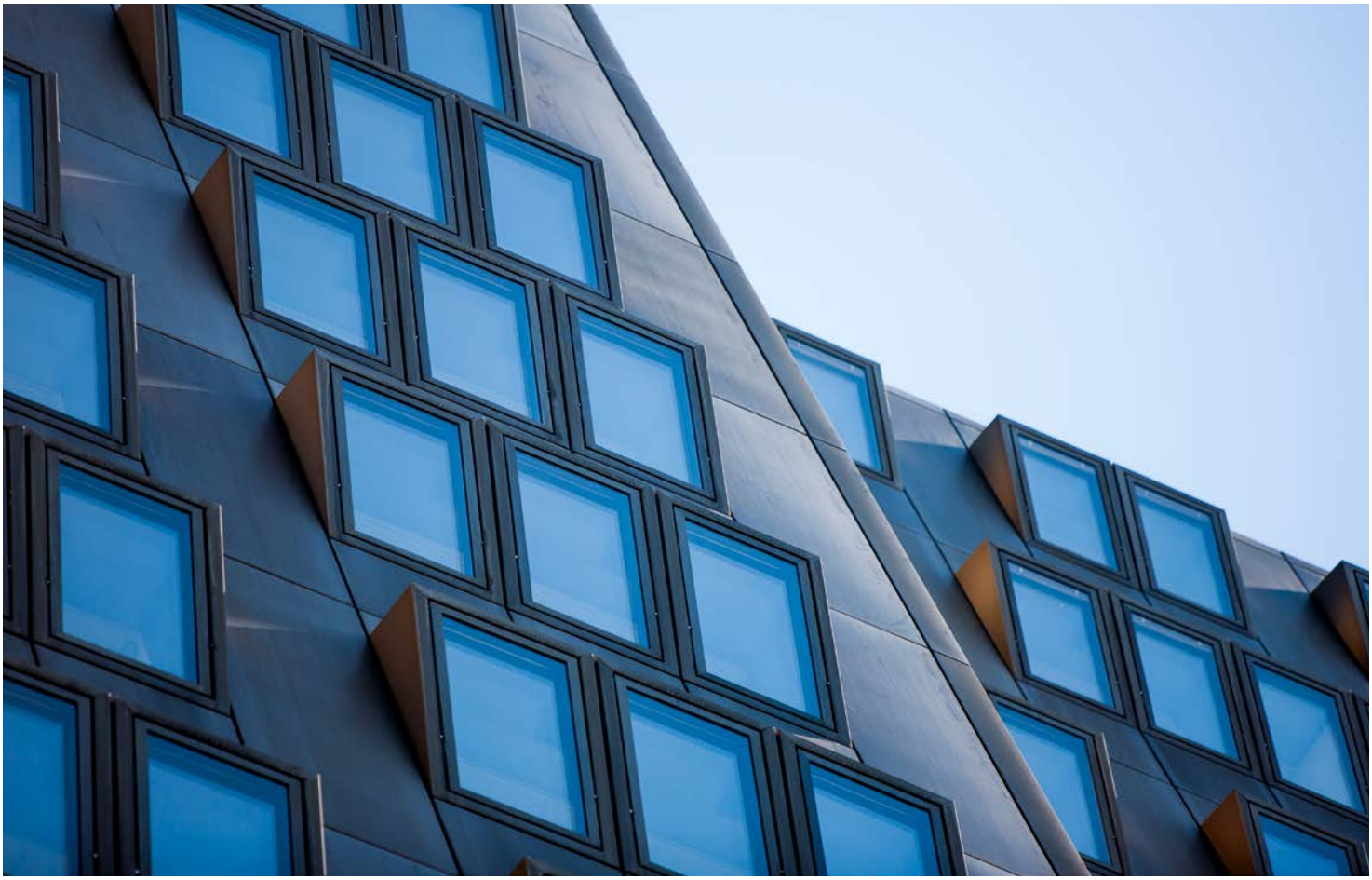
Rechnungshof Österreich

Unabhängig und objektiv für Sie.

IKS-Elemente der Spionageprävention im Innenministerium, Verteidigungsministerium und Außenministerium

Reihe BUND 2026/19

Bericht des Rechnungshofes



III-344 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVIII. GP
Rechnungshof GZ 2026-0.456.236 (005.287)

Vorbemerkungen

Vorlage

Der Rechnungshof erstattet dem Nationalrat gemäß Art. 126d Abs. 1 Bundes-Verfassungsgesetz nachstehenden Bericht über Wahrnehmungen, die er bei einer Gebarungsüberprüfung getroffen hat.

Berichtsaufbau

In der Regel werden bei der Berichterstattung punkteweise zusammenfassend die Sachverhaltsdarstellung (Kennzeichnung mit 1 an der zweiten Stelle der Textzahl), deren Beurteilung durch den Rechnungshof (Kennzeichnung mit 2), die Stellungnahme der überprüften Stelle (Kennzeichnung mit 3) sowie die allfällige Gegenäußerung des Rechnungshofes (Kennzeichnung mit 4) aneinandergereiht.

Das in diesem Bericht enthaltene Zahlenwerk beinhaltet allenfalls kaufmännische Auf- und Abrundungen. Der vorliegende Bericht des Rechnungshofes ist nach der Vorlage über die Website des Rechnungshofes www.rechnungshof.gv.at verfügbar.

Prüfkompetenz des Rechnungshofes

Zur Überprüfung der Gebarung des Bundes, der Länder, der Gemeindeverbände, der Gemeinden und anderer durch Gesetz bestimmter Rechtsträger ist der Rechnungshof berufen. Der Gesetzgeber versteht die Gebarung als ein über das bloße Hantieren mit finanziellen Mitteln hinausgehendes Verhalten, nämlich als jedes Verhalten, das finanzielle Auswirkungen (Auswirkungen auf Ausgaben, Einnahmen und Vermögensbestände) hat. „Gebarung“ beschränkt sich also nicht auf den Budgetvollzug; sie umfasst alle Handlungen der prüfungsunterworfenen Rechtsträger, die finanzielle oder vermögensrelevante Auswirkungen haben.

IMPRESSUM

Herausgeber:
Rechnungshof Österreich
1030 Wien, Dampfschiffstraße 2

www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im Juni 2026

AUSKÜNFTE

Rechnungshof
Telefon (+43 1) 711 71 – 8946
E-Mail info@rechnungshof.gv.at
Bluesky: @rhsprecher.bsky.social
facebook/RechnungshofAT

FOTOS

Cover, S. 6, 7: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art.	Artikel
BBG	Bundesbeschaffung GmbH
BGBl.	Bundesgesetzblatt
BlgNR	Beilagen zu den stenografischen Protokollen des Nationalrats
BMEIA	Bundesministerium für europäische und internationale Angelegenheiten
BMI	Bundesministerium für Inneres
BMLV	Bundesministerium für Landesverteidigung
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
bzw.	beziehungsweise
d.h.	das heißt
DSN	Direktion Staatsschutz und Nachrichtendienst
ELAK	elektronischer Akt
ErläutRV	Erläuterungen zur Regierungsvorlage
etc.	et cetera
EU	Europäische Union
EUR	Euro
(f)f.	folgend(e)
GmbH	Gesellschaft mit beschränkter Haftung
GP	Gesetzgebungsperiode
GZ	Geschäftszahl
i.d.(g.)F.	in der (geltenden) Fassung
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie
InfoSiG	Informationssicherheitsgesetz
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnologie
leg. cit.	legis citatae (der zitierten Vorschrift)
lit.	litera (Buchstabe)

Mio.	Million
NATO	North Atlantic Treaty Organization (Nordatlantische Vertragsorganisation)
OGH	Oberster Gerichtshof
OSINT	Open Source Intelligence (Nachrichtengewinnung aus frei verfügbaren Quellen)
rd.	rund
RH	Rechnungshof
S.	Seite
SNG	Staatsschutz- und Nachrichtendienst-Gesetz
TZ	Textzahl
u.a.	unter anderem
VBÄ	Vollbeschäftigungsäquivalent
vgl.	vergleiche
Z	Ziffer
z.B.	zum Beispiel

IKS-ELEMENTE DER SPIONAGEPRÄVENTION IM INNENMINISTERIUM, VERTEIDIGUNGSMINISTERIUM UND AUSSENMINISTERIUM

Das Innen-, das Verteidigungs- und das Außenministerium verfügten jeweils über ein Internes Kontrollsystem mit Elementen zur Spionageprävention. Regelungen und Maßnahmen waren in Dienstvorschriften dokumentiert, Bedienstete wurden darin unterwiesen und regelmäßig fortgebildet. Die Überwachung, ob die Regelungen des Internen Kontrollsystems eingehalten wurden, ist eine Management- bzw. Führungsaufgabe, die die bzw. der jeweilige Vorgesetzte wahrzunehmen hat. Nur im Rahmen regelmäßiger Kontrollen kann das erwartete Schutzniveau aufrechterhalten werden.

STRATEGISCHE RAHMENBEDINGUNGEN

Die österreichische Bundesregierung legte dem Nationalrat im Jahr 2024 eine neue Sicherheitsstrategie vor, die den Veränderungen der nationalen und internationalen Sicherheitslage – auch im Bereich der Spionage – Rechnung tragen sollte. Die Veränderungen im geopolitischen Umfeld gestalteten sich seit 2022 dynamischer als im vorangegangenen Jahrzehnt. Auch wenn strategische Ziele im Optimalfall für einen längeren Zeitraum Gültigkeit haben sollten, war nicht auszuschließen, dass geopolitische Entwicklungen kurzfristig Veränderungs- oder Anpassungsbedarf anstoßen konnten.

SPIONAGEPRÄVENTION – PERSONAL

Das Innen-, das Verteidigungs- und das Außenministerium sahen Überprüfungen ihres Personals vor. Die Sicherheitsüberprüfung (nach dem Sicherheitspolizeigesetz) setzten das Innen- und das Außenministerium bei Personalaufnahmen ein. Personal der Direktion Staatsschutz und Nachrichtendienst (DSN) war einer Vertrauenswürdigkeitsprüfung zu unterziehen. Das Verteidigungsministerium nahm eine Verlässlichkeitsprüfung (nach dem Militärbefugnisgesetz) vor.

Die Überprüfungen des Personals waren darüber hinaus Voraussetzung für den Zugang zu Informationen höherer Klassifizierungsstufen, aber auch für den Zutritt zu militärischen Liegenschaften oder zur DSN. Sie waren in unterschiedlichen zeitlichen Abständen zu erneuern und erfassten nicht alle Personen mit Einblick in sensible Bereiche des Verfassungsschutzes.

