter ließen sich in einem Regel-Ausnahme-Verhältnis auch die diversen Tätigkeiten des Militärischen Nachrichtenwesens gut abbilden. Auch die unabhängige Kontrolle ließe sich bei so einem Vorgehen deutlich einfacher gestalten, indem bestehende Strukturen zur Anwendung kämen.

Im Regel-Ausnahme-Verhältnis, in dem zunächst ganz grundsätzlich die nötigen verfassungsrechtlichen Vorgaben zur Schaffung von Rechtmäßigkeit und Verhältnismäßigkeit festgeschrieben werden, ließen sich dann Ausnahmen formulieren, die in bestimmten Kontexten oder unter bestimmten Voraussetzungen das MilNW von den allgemeinen Vorgaben für nachrichtendienstliche Tätigkeiten des Bundes ausnehmen würden. Das erscheint insbesondere mit Blick auf die Verteidigungsfähigkeit und Resilienz der wehrhaften Demokratie in einigen klar zu begrenzenden Situationen sinnvoll. Nicht jeder Einsatz der Bundeswehr, in dessen Rahmen Aufklärungstätigkeiten stattfinden, kann wie die strategische Fernmeldeaufklärung des BND reguliert und kontrolliert werden. Das betrifft zum Beispiel Operationen, die im Verbund mit alliierten Armeen stattfinden, wie etwa in Mali. Der Verteidigungsfall, aber auch weitere Szenarien ließen sich mit dem Regel-Ausnahme-Verhältnis gut im Gesetzgebungsprozess abbilden. Somit würde auch dem Pauschalargument, eine gesetzliche Regelung des MilNW würde der Fähigkeit der Bundeswehr zur Landes- und Bündnisverteidigung schaden, der Wind aus den Segeln genommen.

Wir haben in diesem Kapitel lediglich drei unterschiedliche Handlungsoptionen für den Bundestag skizziert und bewertet. Egal welcher Weg gewählt wird, der Gesetzgeber sollte nicht länger zögern, die Aufklärungstätigkeiten der Bundeswehr endlich mit einer umfassenden Rechtsgrundlage auszustatten, die der Wesentlichkeitstheorie und dem Bestimmtheitsgebot (siehe Kapitel 3) des Bundesverfassungsgerichts in der Sache gerecht wird. Diese muss die mit Aufklärungstätigkeiten betrauten Stellen benennen und ihr Mandat beschreiben. Darüber hinaus sollte die Überwachungsbefugnisse, die in Grundrechte eingreifen, Anlassgefahren, Eingriffsschwellen und Anordnungsvoraussetzungen sowie Begrenzungen vorgeben.

15 Großbritannien hat sich im Zuge der nach den Enthüllungen von Edward Snowden im Jahr 2016 verabschiedeten Reformen einen einheitlichen Rechtsrahmen für alle nachrichtendienstlichen Tätigkeiten gegeben. Der Investigatory Powers Act unterscheidet zunächst einmal nicht danach, ob bestimmte Überwachungsbefugnisse von bestimmten Diensten ausgeübt werden, sondern stellt ganz allgemein ein einheitliches Regelwerk da für den Einsatz von staatlichen Überwachungsbefugnissen. In Kanada wurde mit der Schaffung der National Security and Intelligence Review Agency (NSIRA) ebenfalls ganz bewusst ein Weg beschritten, die unabhängige Kontrolle auf weitere nachrichtendienstliche Tätigkeiten des Staates auszuweiten, die nicht von den Nachrichtendiensten ausgeübt werden: „NSIRA will also build on the knowledge it has acquired of departments and agencies, such as the RCMP, the Canada Border Services Agency, Immigration, Refugees and Citizenship Canada, and the Department of National Defence and Canadian Armed Forces. Using that knowledge, NSIRA will ensure these organizations' national security or intelligence activities are independently verified and assessed. NSIRA is committed to transcending the silos that have characterized national security review until now, and will 'follow the thread' of an activity between agencies to ensure its assessments reflect the complex and interwoven approach Canada takes to national security” (NSIRA, 2020).