Die Veränderungen im geopolitischen Umfeld – insbesondere infolge des Krieges in der Ukraine sowie verstärkter Spionagetätigkeit – hatten zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt. Diese Dynamik spiegelte sich im Erfordernis personeller und finanzieller Ressourcen

zur Spionageprävention wider. Das Innenministerium erhöhte die diesbezüglichen Ressourcen vor allem ab Einrichtung der DSN mit Dezember 2021; die Anträge der DSN auf eine Personalaufstockung in allen Bedrohungsbereichen und im Konkreten auch im Bereich Spionageabwehr waren Anfang 2025 aber noch nicht vollständig umgesetzt. Auch für das Abwehramt im Verteidigungsministerium waren zusätzliche personelle Ressourcen für die militärische Spionageabwehr erforderlich.

SPIONAGEPRÄVENTION – INFORMATION

Ein Informationsaustausch zur Spionageprävention zwischen Innen-, Verteidigungs- und Außenministerium und auf internationaler Ebene fand in unterschiedlichen Formaten statt, z.B. im Nationalen Sicherheitsrat, in der Arbeitsgruppe Hybride Bedrohungen und in der Kerngruppe Desinformation.

Der Umgang mit Informationen, die einer besonderen Geheimhaltung unterlagen (sogenannte klassifizierte Informationen), war durch das Informationssicherheitsgesetz geregelt. Außerhalb des Gesetzes bestimmte die Geheimschutzordnung des Bundes den Umgang mit klassifizierten Informationen. Die Sanktionierung von Verstößen war im internationalen und im nationalen Geheimschutz unterschiedlich.

SPIONAGEPRÄVENTION – BESCHAFFUNGEN

Die Überprüfung von Unternehmen, die in vertraglicher Beziehung zum Bund stehen, war nur eingeschränkt möglich. Eine rechtliche Grundlage war das Informationssicherheitsgesetz, das auf eine sichere Verwendung klassifizierter Informationen abstellte. Spezifische Aspekte der Spionageprävention waren davon nicht umfasst. Die personenbezogenen Überprüfungen (Sicherheitsüberprüfung, Verlässlichkeitsprüfung) beruhten auf einer Selbstauskunft der überprüften Personen. Mangels gesetzlicher Grundlage war es nicht möglich, nachrichtendienstliche Informationen heranzuziehen sowie zivile und militärische Informationen zu Unternehmen auszutauschen.

WIRKUNGSBEREICH

- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung
- Bundesministerium für europäische und internationale Angelegenheiten

IKS-Elemente der Spionageprävention im Innenministerium, Verteidigungsministerium und Außenministerium

Prüfungsziel

Der RH überprüfte von Oktober 2024 bis Mai 2025 im Innenministerium, im Verteidigungsministerium sowie im Außenministerium den Präventionsmechanismus, mit dem Spionagevorfälle verhindert werden sollen. Die Gebarungsüberprüfung erfolgte gemäß Art. 126b Abs. 4 Bundes-Verfassungsgesetz aufgrund eines Antrags gemäß § 99 Abs. 2 Geschäftsordnungsgesetz 1975 des Abgeordneten Douglas Hoyos-Trauttmansdorff und weiterer Abgeordneter vom 15. Mai 2024. Ziele der Gebarungsüberprüfung waren insbesondere die Darstellung und Beurteilung rechtlicher Grundlagen für die Spionageprävention, der Maßnahmen des Internen Kontrollsystems, der Beschaffungen von IT-Infrastruktur sowie der Zusammenarbeit im Bereich der Spionageprävention.

Kurzfassung

Spionage und Spionageprävention

Die Begriffe Spionage bzw. Spionageabwehr waren gesetzlich nicht definiert. Das Strafgesetzbuch stellte das Einrichten, Betreiben oder Unterstützen eines geheimen Nachrichtendienstes zum Nachteil der Republik Österreich unter Strafe. Das Verständnis der überprüften Bundesministerien von Spionage bzw. Spionageabwehr war inhaltlich ausreichend deckungsgleich: Das Beschaffen und Erlangen von unbekannten, geschützten Informationen unter Einsatz nachrichtendienstlicher Methoden. (TZ 2)

Rechtliche und strategische Rahmenbedingungen

Spionageabwehr bzw. -prävention ist eine Querschnittsmaterie. Ausgehend von der inhaltlichen Definition der Spionage – Beschaffen und Erlangen von unbekannten, geschützten Informationen unter Einsatz nachrichtendienstlicher Methoden – fanden sich in mehreren Gesetzen Grundlagen der Spionageprävention: z.B. im Bundes-Verfassungsgesetz, im Strafgesetzbuch, im Militärbefugnisgesetz und im Informationssicherheitsgesetz. (TZ 3)

Die Regierungsprogramme seit 2020 enthielten strategische Ziele zur Bekämpfung von Spionage. Die österreichische Bundesregierung hatte im Jahr 2024 eine neue Sicherheitsstrategie vorgelegt, die den Veränderungen der nationalen und internationalen Sicherheitslage der letzten Jahre – auch im Bereich der Spionage – Rechnung trug. Eine Überarbeitung dieser beschloss die Bundesregierung im April 2025. (TZ 5)

Im Innenministerium waren Gefahrenerforschung und -abwehr im Bereich Spionage von Anfang 2017 bis Ende November 2021 im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (**BVT**) angesiedelt. Mit Einrichtung der Direktion Staatsschutz und Nachrichtendienst (**DSN**) mit Dezember 2021 gingen die Aufgaben auf diese über. Im Verteidigungsministerium waren das Abwehramt und das Heeres-Nachrichtenamt für die nachrichtendienstliche Aufklärung und Abwehr eingerichtet. Das Außenministerium war auf Grundlage des Art. 9 des Wiener Übereinkommens über diplomatische Beziehungen (in der Folge: **Wiener Übereinkommen**) berechtigt, ohne Angabe von Gründen Diplomatinnen und Diplomaten zur unerwünschten Person (persona non grata) zu erklären und sie aufzufordern, das Land zu verlassen. (TZ 6)

Personelle und finanzielle Ressourcen zur Spionageprävention

Die Veränderungen im geopolitischen Umfeld (TZ 5) führten zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung personeller und finanzieller Ressourcen zur Spionageprävention einzubeziehen. (TZ 7, TZ 8, TZ 9, TZ 10, TZ 11, TZ 12)

Das Innenministerium erhöhte die personellen Ressourcen für die Spionageabwehr im überprüften Zeitraum (1. Jänner 2017 bis 1. Jänner 2025), vor allem ab Einrichtung der DSN mit Dezember 2021. Der Personalstand in Vollbeschäftigungsäquivalenten (**VBÄ**) lag am 1. Jänner 2025 bei 207 % des Wertes vom 1. Jänner 2017. Gleichzeitig stiegen im Hinblick auf internationale Entwicklungen und die veränderte Bedrohungslage die Anforderungen an die DSN insgesamt und insbesondere auch

im Bereich der Spionageabwehr. Dies kam u.a. auch durch den starken Anstieg der Auszahlungen für Mehrdienstleistungen zwischen 2017 und 2024 – insbesondere ab 2022 – auf 373 % des Ausgangswerts 2017 zum Ausdruck. (TZ 7)

Die Auszahlungen des Innenministeriums für den Staatsschutz und den Nachrichtendienst verdreifachten sich zwischen 2017 und 2024. Von 2017 bis 2021 stiegen sie moderat, ab 2022 stark. Der vergleichsweise hohe Anteil des Sachaufwands im Jahr 2022 war insbesondere auf IKT-Investitionen im Zusammenhang mit dem Aufbau der DSN zurückzuführen. (TZ 8)

Die im Abwehramt spezifisch für den Bereich der Spionageabwehr zur Verfügung stehenden Personalressourcen verdoppelten sich von 2017 bis 2024; dies war im Wesentlichen mit der Umsetzung eines neuen Organisationsplans im Jahr 2022 und internen Umschichtungen begründet. Die durch die internationale Bedrohungslage – insbesondere infolge des Krieges in der Ukraine sowie verstärkter Spionagetätigkeit – gestiegenen Anforderungen an die militärische Spionageabwehr verursachten allerdings Bedarf an zusätzlichen personellen Ressourcen, was sich u.a. auch in einer deutlichen Steigerung der Auszahlungen für Mehrdienstleistungen in diesem Bereich zeigte. Die Auszahlungen für Mehrdienstleistungen blieben von 2017 bis 2021 nahezu unverändert, ab 2022 stiegen sie markant auf das Dreieinhalbfache im Jahr 2024. (TZ 9)

Wegen der fehlenden budgetären Zuordnung sowie der Änderung der Budgetstruktur im überprüften Zeitraum war es nicht möglich, valide Zahlen zu den finanziellen Ressourcen zu erheben, die den Nachrichtendiensten des Bundesheeres und konkret dem Abwehramt insgesamt bzw. der Spionageabwehr zur Verfügung standen; auch war die Entwicklung der Auszahlungen in diesem Bereich nicht zuverlässig darstellbar. (TZ 10)

Im Außenministerium war keine spezifische Organisationseinheit für Spionageabwehr zuständig, entsprechende Aufgaben waren auf mehrere Abteilungen verteilt. Zwischen 1. Jänner 2017 und 1. Jänner 2025 stieg der Personalstand in den primär mit diesem Aufgabenbereich befassten Abteilungen auf knapp mehr als das Doppelte. (TZ 11)

Daten zum Einsatz finanzieller Ressourcen im Außenministerium für dessen Aufgabenerfüllung lagen vor. Finanzielle Ressourcen im Zusammenhang mit Spionageprävention – die keine explizite Aufgabe des Außenministeriums war – waren nicht gesondert ausgewiesen. (TZ 12)

Spionageprävention im Internen Kontrollsystem

Ein Internes Kontrollsystem (**IKS**) ist ein in die Arbeits- und Betriebsabläufe einer Organisation eingebetteter Prozess, der von den Führungskräften sowie den Mitarbeiterinnen und Mitarbeitern durchgeführt wird. Ziel ist, bestehende Risiken zu erfassen und mit ausreichender Gewähr sicherstellen zu können, dass die Organisation im Rahmen der Erfüllung ihrer Aufgaben ihre Ziele erreicht. Das IKS muss auf eine Minimierung dieser Risiken im laufenden Geschäftsprozess mittels angemessener organisatorischer und technischer Maßnahmen ausgerichtet sein. (TZ 13)

Das Innen-, das Verteidigungs- und das Außenministerium identifizierten als Risiken im Zusammenhang mit Spionage den Geheimschutz (z.B. Informationsabfluss), Schutz von Rechtsgütern (z.B. Zutritt Unberechtigter) und den Schutz des eigenen Personals (z.B. vor Anwerbungsversuchen). (TZ 14)