Aufgrund der vorhandenen Expertise, der knappen Ressourcen und der Effizienz der unabhängigen Kontrolle schlagen wir zudem vor, das Kontrollmandat des PKGr gesetzlich auf die Tätigkeiten des Militärischen Nachrichtenwesens auszuweiten. Zudem sollte, wo es der Grundrechtsschutz verlangt, das Mandat des Unabhängigen Kontrollrats ebenfalls auf die Prüfung der Rechtmäßigkeit der Überwachungstätigkeiten des Militärischen Nachrichtenwesens gesetzlich ausgedehnt werden. Somit würde auch ein weiterer Schritt dafür getan, dass die Aufsichtsgremien einen gesamtheitlichen Blick auf das Spektrum nachrichtendienstlicher Tätigkeiten des Bundes werfen können. Außerdem würde es weniger Anreize zur illegitimen Übermittlung von Daten an Stellen geben, die weniger intensiv kontrolliert werden, um Datenverarbeitungskontrollen zu umgehen.

#### **4.3. Weitere Empfehlungen zur Behebung rechtsstaatlicher Defizite**

Besondere Aufmerksamkeit sollte der Gesetzgeber auf die Kooperation der Bundeswehr mit Partnern im In- und Ausland richten. Die Übermittlung von personenbezogenen Daten an ausländische Partnerinstitutionen beinhaltet insbesondere dann schwerwiegende Risiken für den Grundrechtsschutz, wenn die Datenverarbeitung beim Empfänger ohne genügende Schutznormen praktiziert wird, beziehungsweise deren Einhaltung nicht kontrolliert wird. Um den notwendigen Grundrechtsschutz zu wahren und um möglichen Missbrauch der unterschiedlichen Datenschutzniveaus vorzubeugen, sollten diese Herausforderungen auf nationaler und internationaler Ebene offener diskutiert und Lösungen vorangetrieben werden.

Eine Handlungsmöglichkeit für den deutschen Gesetzgeber ist die automatisierte Übermittlung von Daten des Militärischen Nachrichtenwesens an Partnerinstitutionen an konkretere Bedingungen zu knüpfen. Für die Kooperation mit inländischen Behörden kann dies insbesondere bedeuten, die Kontrollbefugnisse des BfDI auszuweiten. Bisher ist dieser bei der stichprobenartigen Kontrolle gemeinsam geführter Dateien zwar in der Lage, Verstöße gegenüber der Fachaufsicht zu beanstanden. Da diese Beanstandungen in der Praxis jedoch häufig keine Handlungen der Exekutive nach sich ziehen, wären bindende Abhilfemaßnahmen an dieser Stelle für einen effektiven Grundrechtsschutz zielführend (Sosna, 2022). Die Zusammenarbeit mit ausländischen Behörden im Bereich des MilNW sollten auf Grundlage von Kooperationsvereinbarungen erfolgen, welche das Parlamentarische Kontrollgremium auch einsehen und gegebenenfalls beanstanden können sollte.

Im Rahmen dieses Impulses haben wir mehrfach die privilegierte Zusammenarbeit von BND und Bundeswehr thematisiert. Aus ihr erwachsen mehrere Gefahren: So kann der BND im Rahmen der Eignungsprüfung nach §24 Abs. 7 automatisiert personenbezogene Daten an die Bundeswehr übermitteln, ohne dass eine ausreichende Volumenbegrenzung oder Zweckbindung vorgeschrieben ist. Angesichts der fehlen-

den gesetzlichen Vorgaben für die Datenverarbeitung bei der Bundeswehr und der unzureichenden Ausgestaltung der unabhängigen Kontrolle besteht für den BND ein Anreiz, die strengeren eigenen Vorgaben im Rahmen der Kooperation mit der Bundeswehr zu umgehen.

Es gibt aber noch zahlreiche weitere Möglichkeiten, wie verfassungsrechtlich begründete Schutzrechte unterlaufen werden könnten. Eine davon hat die SPD-Bundstagsfraktion in ihrem Sondervotum zum Untersuchungsausschuss zum Luftangriff in Kundus thematisiert: Beispielsweise könnten „durch das MilNW gewonnene grundrechtsrelevante Erkenntnisse in präventiver oder repressiver Hinsicht durch andere staatliche Stellen im Inland“ verwendet werden. So könnten „Erkenntnisse des MilNW über den BND an andere Stellen – etwa Strafverfolgungsbehörden – gelangen, obwohl die gesetzlichen Beschränkungen, denen der BND bei der originären Gewinnung solcher Informationen unterlegen hätte, eventuell durch die Bundeswehr nicht eingehalten worden seien“ (Deutscher Bundestag, 2011, S. 237). Daher ist es wichtig, die gesetzlichen Regelungen der Übermittlungen zwischen Bundeswehr und den Nachrichtendiensten derart zu härten, dass keine Anreize für das Unterwandern von verfassungsrechtlichen Schutzwerten bestehen bleiben.

Aber natürlich kooperiert die Bundeswehr im Rahmen zahlreicher internationaler Verpflichtungen auch mit anderen Armeen bzw. mit den Institutionen innerhalb der NATO oder der EU, die die internationale militärische Zusammenarbeit koordinieren und steuern. Beispielsweise bezieht der Militärstab der Europäischen Union (EUMS) zur Vorbereitung von EU-Militäroperationen Daten und Informationen von den „national military intelligence agencies“ (Gruszczak, 2016, S. 112) – und auch hier ist vermutlich nicht allein der BND beteiligt. Jedwede Kooperation des Militärischen Nachrichtenwesens mit EU- und NATO-Strukturen ist bisher nicht in ausreichender Form gesetzlich geregelt. Idealerweise müssten die Mitgliedsstaaten bzw. die Parlamente der Mitgliedsstaaten einen Weg finden, eine multilaterale Kontrolle der multilateralen Überwachungs Kooperation von „national military intelligence agencies“ (Gruszczak, 2016, S. 112) anzuschließen. Zumindest im europäischen Kontext sollte man noch mehr dafür Sorge tragen, dass neben der Kooperation beim Austausch von Daten auch die Kooperation bei der Kontrolle mitgedacht wird.

## **5. Fazit**

Die Ampelkoalition hat sich im Koalitionsvertrag vorgenommen, die Kontrolle aller nachrichtendienstlichen Tätigkeiten des Bundes auszubauen. Bislang ist es bei der Ankündigung geblieben. Während die zuletzt vom Kabinett beschlossenen Gesetzesänderungen die Vorgaben des Bundesverfassungsgerichts zu Übermittlungsvorschriften umsetzen, bleibt sie Maßnahmen zur Ausweitung der Kontrolle der nachrichtendienstlichen Tätigkeiten des Bundes noch schuldig. Zwar gibt es bereits konkrete Vorschläge wie eine reformierte Kontrollstruktur aussehen soll (Flade, 2023; Wetzling & Vieth-Ditlmann, 2023; UK-Rat, 2023), davon ausgespart bleibt bisher jedoch das Militärische Nachrichtenwesen der Bundeswehr.

In diesem Impuls haben wir aber gezeigt, dass hier dringender Handlungsbedarf besteht. Die bisherige Praxis, diese bedeutsamen Aufklärungstätigkeiten in nicht-öffentlichen Dienstvorschriften zu regeln, genügt demokratischen und rechtsstaatlichen Standards nicht. Das Gleiche gilt für die aktuell unzureichenden Kontrollmechanismen. Um diesen Missstand zu beheben und zentrale Rechtslücken zu schließen, müssen die Bundesregierung und der Deutsche Bundestag das Militärische Nachrichtenwesen mit einem einfachgesetzlichen Rechtsrahmen ausstatten und wirksame Kontrollmechanismen einführen.

Dafür sollten sie sich an den Vorgaben des Verfassungsgerichts orientieren und Grundrechtseingriffe begrenzen (siehe Kapitel 3.1). So würde der Gesetzgeber das Vertrauen der Öffentlichkeit stärken und mehr Rechtssicherheit für die Soldat:innen schaffen. Ohne diese wichtigen Reformen ließe sich auch gegenüber autoritären Systemen deutlich weniger glaubhaft Rechtsstaatlichkeit und Demokratie einfordern.