In den überprüften Bundesministerien war der Bereich Spionageprävention kein eigener oder vom allgemeinen IKS getrennter Bestandteil. Vielmehr sollten unterschiedliche, nicht explizit auf die Spionageprävention und -abwehr ausgelegte IKS-Elemente im Zusammenspiel auch das Spionagerisiko reduzieren. Das Außenministerium arbeitete seit 2023 an der Implementierung eines Informationssicherheitsmanagementsystems mit dem Ziel, das IKS zu verstärken. (TZ 14)

Im Innen- und im Außenministerium bestand gemäß Geschäftseinteilung keine spezifische IKS-Zuständigkeit betreffend Spionageprävention. Jede Organisationseinheit setzte IKS-Maßnahmen für den ihr zugewiesenen Aufgabenbereich um. Zentrale Vorgaben an die Ausgestaltung des IKS für den Bereich Spionageprävention bestanden auch im Verteidigungsministerium nicht. Die Geschäftseinteilung des Verteidigungsministeriums wies die Angelegenheiten der militärischen Sicherheit und der bzw. des Sicherheits- und Informationssicherheitsbeauftragten der nachrichtendienstlichen Abwehr zu. Die Verantwortung für Regelungen des IKS für Spionageprävention war bei der nachrichtendienstlichen Abwehr zentralisiert. (TZ 14)

Geheimschutz

Das Informationssicherheitsgesetz und die Informationssicherheitsverordnung regelten den Umgang mit Informationen, die einer besonderen Geheimhaltung unterliegen (klassifizierte Informationen) und die Österreich im Einklang mit völkerrechtlichen Regelungen erhält („internationaler Geheimschutz“). Klassifizierte Informationen sind materielle und immaterielle Informationen, unabhängig von Darstellungsform und Datenträger, die aufgrund ihres Inhalts einer besonderen Geheimhaltung bedürfen. Sie waren daher nur für einen begrenzten Personenkreis

zugänglich und besonders gegen Kenntnisnahme und Zugriff durch Unbefugte geschützt. (TZ 15, TZ 16)

Der Umgang mit klassifizierten Informationen außerhalb des Anwendungsbereichs des Informationssicherheitsgesetzes („nationaler Geheimschutz“) war in der Geheimschutzordnung des Bundes geregelt. Das Innen-, das Verteidigungs- und das Außenministerium setzten die Geheimschutzordnung des Bundes um. (TZ 15)

Im Jahr 2024 arbeitete das Bundeskanzleramt an einem Entwurf für ein novelliertes Informationssicherheitsgesetz. Mit ihm sollten nationale und internationale klassifizierte Informationen gleich behandelt und in einem Gesetz geregelt werden. (TZ 15)

Der internationale und der nationale Geheimschutz sahen ein nach den Auswirkungen eines Missbrauchs der Information abgestuftes Klassifizierungssystem vor, mit den vier Klassifizierungsstufen „EINGESCHRÄNKT“, „VERTRAULICH“, „GEHEIM“ und „STRENG GEHEIM“. Bedienstete, die eine klassifizierte Information erstellten, mussten diese Information den Klassifizierungsstufen zuordnen. Dabei war das Ausmaß der Schädigung der Geheimschutzinteressen zu beurteilen. Die Vorschriften zur Klassifizierung in der Geheimschutzordnung ließen einen erheblichen Interpretationsspielraum offen. (TZ 16)

Das Informationssicherheitsgesetz, die Informationssicherheitsverordnung und die Geheimschutzordnung legten Mindeststandards für den Schutz von klassifizierten Informationen fest. Diese waren von den betroffenen Organisationseinheiten durch Maßnahmen zu konkretisieren. Die Anforderungen an Kennzeichnung, Verarbeitung, Kommunikation, Vervielfältigung und Vernichtung von klassifizierten Informationen stiegen mit der Klassifizierungsstufe. Die überprüften Bundesministerien verfügten über Regelungen für Kennzeichnung, Verarbeitung, Kommunikation, Vervielfältigung und Vernichtung. (TZ 17)

Der internationale und der nationale Geheimschutz sahen übereinstimmend nachweisliche jährliche Überprüfungen der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen vor. Dabei waren insbesondere die Vollständigkeit der Aufzeichnungen, die Sicherheit der Behältnisse, das Schlüsselsystem und die Sicherungsmaßnahmen von Kommunikations- und Informationssystemen zu kontrollieren. Die überprüften Bundesministerien verfügten über Vorschriften für die jährlichen Überprüfungen der Sicherheitsvorkehrungen zum Schutz von klassifizierten Informationen. (TZ 18)

Überprüfung von Personen

In den überprüften Bundesministerien waren personenbezogene Überprüfungen eine Aufnahmevoraussetzung. Die Ministerien konnten diese Überprüfungen je nach Erfordernis des Geheimschutzes für den Zugang zu Informationen abgestuft für den jeweiligen Einsatzbereich anwenden. Abhängig von der Verwendung der Bediensteten waren die personenbezogenen Überprüfungen in regelmäßigen Abständen (drei, fünf oder zehn Jahre) zu erneuern. (TZ 19, TZ 20, TZ 21, TZ 22)

Im Innenministerium und der DSN kamen Vertrauenswürdigkeitsprüfungen und Sicherheitsüberprüfungen (TZ 20) zur Anwendung. Sicherheitsüberprüfungen veranlasste auch das Außenministerium für sein Personal. Gesonderte Regelungen für eine Verlässlichkeitsprüfung (TZ 21) bestanden im Verteidigungsministerium.

Vor Beginn der Tätigkeit in der DSN mussten sich künftige Bedienstete einer Vertrauenswürdigkeitsprüfung für den Verfassungsschutz unterziehen. (TZ 20)

Die Vertrauenswürdigkeitsprüfung diente der Abklärung der Vertrauenswürdigkeit einer Person anhand personenbezogener Daten, die Aufschluss über allfällige Anhaltspunkte geben, ob von dieser Person ein Risiko für den Verfassungsschutz ausgeht. Sie bestand aus den Angaben der Vertrauenswürdigkeitserklärung und der Überprüfung der darin enthaltenen Informationen einschließlich einer mündlichen Erörterung mit der überprüften Person. (TZ 20)

Die Sicherheitsüberprüfung war Voraussetzung für den Zugang zu klassifizierten Informationen ab der Klassifizierungsstufe „VERTRAULICH“. Für den Zugang zu Informationen der Stufe „STRENG GEHEIM“ waren auch Bezugspersonen zu überprüfen. Die Sicherheitsüberprüfung fand auf Basis einer Sicherheitserklärung statt. Ihr Umfang richtete sich nach der Klassifizierungsstufe der zugänglichen Information. Das Ergebnis der Sicherheitsüberprüfung enthielt Feststellungen darüber, ob Anhaltspunkte vorlagen, dass die Person gefährliche Angriffe begehen könnte. (TZ 20)

Die Überprüfung künftiger und bestehender Bediensteter der DSN im Rahmen der Vertrauenswürdigkeitsprüfung war umfassender und tiefgehender als bei der vormaligen Sicherheitsüberprüfung. Die Vertrauenswürdigkeitsprüfungen waren eine wichtige präventive Schutzmaßnahme insbesondere zum Schutz vor Spionage. (TZ 20)

Nicht alle Personen, die durch ihre Kontroll- und Dienstleistungsaufgaben umfangreiche Einblicke in sensible Bereiche des Verfassungsschutzes erhielten, mussten eine Vertrauenswürdigkeitsprüfung durchlaufen. (TZ 20)

Das Militärbefugnisgesetz enthielt gesetzliche Ausschlussgründe, bei deren Vorliegen Betroffene als nicht „verlässlich“ galten und dadurch ex lege von der Ausübung einer entsprechenden Tätigkeit ausgeschlossen waren. Eine vergleichbare Regelung sah weder das Staatsschutz- und Nachrichtendienst-Gesetz – ausgenommen jene Fälle, in denen die betroffene Person die Überprüfung verweigerte oder ungenügend mitwirkte – noch das Sicherheitspolizeigesetz vor. (TZ 20)

Im Verteidigungsministerium war die Verlässlichkeitsprüfung die Voraussetzung für die Aufnahme in ein Dienstverhältnis. Sie fand auf Basis einer Verlässlichkeitserklärung der zu überprüfenden Person statt. Das Verteidigungsministerium unterschied – nach Maßgabe der Gefahr für die militärische Sicherheit – zwischen einer einfachen und erweiterten Verlässlichkeitserklärung. (TZ 21)

Personenbezogene Elemente der Kontrollsysteme

Die Aus- und Weiterbildungsprogramme der überprüften Bundesministerien enthielten Inhalte über Spionage, Spionageprävention und -abwehr. Zusätzlich gestaltete das Abwehramt Sensibilisierungs- und Informationsvorträge für Militärangehörige und externe Personen. Im Außenministerium waren unter Berücksichtigung wechselnder Auslandsverwendung etwa Sicherheitsgespräche vor Versetzungen oder die Nutzung von Tagungen für Fortbildungen vorgesehen. (TZ 23)

Die Nebenbeschäftigungen in den überprüften Bundesministerien waren restriktiv im Sinne der Spionageprävention geregelt. Für das Innen- und das Verteidigungsministerium bestanden eigene Verordnungen für jedenfalls unzulässige Nebenbeschäftigungen. Die Interne Revision im Verteidigungsministerium hob im Rahmen einer Prüfung einen präventiven Handlungsbedarf zur Wahrung von Dienstgeberinteressen hervor. Im Außenministerium bestanden für Nebenbeschäftigungen Meldevorschriften, die sowohl erwerbsmäßige als auch nicht erwerbsmäßige Nebenbeschäftigungen umfassten. Zweifel an der Vereinbarkeit mit der offiziellen Funktion im Empfangsstaat führten zur Untersagung. (TZ 24)

Zutrittsbeschränkungen bestanden in allen überprüften Ministerien. Diese waren durch bauliche (z.B. äußere Abgrenzungen, Lage von Räumlichkeiten) und technische (z.B. Zutrittskarten) sowie zusätzlich durch organisatorische Maßnahmen (z.B. Begleitung externer Personen) geregelt. (TZ 25)

Die DSN hatte Zutrittsregelungen für die eigenen Räumlichkeiten schriftlich und je nach Sicherheitsbedarf der Räumlichkeit festgelegt, mit unterschiedlichen Zutrittsvoraussetzungen im Sinne eines IKS. Das Verteidigungsministerium hatte abgestufte Objektschutzkategorien und Zutrittsregelungen je nach Schutzbedarf der militärischen Rechtsgüter und Informationen als IKS-Maßnahmen implementiert. (TZ 25)