Zudem soll durch die von der Bundesregierung angestrebte Reform des Nachrichtendienstrechts im Sommer 2024 auch die Kontrolle der Dienste angepasst werden. Wenn das Militärische Nachrichtenwesen im Rahmen dieser Reform nicht berücksichtigt wird, werden die Unterschiede hinsichtlich der Regelungsdichte für vergleichbare Grundrechtseingriffe durch staatliche Überwachung weiter zunehmen. In Kenntnis dieser Unterschiede können unliebsame Datenverarbeitungsregeln, die beispielsweise für den BND gelten, umgangen werden. Gerade im Kontext der „privilegierten Zusammenarbeit“ (Bundeskanzleramt, 2020, S. 80) zwischen BND und Bundeswehr besteht die Gefahr, dass der BND als „Datenlieferant der Bundeswehr“ (Bäcker, 2022) die geringere Kontroll- und Regelungsdichte im Militärischen Nachrichtenwesen ausnutzt.

Die anvisierte Reform des Nachrichtendienstrechts bietet dem Gesetzgeber eine gute Gelegenheit, eine seit langem bestehende Rechtslücke zu schließen. Er sollte



sie nicht ungenutzt verstreichen lassen und sich endlich auch der Tätigkeiten des Militärischen Nachrichtenwesens annehmen.



## Literatur

- Bäcker, M. (29.12.2022). Verfassungsbeschwerde. Verfügbar unter: [https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/BNDGII\\_Beschwerdeschrift\\_anonymisiert.pdf](https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/BNDGII_Beschwerdeschrift_anonymisiert.pdf)
- Biermann, K. (18.03.2015). BND-Überwachung: Warum schickt der BND der Bundeswehr abgehörte Daten? Die Zeit. Verfügbar unter: <https://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung>
- Big Brother Watch. (2018). The State of Surveillance in 2018. Verfügbar unter: <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/09/The-State-of-Surveillance-in-2018.pdf>
- Binder, A. (2023). Das Militärische Nachrichtenwesen der Bundeswehr. In J.-H. Dietrich, K. F. Gärditz, K. Graulich, C. Gusy und G. Warg (Hrsg.). Nachrichtendienste in vernetzter Sicherheitsarchitektur.
- Brissa, E. (2011). Militärischer Auslandsgeheimdienst der Bundeswehr. Grundlagen und Grenzen des Militärischen Nachrichtenwesens. DöV, 391–398.
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). (2019). Tätigkeitsbericht 2017 und 2018 zum Datenschutz. Verfügbar unter: <https://dserver.bundestag.de/btd/19/098/1909800.pdf>
- Bundeskanzleramt. (2020). Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts. Verfügbar unter: <https://www.bundesregierung.de/resource/blob/976020/1823782/3074e1071c01c425e-00d2ae81ffa907e/2020-12-01-refe-bnd-gesetzentwurf-data.pdf?download=1>
- Bundeskanzleramt. (2023). Entwurf eines Gesetzes zur Änderung des BND-Gesetzes. Verfügbar unter: <https://dserver.bundestag.de/brd/2023/0436-23.pdf>
- Bundesministerium der Verteidigung (BMVg). (2023). 17. Bericht des Bundesministeriums der Verteidigung zu Rüstungsangelegenheiten: Teil 1. Verfügbar unter: <https://www.bmvg.de/resource/blob/5639826/45547a72b96fb60d6d82f061913d-9d3a/17-ruestungsbericht-data.pdf>
- Bundesregierung. (2021). Antwort der Bundesregierung auf die Kleine Anfrage B90/Die Grünen – Rechtsgrundlage und Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr. Verfügbar unter: <https://dserver.bundestag.de/btd/19/261/1926114.pdf>
- Bundesregierung. (2023a). Antwort der Bundesregierung auf die Kleine Anfrage der Bundestagsfraktion Die Linke. Verfügbar unter: <https://dserver.bundestag.de/btd/20/058/2005854.pdf>
- Bundesregierung. (2023b). Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts. Verfügbar unter: <https://dserver.bundestag.de/btd/20/086/2008626.pdf>
- Bundesregierung. (2023c). Entwurf eines Gesetzes zur Änderung des BND-Gesetzes. Verfügbar unter: <https://dserver.bundestag.de/btd/20/086/2008627.pdf>

- Bundeswehr. (2022). Bataillon Elektronische Kampfführung 911. Verfügbar unter: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum/kommando-aufklaerung-wirkung/bataillon-elektronische-kampffuehrung-911>
- Bundeswehr. (2023a). Kommando Cyber- und Informationsraum. Verfügbar unter: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum>
- Bundeswehr. (2023b). Fernmeldeaufklärungszentrale Nord. Verfügbar unter: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum/kommando-aufklaerung-wirkung/fmaufklzentr-nord>
- Bundeswehr. (2023c). Methoden der Informationsgewinnung. Verfügbar unter: <https://www.bundeswehr.de/de/aktuelles/meldungen/so-arbeitet-militaerisches-nachrichtenwesen>
- Conradi, A. (2020). Das Militärische Nachrichtenwesen der Bundeswehr: Operative und rechtliche Dimensionen. In J.-H. Dietrich, K. F. Gärditz, K. Graulich, C. Gusy und G. Warg (Hrsg.). Nachrichtendienste in vernetzter Sicherheitsarchitektur.
- cpm. (2022). CIR 2.0 Von der Idee zur Dimension Verfügbar unter: <https://publish.flyeralarm.digital/cpmforum-sonderausgabe-cir-2-0-von-der-idee-zur-dimension/#66>
- Deutscher Bundestag. (2021). Entschließungsantrag Fraktion BÜNDNIS 90/DIE GRÜNEN: Legitimität und Leistungsfähigkeit der Nachrichtendienste stärken – Kontrolle auf allen Ebenen verbessern und ausbauen. Verfügbar unter: <https://dserver.bundestag.de/btd/19/262/1926221.pdf>
- Deutscher Bundestag. (2011). Beschlussempfehlung und Bericht des Verteidigungsausschusses als 1. Untersuchungsausschuss gemäß Artikel 45a Absatz 2 des Grundgesetzes. Beschlussempfehlung. Verfügbar unter: <https://dserver.bundestag.de/btd/17/074/1707400.pdf>
- Flade, F. (2023, September 6). Die große Geheimdienst-Reform.
- Gebauer, M. & Schmid, F. (16.01.2019). Bundeswehr: So überführte der MAD den Iran-Spion. Der Spiegel. Verfügbar unter: <https://www.spiegel.de/politik/deutschland/bundeswehr-so-ueberfuehrte-der-mad-den-iran-spion-a-1248397.html>
- Golla, S. (2022). Grundrechtliche Eingriffe durch Internetauswertungen (S. 9–13). In Polizei.Wissen. Heft 1/2022.
- Gruszczak, A. (2016). Military Intelligence in the EU. Intelligence Security in the European Union (S. 95–121). Palgrave Macmillan.
- Heidtmann, J. (26.10.2020). Aktionskunst vom ZPS: Wo sind all die Waffen hin? Süddeutsche.de. Verfügbar unter: <https://www.sueddeutsche.de/kultur/zentrum-politische-schoenheit-waffen-1.5093956>
- Huber, B. (2021). Strategische Fernmeldeaufklärung und die Rechtsprechung des EGMR. Neue Zeitschrift für Verwaltungsrecht, Beilage 1 zu Heft 24/2021, 1–44.