Die Beendigung von Dienstverhältnissen im Außenministerium und bei der DSN unterlag einem Offboarding-Prozess. Dieser reichte von der Abgabe elektronischer Geräte bis zur Übergabe von Schlüsselkarten und der Löschung von Zugangsberechtigungen im IKT-System. Das Abwehramt arbeitete an einem Offboarding-Prozess für die militärischen Nachrichtendienste. (TZ 26)

Beschaffungen

Für öffentliche Auftragsvergaben war das Bundesvergabegesetz, bei Beschaffung bestimmter Leistungen des Verteidigungs- und Sicherheitsbereichs das Bundesvergabegesetz Verteidigung und Sicherheit 2012 anzuwenden. Beide Vergabegesetze enthielten Ausnahmen, etwa zu Aufträgen, auf die die Ausnahmebestimmung in Art. 346 des Vertrags über die Arbeitsweise der Europäischen Union (**AEUV**) zur Wahrung der wesentlichen Sicherheitsinteressen des Mitgliedstaates Anwendung fand. (TZ 27)

Der RH erhob im Innen-, Verteidigungs- und Außenministerium Beschaffungen im Zusammenhang mit der IT-Sicherheitsinfrastruktur, etwa Server, Netzwerkkomponenten, unterbrechungsfreie Stromversorgung und Komponenten zur verschlüsselten Kommunikation. Für die im Zeitraum 2017 bis 2024 durchgeführten Beschaffungen der IT-Sicherheitsinfrastruktur bedienten sich die Ministerien der Bundesbeschaffung GmbH (Innenministerium 58 %, Verteidigungsministerium 89 % und Außenministerium 70 %) oder führten diese selbst durch (Innenministerium 42 %, Verteidigungsministerium 2 % und Außenministerium 14 %). Das Verteidigungsministerium (9 %) und das Außenministerium (16 %) zogen das Bundesvergabegesetz Verteidigung und Sicherheit 2012 und Ausnahmeregelungen heran. (TZ 28)

Zur Unterstützung der Umsetzung von Hochsicherheitsnetzwerken der DSN sollten externe Leistungen zugekauft werden. Laut Einstufung durch das Innenministerium betraf die Auftragsvergabe wesentliche Sicherheitsinteressen des Bundes. Das Innenministerium vergab die Leistung im Oktober 2021 selbst, ohne Einbindung der Bundesbeschaffung GmbH (**BBG**), und zog dabei die Ausnahme nach § 3 Abs. 1 Z 1 BBG-Gesetz heran. Bei der Vergabe der Leistungen zum Hochsicherheitsnetzwerk berief sich das Innenministerium auf die Ausnahmen des Art. 346 AEUV bzw. des § 9 Abs. 1 Z 5 Bundesvergabegesetz Verteidigung und Sicherheit 2012; die Vergabe erfolgte sohin außerhalb des Vergaberechts. (TZ 27)

Im Juni 2022 berichtete eine deutsche Mediengesellschaft über die Aufträge des Innenministeriums im Zusammenhang mit einem IKT-Projekt für die DSN, über Verbindungen des beauftragten Unternehmens zu einem ehemaligen Geschäftsführer eines deutschen Zahlungsdienstleisters sowie über mögliche, damit zusammenhängende Verbindungen zur Russischen Föderation. Infolge dieser Berichterstattung

nahm die DSN von der Umsetzung des Hochsicherheitsnetzwerks durch externe Unternehmen Abstand. Das Konzept des externen Unternehmens kam nicht zur Anwendung. Potenzielle Auswirkungen der medialen Vorhalte auf andere Projekte des Unternehmens für die Republik Österreich untersuchte weder das Innenministerium noch die DSN. (TZ 27)

Die DSN gab an, über keine Möglichkeiten zur Überprüfung von Unternehmen zu verfügen. Das Abwehramt war für die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen zuständig. Die rechtliche Grundlage dieser Bescheinigungen stellte auf eine sichere Verwendung klassifizierter Informationen ab. Spezifische Aspekte der Spionageprävention waren davon nicht umfasst. Die personenbezogenen Überprüfungen (Sicherheitsüberprüfung, Verlässlichkeitsprüfung) beruhten auf einer Selbstauskunft der überprüften Person. Mangels gesetzlicher Grundlage war es bei diesen Überprüfungen nicht möglich, nachrichtendienstliche Informationen heranzuziehen sowie zivile und militärische Informationen zu Unternehmen auszutauschen. (TZ 27)

Zusammenfassung Kontrollbereiche

Die überprüften Ressorts verfügten jeweils über ein IKS mit Elementen zur Spionageprävention. Regelungen und Maßnahmen waren in Dienstvorschriften dokumentiert, Bedienstete wurden darin unterwiesen und regelmäßig fortgebildet. Die Feststellungen des RH trafen nur auf den Zeitpunkt der Überprüfung zu. Eine darüber hinausgehende Beurteilung der Wirksamkeit der Kontrollmaßnahmen konnte der RH nicht vornehmen. Die Überwachung der Einhaltung der Regelungen des IKS stellt eine Management- bzw. Führungsaufgabe dar, die von den jeweiligen Vorgesetzten wahrzunehmen ist. Nur im Rahmen regelmäßiger Kontrollen kann das erwartete Schutzniveau aufrechterhalten werden. (TZ 29)

Interministerielle Zusammenarbeit

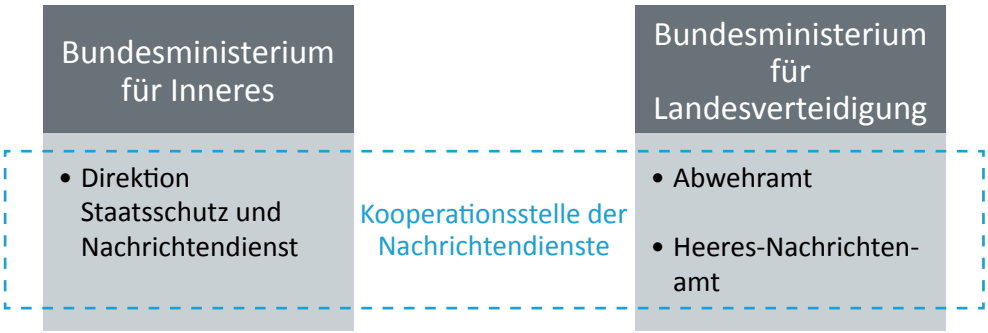
Im Rahmen der innerstaatlichen Formate Nationaler Sicherheitsrat, Arbeitsgruppe Hybride Bedrohungen, Kerngruppe Desinformation sowie in den Gremien gemäß Bundes-Krisensicherheitsgesetz fand anlassbezogen und regelmäßig ein Informationsaustausch zu Aspekten der nachrichtendienstlichen Tätigkeit fremder Staaten statt. Die Bundesministerien tauschten im „Inneren Kreis der Operativen Koordinationsstruktur“ für den Cyberraum spionagerelevante Informationen aus. (TZ 31)

Spionage war zudem im Rahmen der EU ein Thema im Kontext der hybriden Bedrohungen. Für die Analyse und den Informationsaustausch unter den EU-Mitgliedstaaten war im Lagezentrum der EU (EU Intelligence and Situation Centre) die Hybrid

Fusion Cell eingerichtet. Seit 2018 fanden in deren Rahmen halbjährlich Treffen der Nationalen Kontaktpunkte der EU-Mitgliedstaaten statt. Das Außenministerium nahm die Funktion des Nationalen Kontaktpunkts für Österreich wahr. (TZ 31)

Das Innen- und das Verteidigungsministerium arbeiteten zudem in der „Kooperationsstelle der Nachrichtendienste" zusammen. In dieser waren die DSN, das Abwehramt und das Heeres-Nachrichtenamt vertreten. (TZ 31)

Abbildung: Zusammenarbeit der Nachrichtendienste



Quellen: BMI; BMLV; Darstellung: RH

In Österreich – insbesondere in Wien – haben zahlreiche diplomatische Vertretungen sowie internationale Organisationen ihren Sitz. Das Wiener Übereinkommen regelt die Rahmenbedingungen für die diplomatischen Beziehungen zwischen den Staaten. Vorbehaltlich der Art. 5, 8, 9 und 11 des Wiener Übereinkommens konnte der Entsendestaat die Mitglieder des Personals seiner Mission nach freiem Ermessen ernennen. Das Außenministerium befasste die relevanten Bundesministerien und Nachrichtendienste u.a. in allen Agrémentverfahren (für bilaterale Botschafterinnen und Botschafter und für Militärattachés) sowie in einigen Fällen vor der Erteilung von Dienstantrittsvisa für andere Personen. (TZ 31)

Die Gesamtzahl des in Österreich akkreditierten diplomatischen Personals bei wesentlichen Einrichtungen lag mit Stand 1. März 2025 bei rd. 8.200 Personen. (TZ 31)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

ZENTRALE EMPFEHLUNGEN

Bundesministerium für Inneres; Bundesministerium für Landesverteidigung; Bundesministerium für europäische und internationale Angelegenheiten

- Die personellen und finanziellen Ressourcen zur Spionageprävention wären entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen. (TZ 7, TZ 8, TZ 9, TZ 10, TZ 11, TZ 12)

- Die Auswirkungen der geopolitischen Entwicklungen auf einen Veränderungs- oder Anpassungsbedarf der Österreichischen Sicherheitsstrategie wären weiterhin zu beobachten; allfällige notwendige Weiterentwicklungen der Österreichischen Sicherheitsstrategie wären beim Bundeskanzleramt anzustoßen und einer Beschlussfassung im Nationalrat zuzuführen. (TZ 5)

- Die Vorbereitung der Regierungsvorlage für ein novelliertes Informationssicherheitsgesetz wäre in der Informationssicherheitskommission sowie im Abstimmungsprozess mit sämtlichen Bundesministerien zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen. (TZ 15)

- Der Wahrnehmung der Management- und Führungsaufgaben wäre – zum Erhalt des Schutzniveaus des Internen Kontrollsystems – hohe Aufmerksamkeit zu schenken. (TZ 29)

Bundesministerium für Inneres; Bundesministerium für Landesverteidigung

- Für Beschaffungen, die wesentliche Sicherheitsinteressen des Bundes betreffen und die damit für eine Ausnahme von den Bundesvergabegesetzen zugänglich sind, wäre auf eine gesetzliche Regelung hinzuwirken, die eine Überprüfung von Unternehmen vor Beauftragung (im Rahmen der Eignungsprüfung) unter Heranziehung nachrichtendienstlicher Erkenntnisse ermöglicht. (TZ 27)

Bundesministerium für Inneres

- Analog zu den bestehenden Regelungen im Staatsschutz- und Nachrichtendienst-Gesetz zu den Personen, die einer Vertrauenswürdigkeitsprüfung unterzogen werden, wäre eine gesetzliche Regelung im Nationalrat zu initiieren, die Verwaltungspersonal mit vergleichbarem Einblick in die sensible Tätigkeit des Verfassungsschutzes in die Vertrauenswürdigkeitsprüfung einbezieht. (TZ 20)

- Der personelle Ausbau der Direktion Staatsschutz und Nachrichtendienst (DSN), insbesondere im Bereich der Spionageabwehr, wäre weiterhin voranzutreiben. Bei der Beantragung zusätzlicher Planstellen bzw. bewerteter Arbeitsplätze wäre dabei auf Basis regelmäßiger Bedarfsanalysen eine Priorisierung nach Dringlichkeit vorzunehmen. (TZ 7)

Bundesministerium für Landesverteidigung

- Die personellen Ressourcen für die Spionageabwehr wären regelmäßig der internationalen Bedrohungslage anzupassen; der Organisationsplan des Abwehramtes wäre in diesem Sinne zu überarbeiten. (TZ 9)

Zahlen und Fakten zur Prüfung

IKS-Elemente der Spionageprävention im Innenministerium, Verteidigungsministerium und Außenministerium							
Rechtsgrundlagen	Bundes-Verfassungsgesetz, BGBl. 1/1930 i.d.g.F. Beamten-Dienstrechtsgesetz 1979, BGBl. 333/1979 i.d.g.F. Informationssicherheitsgesetz, BGBl.I 23/2002 i.d.g.F. Militärbefugnisgesetz, BGBl. I 86/2000 i.d.g.F. Staatsschutz- und Nachrichtendienst-Gesetz, BGBl. I 5/2016 i.d.g.F. Strafgesetzbuch, BGBl. 60/1974 i.d.g.F.						
Personal Spionageprävention[1]	2019	2020	2021	2022	2023	2024	2025
	Stand in % zu Basisjahr 2017[2]						
Innenministerium							
Personalstand	133	133	120	111	158	180	207
Mehrdienstleistungen	136	129	157	229	293	373	
Verteidigungsministerium							
Personalstand	100	100	100	211	211	211	211
Mehrdienstleistungen	115	91	98	174	279	348	
Außenministerium							
Personalstand	136	136	156	176	160	150	207

[1] Personalstand jeweils 1. Jänner
[2] 1. Jänner 2017 bildet die Basis mit 100 %.

Quellen: BMI; BMLV; BMEIA; Zusammenstellung: RH

Prüfungsablauf und -gegenstand

1 (1) Der RH überprüfte von Oktober 2024 bis Mai 2025 zentrale Elemente des Präventionsmechanismus, mit denen Spionagevorfälle im Bundesministerium für Inneres (in der Folge: **Innenministerium**), im Bundesministerium für Landesverteidigung (in der Folge: **Verteidigungsministerium**) sowie im Bundesministerium für europäische und internationale Angelegenheiten (in der Folge: **Außenministerium**)[1] verhindert werden sollten. Die Gebarungsüberprüfung erfolgte gemäß Art. 126b Abs. 4 Bundes-Verfassungsgesetz[2] aufgrund eines Antrags gemäß § 99 Abs. 2 Geschäftsordnungsgesetz 1975[3] des Abgeordneten Douglas Hoyos-Trauttmansdorff und weiterer Abgeordneter vom 15. Mai 2024 (4017/A BlgNR 27. GP). Das Verlangen zur Durchführung der Gebarungsüberprüfung umfasste sechs Fragen. Die Beantwortung der Fragen befindet sich in TZ 33.

(2) Ziele der Gebarungsüberprüfung waren in Übereinstimmung mit dem Prüfungsverlangen insbesondere die Darstellung und Beurteilung

- rechtlicher Grundlagen für die Spionageprävention,
- der Maßnahmen des Internen Kontrollsystems (**IKS**),
- der Beschaffungen im IT-Bereich im Sinne eines Überblicks sowie einer ausgewählten Beschaffung sowie
- der Zusammenarbeit im Bereich der Spionageprävention.

Der überprüfte Zeitraum umfasste im Wesentlichen die Jahre 2017 bis 2024. Darüber hinaus bezog der RH auch aktuellere Entwicklungen mit ein.

(3) Das zum Innenministerium ressortierende Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (**BVT**) bestand bis Ende November 2021. Die Nachfolgeorganisation Direktion Staatsschutz und Nachrichtendienst (**DSN**) nahm mit Dezember 2021 ihre Tätigkeit auf. Der RH bezog den organisatorischen Übergang von BVT zur DSN insofern in seine Gebarungsüberprüfung ein, als sich daraus Ableitungen für die Ausgestaltung des IKS treffen ließen. Die Reorganisation selbst vom BVT zur DSN war nicht Gegenstand der Gebarungsüberprüfung.

Der RH überprüfte in Übereinstimmung mit dem Prüfungsverlangen die operativen (insbesondere nachrichtendienstlichen) Tätigkeiten der Bundesministerien nicht.

[1] Die Bezeichnungen des Verteidigungs- und Außenministeriums wechselten im überprüften Zeitraum; siehe dazu die Tabellen im Anhang. Der RH verwendet im Folgenden einheitlich die Bezeichnungen Verteidigungsministerium und Außenministerium.

[2] BGBl. 1/1930 i.d.g.F.

[3] BGBl. 410/1975 i.d.g.F.

(4) Auf parlamentarischer Ebene war zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit der Ständige Unterausschuss des Ausschusses für innere Angelegenheiten (in der Folge: **Ständiger Unterausschuss**) eingerichtet. Die Sitzungen des Ständigen Unterausschusses sind grundsätzlich geheim.

Für die Innenministerin bzw. den Innenminister bestanden gemäß § 17 Abs. 3 Staatsschutz- und Nachrichtendienst-Gesetz[4] (**SNG**) Berichtspflichten an den Ständigen Unterausschuss. Die Berichte waren klassifiziert. Der Nationalrat war damit regelmäßig informiert: halbjährlich über die Wahrnehmung der Aufgaben nach dem SNG sowie jährlich über die personelle und finanzielle Ressourcenausstattung der DSN.

(5) Darüber hinaus war bei der Innenministerin bzw. dem Innenminister die Unabhängige Kontrollkommission Verfassungsschutz (in der Folge: **Kontrollkommission**) eingerichtet, die mit Ende 2023 ihre Arbeit aufnahm. Die Kontrollkommission erstattet an die Innenministerin bzw. den Innenminister und den Ständigen Unterausschuss Bericht über ihre Tätigkeit.[5]

(6) Die Veränderungen der geopolitischen Lage, u.a. infolge des Krieges in der Ukraine, des Terrorangriffs auf Israel und der Eskalation der Sicherheitslage im Nahen Osten, hatten auch Auswirkungen auf die Anforderungen an den Verfassungsschutz (Staatsschutz und Nachrichtendienst) in Österreich insgesamt und an die Spionageabwehr im Konkreten. Auch war die Republik Österreich – aufgrund ihrer geografischen Lage und ihrer Rolle als EU-Mitglied, weil multilaterale Organisationen ihren Sitz in Österreich hatten, infolge der Zusammenarbeit der Republik Österreich mit der NATO im Rahmen der Partnerschaft für den Frieden sowie Österreichs Funktion als Wirtschafts- und Forschungszentrum – von nachrichtendienstlichem Interesse.

(7) Zu dem im Dezember 2025 übermittelten Prüfungsergebnis nahmen das Verteidigungsministerium im Februar 2026, das Innen- und das Außenministerium im März 2026 Stellung. Der RH erstattete seine Gegenäußerungen im Juni 2026.

[4] BGBl. I 5/2016 i.d.g.F.

[5] Die fünf Mitglieder der Kontrollkommission werden auf Vorschlag des Hauptausschusses vom Nationalrat in Anwesenheit von mindestens der Hälfte der Mitglieder mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen für eine Funktionsperiode von zehn Jahren gewählt.

Spionage und Spionageprävention

2 Die Begriffe Spionage und Spionageabwehr waren gesetzlich nicht definiert. Auch die §§ 252 ff. Strafgesetzbuch[6] enthielten keine Definition. Der sogenannte „Spionageparagraf" – § 256 Strafgesetzbuch – stellte das Einrichten, Betreiben oder Unterstützen eines geheimen Nachrichtendienstes zum Nachteil der Republik Österreich unter Strafe.

Abseits einer gesetzlichen Definition von Spionage und Spionageabwehr war das Verständnis der überprüften Bundesministerien inhaltlich ausreichend deckungsgleich: Das Beschaffen und Erlangen von unbekannten, geschützten Informationen unter Einsatz nachrichtendienstlicher Methoden.

Der RH verwendet den Begriff Spionageprävention, um die Elemente der IKS der überprüften Ministerien zusammenzufassen, die für die Hintanhaltung von Spionage geeignet sind. Der RH überprüfte die IKS mit Fokus auf die Ausprägung Spionageprävention und stellte sie den allgemeinen Prinzipien eines IKS (z.B. Funktionstrennung) gegenüber (TZ 29).

Rechtliche und strategische Rahmenbedingungen

Rechtliche Rahmenbedingungen

3 Spionageprävention ist eine Querschnittsmaterie. Ausgehend von der inhaltlichen Definition der Spionage – Beschaffen und Erlangen von unbekannten, geschützten Informationen unter Einsatz nachrichtendienstlicher Methoden – fanden sich in mehreren Gesetzen Grundlagen der Spionageprävention.

Schon das Bundes-Verfassungsgesetz enthielt bis Ende August 2025 in Art. 20 Abs. 3 (Amtsverschwiegenheit) und Art. 52a (Ständige Unterausschüsse) grundlegende Bestimmungen zum Schutz der Republik und ihrer Institutionen, die indirekt auch Spionageaktivitäten betreffen.

Die Amtsverschwiegenheit entfiel mit Inkrafttreten des Informationsfreiheitsgesetzes[7] am 1. September 2025. Das im Informationsfreiheitsgesetz normierte Recht auf Zugang zur Information gilt allerdings nicht, soweit die Geheimhaltung im Interesse

6 BGBl. 60/1974 i.d.g.F.

7 BGBl. I 5/2024

der nationalen Sicherheit, der umfassenden Landesverteidigung oder der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit erforderlich ist und gesetzlich nichts anderes bestimmt ist (Art. 22a Abs. 2 Bundes-Verfassungsgesetz i.d.F. BGBl. I 5/2024).

Darüber hinaus finden sich Regelungen etwa im Dienstrecht mit § 46 Beamten-Dienstrechtsgesetz 1979[8], der die Amtsverschwiegenheit bzw. seit September 2025 die Geheimhaltung regelt.