- Joshi, S. (03.07.2023). The war in Ukraine shows how technology is changing the battlefield. The Economist. Verfügbar unter: <https://www.economist.com/special-report/2023/07/03/the-war-in-ukraine-shows-how-technology-is-changing-the-battlefield>
- Kaleta, P. & Fuchs, T. (15.01.2023). Spionageaffäre: Wie die Bundeswehr mit Hilfe von künstlicher Intelligenz Künstler und Kritiker im Inland überwacht. Business Insider. Verfügbar unter: <https://www.businessinsider.de/politik/spionageaffaere-wie-die-bundeswehr-mit-hilfe-von-kuenstlicher-intelligenz-kuenstler-und-kritiker-im-inland-ueberwacht-c/>
- Löffelmann, M. & Zöller, M. A. (2022). Nachrichtendienstrecht. Nomos VG.
- National Security and Intelligence Review Agency (NSIRA). (2020). 2021–22 Departmental Plan. Verfügbar unter: <https://nsira-ossnr.gc.ca/html/2021-2022/index-eng.html>
- rola Security Solutions GmbH. (o. J.). Militärische und Nachrichtendienstliche Aufklärung, Auswertung, Analyse und Reporting. Verfügbar unter: <https://www.rola.com/rsintcent/>
- Schulze, M. (2020). Militärische Cyber-Operationen. No. 15. Berlin: Stiftung Wissenschaft und Politik. Verfügbar unter: <https://www.swp-berlin.org/publikation/militaerische-cyber-operationen>
- Schulze-Fielitz, H. (2015). Art. 20 (Rechtsstaat). In D. Horst (Hrsg.), Grundgesetz Kommentar: GG (3. Auflage, Bände 1–3, Band 2). Mohr Siebeck.
- Siemsen, A. E. M. (2018). Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrosoldaten (1. Auflage). Duncker & Humblot.
- Singer, J. (2016). Praxiskommentar zum Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes: Kontrollgremiumgesetz – PKGrG. Berlin, Heidelberg: Springer.
- Sosna, S. (2022). Der BfDI – ein Kontrollorgan unter dem Radar? Zeitschrift für das Gesamte Sicherheitsrecht, Heft 6, 245.
- Szandar, A. (01.09.2008). Strategische Aufklärung: Bundeswehr belauscht die Welt. Der Spiegel. Verfügbar unter: <https://www.spiegel.de/politik/deutschland/strategische-aufklaerung-bundeswehr-belauscht-die-welt-a-575417.html>
- Unabhängiger Kontrollrat. (01.08.2023). Diskussionsentwurf eines Gesetzes über den Unabhängigen Kontrollrat und zur Änderung des BND-Gesetzes. Verfügbar unter: [https://ukrat.de/DE/UKRatG/UKRatG-Diskussionsentwurf.pdf?\\_\\_blob=publicationFile&v=2](https://ukrat.de/DE/UKRatG/UKRatG-Diskussionsentwurf.pdf?__blob=publicationFile&v=2)
- Wetzling, T. (21.02.2021). Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts. Verfügbar unter: <https://www.bundestag.de/resource/blob/823556/760abb7961fa7df144e1bc834702d44f/A-Drs-19-4-731-F-data.pdf>

- Wetzling, T. & Dietrich, C. (2022). Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform? Berlin: SNV. Verfügbar unter: <https://www.stiftung-nv.de/en/publication/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier>
- Wetzling, T. & Vieth-Ditlmann, K. (2023). Mehr Rechtskontrolle wagen. Verfügbar unter: [https://www.stiftung-nv.de/sites/default/files/snv\\_impuls\\_mehr\\_rechtskontrolle\\_wagen.pdf](https://www.stiftung-nv.de/sites/default/files/snv_impuls_mehr_rechtskontrolle_wagen.pdf)
- Wissenschaftliche Dienste des Deutschen Bundestages. (2019). Kriterien der Wesentlichkeitslehre des Bundesverfassungsgericht. WD 3-3000-152/19. Deutscher Bundestag. Verfügbar unter: <https://www.bundestag.de/resource/blob/655254/1764b49aa3c85458a840652cf134e031/WD-3-152-19-pdf-data.pdf>
- Wissenschaftliche Dienste des Deutschen Bundestages. (2020). Gesetzesvorbehalt bei der Fernmelde- und elektronischen Aufklärung der Bundeswehr im Ausland. Verfügbar unter: <https://www.bundestag.de/resource/blob/709162/5919d437e3c4957ff5d14061b09cddad/WD-3-151-20-pdf-data.pdf>

## Rechtsprechung

- Bundesverfassungsgericht. (2023). Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 –, Rn. 1–178. (2023). Verfügbar unter: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216\\_1bvr154719.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html)
- Bundesverfassungsgericht. (2022). Urteil des Ersten Senats vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 1–407. (2022). Verfügbar unter: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2022/04/rs20220426\\_1bvr161917.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2022/04/rs20220426_1bvr161917.html)
- Bundesverfassungsgericht. (2020). Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 – Rn. 1–332. Urteil des Ersten Senats vom 19. Mai 2020. Bundesverfassungsgericht. Zugriff am 17.8.2023. Verfügbar unter: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519\\_1bvr283517.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html)
- Bundesverfassungsgericht. (2019). Beschluss des Ersten Senats vom 06. November 2019 – 1 BvR 16/13 –, Rn. 1–157. Verfügbar unter: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106\\_1bvr001613.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106_1bvr001613.html)
- Bundesverwaltungsgericht. (2014). Urteil vom 22.10.2014 – 6 C 7.13. Verfügbar unter: <https://www.bverwg.de/221014U6C7.13.0>
- Bundesverwaltungsgericht. (2011). Urteil vom 30.06.2011 – 2 A 3.10. Verfügbar unter: <https://www.bverwg.de/de/300611U2A3.10.0>
- Europäischer Gerichtshof für Menschenrechte. (12.09.2023). Wieder and Guarnieri v. United Kingdom. 64371/16 und 64407/16. Verfügbar unter: <https://hudoc.echr.coe.int/i=001-226468>
- Europäischer Gerichtshof für Menschenrechte. (25.05.2021). Centrum För Rättvisa v. Sweden. 35252/08. Verfügbar unter: <https://hudoc.echr.coe.int/fre?i=001-210078>
- Europäischer Gerichtshof für Menschenrechte. (13.09.2018). Big Brother Watch and Others v. the United Kingdom. 58170/13, 62322/14 und 24960/15. Verfügbar unter: <https://hudoc.echr.coe.int/fre?i=001-186048>
- Europäischer Gerichtshof für Menschenrechte. (04.12.2015). Zakharov v. Russia. 47143/06 Verfügbar unter: <https://hudoc.echr.coe.int/fre?i=001-159324>

## **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**

**Corbinian Ruckerbauer** ist für die SNV im Bereich „Digitale Grundrechte, Überwachung & Demokratie“ tätig. Er koordiniert das European Intelligence Oversight Network (EION), das Nachrichtendienstkontrollleur:innen und anderen Expert:innen eine Plattform für regelmäßigen und strukturierten Austausch bietet. Er gehört zum Redaktionsteam von about:intel, einer Diskussionsplattform, die Expert:innen zu einem sektor- und länderübergreifenden Dialog zusammenbringt, um drängende Fragen an der Schnittstelle von Technologie, Überwachung und Demokratie zu diskutieren.

**Dr. Thorsten Wetzling** leitet das Themenfeld „Digitale Grundrechte, Überwachung & Demokratie“ in der Stiftung Neue Verantwortung. Dort stehen die verschiedenen Formen des sicherheitsbehördlichen Zugangs und der Verarbeitung von personenbezogenen Daten im Fokus unterschiedlicher Projektarbeiten. Dabei geht es häufig um rechtspraktische Fragen, ob und wie der Einsatz moderner Überwachungstechnologie vom Gesetzgeber rechtsstaatlich einzuhegen und von den unabhängigen Aufsichtsbehörden effektiv und umfassend zu kontrollieren ist.

## **So erreichen Sie die Autoren**

Corbinian Ruckerbauer  
[cruckerbauer@stiftung-nv.de](mailto:cruckerbauer@stiftung-nv.de)

Dr. Thorsten Wetzling  
[twetzling@stiftung-nv.de](mailto:twetzling@stiftung-nv.de)



## Impressum

Stiftung Neue Verantwortung e. V.  
Ebertstraße 2  
10117 Berlin

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

[www.stiftung-nv.de](http://www.stiftung-nv.de)  
[info@stiftung-nv.de](mailto:info@stiftung-nv.de)

Design:  
Make Studio  
[www.make-studio.net](http://www.make-studio.net)

Layout:  
Thorsten Kirchhoff  
Visuals:  
Alina Siebert



Dieser Beitrag unterliegt einer CreativeCommons-Lizenz (CC BY-SA). Die Vervielfältigung, Verbreitung und Veröffentlichung, Veränderung oder Übersetzung von Inhalten der Stiftung Neue Verantwortung, die mit der Lizenz „CC BY-SA“ gekennzeichnet sind, sowie die Erstellung daraus abgeleiteter Produkte sind unter den Bedingungen „Namensnennung“ und „Weiterverwendung unter gleicher Lizenz“ gestattet. Ausführliche Informationen zu den Lizenzbedingungen finden Sie hier: <http://creativecommons.org/licenses/by-sa/4.0/>