Im Strafrecht ist u.a. der 16. Abschnitt des Besonderen Teils des Strafgesetzbuches (Landesverrat) relevant, insbesondere § 256, der „Spionage" zum Nachteil der Republik Österreich unter Strafe stellt, und § 310 (Verletzung des Amtsgeheimnisses) sowie § 319 (Militärischer Nachrichtendienst für einen fremden Staat). Zur „Cyber-Spionage" sind z.B. § 126c (Missbrauch von Computerprogrammen oder Zugangsdaten), § 118a (Widerrechtlicher Zugriff auf ein Computersystem) sowie § 119a (Missbräuchliches Abfangen von Daten) einschlägig.

Auch in der Datenschutz-Grundverordnung[9] und dem Datenschutzgesetz[10] finden sich Regelungen, die der Spionageprävention dienen (beispielsweise Schutz personenbezogener Daten oder Datensicherheit).

4.1 (1) Im Zuge der Prüfgespräche hielten die DSN und das Abwehramt im Verteidigungsministerium dem RH gegenüber fest, dass Staatsanwaltschaften den Begriff „zum Nachteil der Republik Österreich" in § 256 Strafgesetzbuch im überprüften Zeitraum zu restriktiv ausgelegt hätten, was zu Einstellungen der Ermittlungsverfahren führen würde.

Das Bundesministerium für Justiz (in der Folge: **Justizministerium**) legte mit Erlass vom Dezember 2024 – unvorgreiflich der unabhängigen Rechtsprechung – seine Ansicht zur Auslegung des Begriffs „zum Nachteil der Republik Österreich" in § 256 Strafgesetzbuch dar:

Aufbauend auf Judikatur[11], Gesetzesmaterialien und Lehre vertrat das Justizministerium die Ansicht, dass auch dann konkrete und vitale Interessen Österreichs verletzt sein könnten, wenn die Tätigkeit des geheimen Nachrichtendienstes politische, militärische oder wirtschaftliche Beziehungen zum Ausland negativ beeinträchtige oder objektiv abstrakt geeignet sei, derartige Beziehungen negativ zu beeinträchtigen. Abhängig von den konkreten Umständen im Einzelfall könne eine negative Beein-

8 BGBl. 333/1979 i.d.g.F.

9 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016

10 BGBl. I 165/1999 i.d.g.F.

11 OGH 20. April 1956, 5 Os 182/56, SSt 27/20

trächtigung der politischen Beziehungen zum Ausland beispielsweise vorliegen, wenn in Österreich ein geheimer Nachrichtendienst zum Nachteil eines anderen Mitgliedstaates der EU betrieben werde.

Konkrete und vitale Interessen Österreichs könnten darüber hinaus auch dann verletzt sein, wenn sich die nachrichtendienstliche Tätigkeit gegen in Österreich ansässige über- oder zwischenstaatliche Einrichtungen richte. Der Österreichbezug der nachrichtendienstlichen Tätigkeit sei unter Umständen dadurch gegeben, dass zumindest das Ansehen Österreichs als sicherer Standort für über- oder zwischenstaatliche Einrichtungen beeinträchtigt sein könne, wenn in Österreich ansässige Einrichtungen Ziel von geheimen nachrichtendienstlichen Tätigkeiten würden. Das könne letztlich dazu führen, dass diese Einrichtungen abwandern und Österreich als künftiger Standort für weitere Einrichtungen ausscheide, was einerseits negative außenpolitische Auswirkungen hätte und sich andererseits auf die Prosperität Österreichs auswirken würde. Hierzu gelte es zu bedenken, dass den über- oder zwischenstaatlichen Einrichtungen in Österreich auch als Wirtschaftsfaktor Bedeutung zukomme, insbesondere durch die Schaffung von Arbeitsplätzen und Wertschöpfung.

(2) Im Regierungsprogramm 2025–2029 waren legistische Maßnahmen im Bereich des Justizministeriums vorgesehen, so sollte insbesondere

- § 319 Strafgesetzbuch (Militärischer Nachrichtendienst für einen fremden Staat) auf zivile Nachrichtendienste ausgeweitet werden,
- der Verrat eines militärischen Geheimnisses durch Zivilpersonen künftig strafbar sein und
- die Strafbarkeit von Spionage erweitert werden.

4.2 Der RH hielt fest, dass das Justizministerium im Dezember 2024 seine Rechtsansicht erlassmäßig festgehalten hatte, wonach Strafverfolgungsbehörden Spionagetätigkeiten auch dann verfolgen könnten, wenn diese nur indirekt zum Nachteil der Republik Österreich gesetzt worden seien.

Der RH stellte weiters fest, dass im Regierungsprogramm 2025–2029 gesetzliche Änderungen zur Erweiterung der Strafbarkeit von Spionage vorgesehen waren.

Strategische Rahmenbedingungen

5.1 (1) Bestimmend für die strategischen Rahmenbedingungen zur Spionageprävention im überprüften Zeitraum war bis zum Jahr 2024 die Österreichische Sicherheitsstrategie 2013[12]. Diese enthielt im Bereich Spionageprävention Ziele zur Verbesserung des Zusammenwirkens aller sicherheitspolitischen Akteure bei der Analyse und Bewertung sicherheitsrelevanter Situationen sowie zur Mitwirkung an der europäischen Kooperation beim nachrichtendienstlichen Informationsaustausch. Für Österreich nachteilige nachrichtendienstliche Aktivitäten sollten bekämpft werden.

(2) Das Regierungsprogramm 2017–2022 beinhaltete als Ziele die Verbesserung der Prozesse zur Zusammenarbeit der Nachrichtendienste, die Etablierung von Berichtspflichten sowie die Schaffung eines Straftatbestands für nachrichtendienstliche Aktivitäten gegen Privatpersonen.

Das Regierungsprogramm 2020–2024 hatte im Bereich des Innenministeriums u.a. die umfassende Neuausrichtung des BVT und die damit verbundene Wiederherstellung des Vertrauens seitens der Bevölkerung und der Partnerdienste zum Ziel. Dies umfasste die strukturelle Trennung von Nachrichtendienst und Staatsschutz, die Etablierung von internationalen Standards (z.B. Personalaufnahme, Ausbildung, Sicherheit) sowie die Behebung von Sicherheitsmängeln. Im Bereich des Verteidigungsministeriums sollten die militärischen Nachrichtendienste erhalten bleiben und Weiterentwicklungen im Bereich Cyber vorangetrieben werden.

(3) Seit dem Beschluss der Österreichischen Sicherheitsstrategie 2013 änderten sich die geopolitischen Rahmenbedingungen, insbesondere infolge des Krieges in der Ukraine. Um der Veränderung der nationalen und internationalen Sicherheitslage der letzten Jahre Rechnung zu tragen, legte die Bundesregierung im August 2024 die Österreichische Sicherheitsstrategie 2024 vor. Sie wurde dem Landesverteidigungsausschuss zugewiesen.

Die Österreichische Sicherheitsstrategie 2024 enthielt im Bereich Spionageprävention insbesondere Ziele bzw. Feststellungen zu den Herausforderungen der Wirtschaftsspionage, zum Ausbau der nationalen und internationalen Zusammenarbeit bei der Spionageabwehr, zur Sensibilisierung von Amtsträgerinnen und Amtsträgern für das Thema Spionage, zu den Gefahren der hybriden Beeinflussungen und Bedrohungen sowie zur Anpassung der militärischen nachrichtendienstlichen Aufklärung und Abwehr an die geänderten Rahmenbedingungen. Mit Ministerratsbeschluss vom April 2025 hielt die Bundesregierung die Ausrichtung Österreichs in gemeinsamen außen-, sicherheits- und verteidigungspolitischen Fragen fest. Dieser Beschluss

[12] Die Österreichische Sicherheitsstrategie war eine gesamtstaatliche Strategie zur umfassenden Sicherheitsvorsorge (äußere und innere, zivile und militärische Sicherheit).

umfasste auch die Vorlage einer aktualisierten Österreichischen Sicherheitsstrategie an den Nationalrat.

(4) Das Regierungsprogramm 2025–2029 nannte als Ziele im Bereich des Innenministeriums u.a. die Weiterentwicklung der österreichischen Sicherheitsarchitektur, den Schutz klassifizierter Informationen der DSN, die Schaffung eines bundesländerübergreifenden Datenverbundes von Polizei und Verfassungsschutz sowie die Novellierung des Sicherheitspolizeigesetzes[13] zur Sicherheitsüberprüfung von natürlichen und juristischen Personen. Im Bereich des Verteidigungsministeriums sollten Anpassungen im Militärbefugnisgesetz[14] die Handlungsfähigkeit der militärischen Nachrichtendienste im Cyber-Bereich stärken.

5.2 Der RH hielt fest,

- dass die Regierungsprogramme strategische Ziele zur Bekämpfung von Spionage enthielten.
- dass die Bundesregierung im Jahr 2024 eine neue Sicherheitsstrategie vorgelegt hatte, die den Veränderungen der nationalen und internationalen Sicherheitslage der letzten Jahre – auch im Bereich der Spionage – Rechnung tragen sollte. Eine Überarbeitung dieser beschloss die Bundesregierung mit April 2025.
- dass sich die Veränderungen im geopolitischen Umfeld seit 2022 dynamischer gestalteten als im vorangegangenen Jahrzehnt. Auch wenn strategische Ziele im Optimalfall für einen längeren Zeitraum Gültigkeit haben sollten, war nicht auszuschließen, dass geopolitische Entwicklungen kurzfristig Veränderungs- oder Anpassungsbedarf anstoßen konnten.

Der RH empfahl dem Innen-, Verteidigungs- und Außenministerium, weiterhin die Auswirkungen der geopolitischen Entwicklungen auf einen Veränderungs- oder Anpassungsbedarf der Österreichischen Sicherheitsstrategie zu beobachten und allfällige notwendige Weiterentwicklungen der Österreichischen Sicherheitsstrategie beim Bundeskanzleramt anzustoßen und einer Beschlussfassung im Nationalrat zuzuführen.

5.3 (1) Laut Stellungnahme des Innenministeriums sei der Vorschlag des RH zu begrüßen. Jede Beobachtung relevanter Veränderungen in den geopolitischen Entwicklungen führe zu einem Anstoß zur Adaptierung der Österreichischen Sicherheitsstrategie an das Bundeskanzleramt und stelle in diesem Zusammenhang eine Weiterentwicklung des strategischen Gesamtrahmens in Österreich dar.

[13] BGBl. 566/1991 i.d.g.F.

[14] BGBl. I 86/2000 i.d.g.F.

Die bestehenden Strategien (z.B. Österreichische Sicherheitsstrategie, Österreichische Strategie für die Resilienz kritischer Einrichtungen oder Österreichische Strategie für Cybersicherheit) stünden in einem engen sachlichen Zusammenhang und wirkten in Wechselbeziehungen zueinander. Diese Verbindungen würden zukünftig weiterentwickelt und geschärft, um eine kohärente Fortführung des Gesamtrahmens in Österreich zu gewährleisten.

Seitens der DSN sei eine Verbindungsbeamtin beim zuständigen Regierungskoordinator im Bundeskanzleramt angesiedelt worden, um für einen raschen und zielgerichteten Informationsaustausch zu sorgen.

(2) Das Verteidigungsministerium führte in seiner Stellungnahme aus, dass es bei der im April 2025 begonnenen Überarbeitung der Österreichischen Sicherheitsstrategie in Steuerungs- und Arbeitsgruppen vertreten gewesen sei und die Kernaspekte des Verteidigungsministeriums eingebracht habe. Im Dezember 2025 seien die Arbeiten abgeschlossen worden. Ein formeller Abschluss im Ministerrat und eine Befassung des Nationalrats würden im ersten Quartal 2026 erwartet.

In der erarbeiteten Version der Österreichischen Sicherheitsstrategie sei eine Überarbeitung bzw. Evaluierung thematisiert. Somit sei hinkünftig eine ständige Anpassung an die jeweiligen Umstände (geopolitischen Entwicklungen) geregelt.

(3) Das Außenministerium teilte in seiner Stellungnahme mit, dass die Weiterentwicklung bzw. Anpassung der Österreichischen Sicherheitsstrategie keiner Beschlussfassung des Nationalrats bedürfe, sondern Angelegenheit der Bundesregierung sei. Die Österreichische Sicherheitsstrategie 2013 und die Österreichische Sicherheitsstrategie 2024 seien vom Ministerrat angenommen und dem Nationalrat zur Debatte zugeleitet worden.

5.4 Der RH entgegnete dem Außenministerium, dass die Genese der Österreichischen Sicherheitsstrategie 2013 im Jahr 2011 mit einem von der damaligen Bundesregierung an das Parlament zur weiteren Debatte zugeleiteten Bericht zur neuen Österreichischen Sicherheitsstrategie begonnen hatte. Dieser Bericht und die Entschließung des Nationalrats aus dem Jahr 2013 bildeten gemeinsam die Österreichische Sicherheitsstrategie 2013. Die Österreichische Sicherheitsstrategie 2024 wurde nach Einlangen im Nationalrat im September 2024 an den Landesverteidigungsausschuss zugewiesen. Eine Debatte darüber im Nationalrat fand nicht statt.

Der RH sieht in einem parteiübergreifenden Konsens einen Erfolgsfaktor für eine langfristige Ausrichtung im Sicherheitsbereich.

Aufgabenverteilung

6 (1) In den überprüften Bundesministerien war eine Reihe von Organisationseinheiten mit Aufgaben im Zusammenhang mit Spionageprävention in unterschiedlicher Intensität befasst.

(2) Im Innenministerium waren Gefahrenerforschung und -abwehr im Bereich Spionage von Anfang 2017 bis Ende November 2021 im damaligen BVT angesiedelt, danach in der DSN.

Die DSN diente dem Verfassungsschutz, der gemäß § 1 SNG folgende Aufgaben umfasste:

- Schutz kritischer Infrastruktur,
- Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit,
- Schutz von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen,
- Wahrnehmung zentraler Funktionen der internationalen Zusammenarbeit in den Bereichen des Verfassungsschutzes,
- Schutz der Bevölkerung vor
  - Gefährdung durch Spionage,
  - Gefährdung durch Proliferation[15],
  - Gefährdung durch nachrichtendienstliche Tätigkeit sowie
  - terroristisch, ideologisch oder religiös motivierter Kriminalität.

Die DSN war dementsprechend – auch organisatorisch – in die zwei Bereiche Staatsschutz und Nachrichtendienst getrennt.

- Der Bereich Staatsschutz umfasste insbesondere den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen, Fallkonferenzen sowie sicherheits- und kriminalpolizeiliche Aufgaben im Zusammenhang mit verfassungsgefährdenden Angriffen.[16]
- Dem Bereich Nachrichtendienst oblagen die erweiterte Gefahrenerforschung (§ 6 Abs. 1 SNG) sowie die Gewinnung und Analyse von Informationen hinsichtlich der Zwecke des Verfassungsschutzes (§ 8 Abs. 1 SNG) und somit insbesondere der Spionageabwehr und -prävention.

[15] Proliferation ist die Weiterverbreitung von atomaren, biologischen oder chemischen Massenvernichtungswaffen und entsprechenden Waffenträgersystemen bzw. der zu deren Herstellung verwendeten Produkte, einschließlich des dazu erforderlichen Know-how. Massenvernichtungswaffen gelten als machtpolitisches Instrument, das die Stabilität eines gesamten Staatsgefüges erschüttern kann (https://www.dsn.gv.at/208/; abgerufen am 6. März 2025).

[16] Die Aufgaben der Gefahrenabwehr und die damit verbundenen Befugnisse waren im Sicherheitspolizeigesetz geregelt, sofern das SNG nichts Besonderes regelte (§ 5 SNG).

Die für den Aufgabenbereich Nachrichtendienst zuständige Organisationseinheit der DSN verantwortete insbesondere die umfassende und frühzeitige Aufklärung, Auswertung und Analyse sowie fortlaufende Beurteilung sämtlicher verfassungsschutzrelevanter Bedrohungslagen im Inland. Dazu gehörte auch die Beobachtung einer Gruppierung, wenn im Hinblick auf diese damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität kommt. Somit sollte umfassendes Wissen über die aktuelle Lage, aktuelle Entwicklungen und künftige Szenarien generiert werden, um adäquate Handlungsstrategien entwickeln zu können.

Eine weitere zentrale Aufgabe lag in der Prävention, sohin der Koordination, Steuerung und Förderung der gesamtstaatlichen Zusammenarbeit. Dies umfasste die Erarbeitung von Strategien und Handlungsempfehlungen sowie die Koordination und Durchführung von entsprechenden Maßnahmen. Zudem sollten Nachrichtendienste im regelmäßigen Kommunikations- und Informationsaustausch mit anderen Diensten sein und mit sicherheitsrelevanten Akteuren, jeweils im In- und Ausland, kooperieren. Zum Aufgabenbereich gehörte auch der besondere Schutz von sensiblen Informationen und Geheimnissen, Cyber-Sicherheit sowie die Abwehr von Cyber-Spionage.[17]

Weiters waren zahlreiche Organisationseinheiten in der Zentralstelle des Innenministeriums, die Sicherheitsakademie, die Kontrollkommission[18], die bzw. der Rechtsschutzbeauftragte und auf Ebene der Landespolizeidirektionen die Landesämter Staatsschutz und Extremismusbekämpfung mit Maßnahmen im Bereich der Spionageprävention betraut.

(3) Im Verteidigungsministerium waren das Abwehramt und das Heeres-Nachrichtenamt auf Grundlage des § 20 Militärbefugnisgesetz für die nachrichtendienstliche Aufklärung und Abwehr eingerichtet.

- Das Abwehramt war zuständig für die Abwehr von Gefahren für die militärische Sicherheit sowohl im Inland als auch von zu Auslandseinsätzen entsandten Kontingenten. Es sammelte Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen Leben und Gesundheit von Personen, gegen Infrastruktur und militärisch klassifizierte Informationen erwarten ließen.[19] Durch das vorzeitige Erkennen sollten Straftaten verhindert werden.

[17] vgl. https://www.dsn.gv.at/104/ (abgerufen am 5. März 2025)

[18] Die Kontrollkommission war ein gemäß Art. 20 Abs. 2 Z 2 Bundes-Verfassungsgesetz unabhängiges und weisungsfreies Organ der Verwaltung im Rahmen ihrer Aufgaben. Sie war gemäß § 17a SNG seit ihrer Einsetzung u.a. mit der begleitenden strukturellen Kontrolle der DSN und der Landesämter Staatsschutz und Extremismusbekämpfung betraut, um insbesondere systemische Mängel und bestehenden Optimierungsbedarf der Organisationen aufzuzeigen.

[19] vgl. https://www.bundesheer.at/unser-heer/organisation/nachrichtendienste (abgerufen am 5. März 2025)

- Das Heeres-Nachrichtenamt war zuständig für die strategische Auslandsaufklärung. Seine Bediensteten beschafften Informationen über Regionen, Staaten und Organisationen, die für die österreichische und europäische Sicherheitspolitik relevant waren. Diese Informationen wurden analysiert und in Form von Berichten und Präsentationen als Entscheidungsgrundlage der Führung aufbereitet.[20]

(4) Im Außenministerium wirkten mehrere Organisationseinheiten an der Spionageprävention mit. Das Außenministerium befasste die relevanten Bundesministerien und Nachrichtendienste u.a. in allen Agrémentverfahren[21] – diese betrafen bilaterale Botschafterinnen und Botschafter und Militärattachés – sowie in einigen Fällen vor der Erteilung von Dienstantrittsvisa für andere Personen. Es war darüber hinaus auf Grundlage des Art. 9 des Wiener Übereinkommens über diplomatische Beziehungen (in der Folge: **Wiener Übereinkommen**) berechtigt, ohne Angabe von Gründen Diplomatinnen und Diplomaten zur unerwünschten Person (persona non grata) zu erklären und sie aufzufordern, das Land zu verlassen.

Personelle und finanzielle Ressourcen zur Spionageprävention

Innenministerium

Personelle Ressourcen

7.1 (1) Im Innenministerium nahm eine eigene Organisationseinheit die Aufgaben der Spionageabwehr bzw. Spionageprävention im Zusammenhang mit den Vorgaben des SNG, des Sicherheitspolizeigesetzes, der Strafprozessordnung[22] und des Strafgesetzbuchs wahr. Im vom RH überprüften Zeitraum war dies von 2017 bis November 2021 das BVT, ab Dezember 2021 die DSN. Sie war neben dem Phänomenbereich Spionage insbesondere auch für die Bereiche Extremismus, Terrorismus, Cybersicherheit sowie illegaler Handel mit Kriegswaffen und Proliferation zuständig.

Die Innenministerin bzw. der Innenminister hatte dem Ständigen Unterausschuss gemäß § 17 Abs. 3 SNG halbjährlich Bericht über die Wahrnehmung der Aufgaben nach dem SNG zu erstatten. Mit Wirksamkeit vom 1. Dezember 2021 (Einrichtung der DSN) wurde diese Verpflichtung dahingehend erweitert, dass jährlich auch über die personelle und finanzielle Ressourcenausstattung der DSN zu berichten war.

[20] vgl. https://www.bundesheer.at/unser-heer/organisation/nachrichtendienste (abgerufen am 5. März 2025)

[21] Agrément bezeichnet die völkerrechtliche Zustimmung des Empfangsstaates, Vertreterinnen und Vertreter des Entsendestaates für eine diplomatische oder sonstige Mission zu empfangen.

[22] BGBl. 631/1975 i.d.g.F.

Die DSN wies die Anzahl der ihr zugewiesenen Planstellen und den personellen Ist-Stand in den Berichten gemäß § 17 Abs. 3 SNG an den Ständigen Unterausschuss regelmäßig aus. Zufolge des Berichts für das zweite Halbjahr 2024 hatte sich mit 31. Dezember 2024 die Zahl der bei der DSN beschäftigten Bediensteten im Vergleich zur Zahl der mit 1. Dezember 2021 vom BVT übernommenen Bediensteten annähernd verdoppelt.

(2) Der RH identifizierte in Abstimmung mit dem Innenministerium die dem Phänomenbereich Spionage bzw. Spionageabwehr zuzuordnenden internen Organisationseinheiten der DSN bzw. der Vorläuferorganisation BVT und ermittelte auf dieser Basis – gegebenenfalls anteilig – die dafür verfügbaren personellen Ressourcen (Planstellen und tatsächliche Personalstände) in deren zeitlicher Entwicklung. Die DSN wies in diesem Zusammenhang darauf hin, dass der Begriff „Spionageprävention“ in der Literatur nicht exakt definiert und überdies beim Übergang vom BVT zur DSN eine neue Struktur definiert worden sei. Die erhobenen Zahlen könnten somit nur Näherungswerte darstellen.

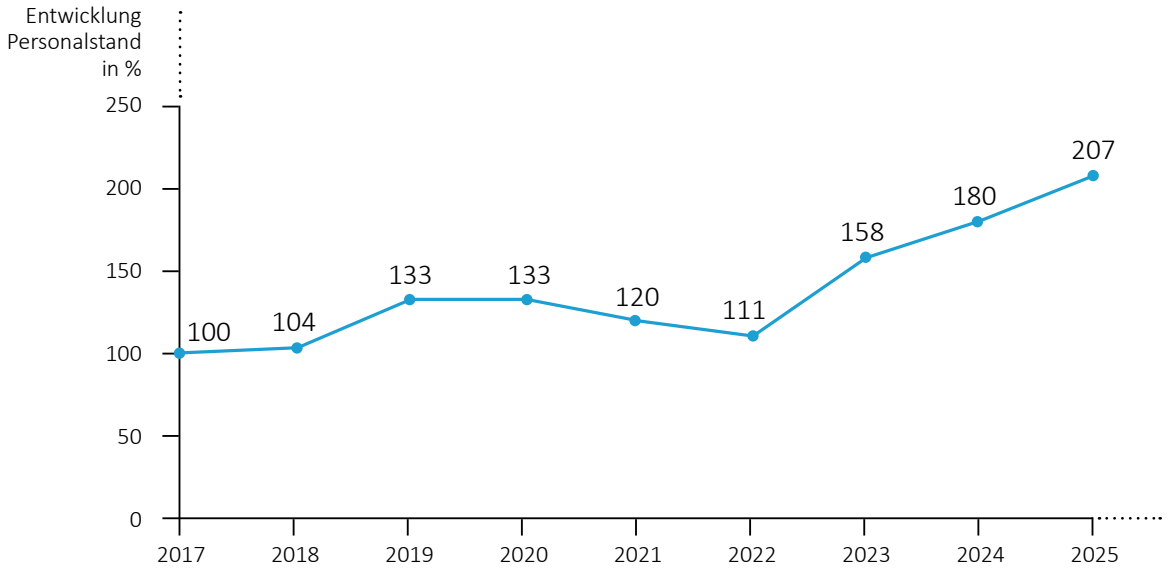
Die für die Spionageabwehr relevanten Organisationseinheiten bzw. Tätigkeitsfelder bei der DSN waren

- Informationssicherheit (seit November 2024),
- interne Sicherheit und Risikomanagement (Informations- und Geheimschutz, Personen- und Objektsicherheit, Vertrauenswürdigkeitsprüfungen),
- Schutz kritischer Infrastrukturen,
- Informationsgewinnung (offene und verdeckte Informationsgewinnung, Observation),
- Informationsauswertung und -analyse (operative Analysen und Lagebilder, Datensicherung, -aufbereitung und -auswertung) sowie
- Ermittlung, Fahndung und Gefahrenabwehr (operative Ermittlungen, vorbeugender Schutz, kriminalpolizeiliche Aufgaben gemäß Strafprozessordnung).

Das Innenministerium erhöhte die Anzahl der gemäß den genannten Tätigkeitsfeldern für die Spionageabwehr (bzw. den Phänomenbereich Spionage) gewidmeten Planstellen insbesondere seit Einrichtung der DSN deutlich: mit 1. Jänner 2022 auf 181 % des Standes vom 1. Jänner 2017, mit 1. Jänner 2025 auf 219 %. Der Anteil des Bereichs am gesamten Personal der DSN betrug mit 1. Jänner 2025 16 %.

Die tatsächlichen für den Phänomenbereich Spionage zur Verfügung stehenden personellen Ressourcen entwickelten sich mit Ausgangsdatum 1. Jänner 2017 und jeweils zum Stand 1. Jänner wie folgt:

Abbildung 1: Personal Spionageabwehr im Innenministerium (DSN bzw. davor BVT)



Personalstand 1. Jänner 2017 bildet Basis von 100 %.
Personalstand jeweils 1. Jänner

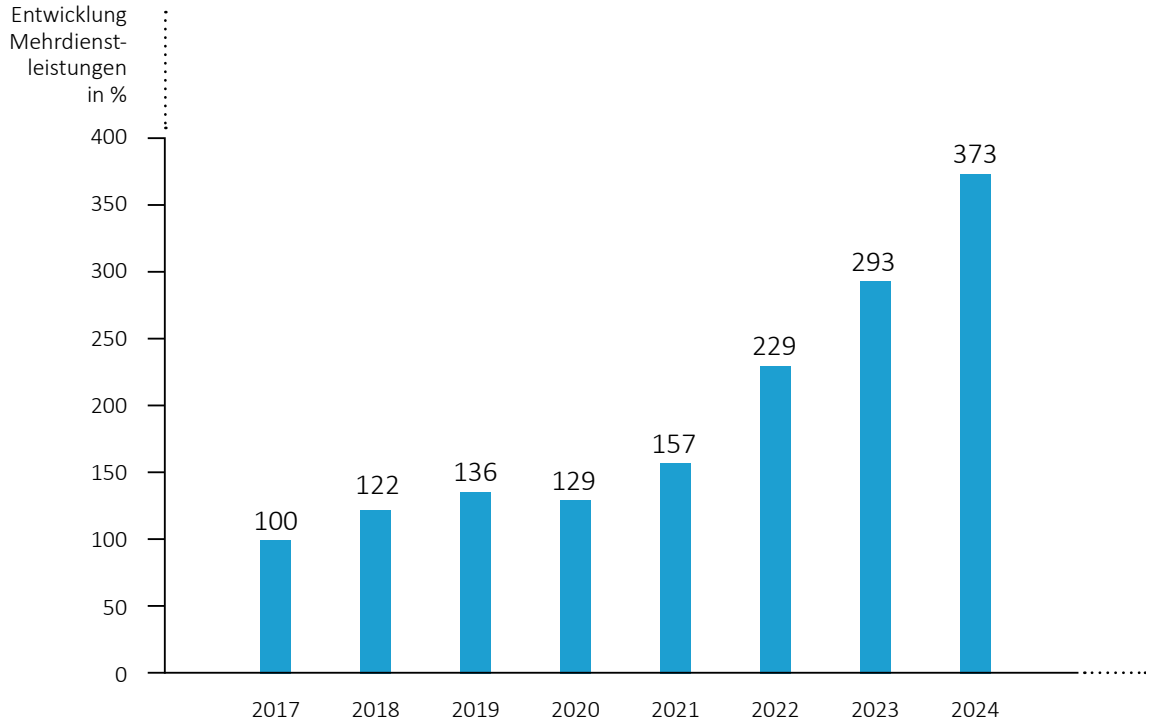
Quelle: BMI; Darstellung: RH

Kurz nach Einrichtung der DSN mit Stand 1. Jänner 2022 waren 57 % der Planstellen im Bereich Spionageabwehr besetzt, mit 1. Jänner 2025 waren es 88 %.

(3) Das Innenministerium evaluierte ab Sommer 2023 alle drei organisatorischen Bereiche (Direktion, Staatsschutz und Nachrichtendienst). Dabei zeigte sich u.a., dass die mit der Einrichtung der DSN zusätzlich übernommenen und erweiterten Aufgaben nur mit einer weiteren deutlichen Erhöhung der Planstellen insgesamt ausreichend erfüllt werden könnten. Die DSN beantragte darauf basierend beim Innenministerium zusätzliche Planstellen und die Genehmigung bewerteter Arbeitsplätze. Das Vorhaben war zur Zeit der Gebarungsüberprüfung des RH noch nicht vollständig umgesetzt. Personeller Handlungsbedarf mit Relevanz für den Phänomenbereich Spionage bestand demnach vor allem in den Aufgabenbereichen Informationsgewinnung und -auswertung sowie Ermittlung, Fahndung und Gefahrenabwehr.

Die zunehmenden – nicht zuletzt geopolitisch bedingten – Herausforderungen für die DSN zeigten sich auch in den von den Bediensteten der DSN erbachten Mehrdienstleistungen. Die Auszahlungen dafür entwickelten sich im überprüften Zeitraum, gemessen am Jahr 2017, wie folgt:

Abbildung 2: Entwicklung Mehrdienstleistungen (DSN bzw. davor BVT)



Mehrdienstleistungen 1. Jänner 2017 bilden Basis von 100 %. Quelle: BMI; Darstellung: RH

Zwischen 2017 und 2024 – insbesondere ab dem Jahr 2022 – stiegen die Auszahlungen für Mehrdienstleistungen deutlich auf nahezu das Vierfache. Der Anteil an den Personalkosten stieg von 12 % auf 15 %. Die DSN wies gegenüber dem RH darauf hin, dass sich die gestiegenen Mehrdienstleistungen aufgrund der Entwicklung der Bedrohungslagen und des dafür zu geringen Personalstandes ergeben hätten.

7.2 (1) Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung personeller Ressourcen zur Spionageprävention einzubeziehen.

Der RH empfahl daher dem Innenministerium, die personellen Ressourcen zur Spionageprävention entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen.

(2) Darüber hinaus hielt der RH fest, dass das Innenministerium die personellen Ressourcen für die Spionageabwehr von 1. Jänner 2017 bis 1. Jänner 2025 deutlich erhöhte, vor allem ab Einrichtung der DSN mit Dezember 2021. Der Personalstand in Vollbeschäftigungsäquivalenten (**VBÄ**) lag am 1. Jänner 2025 bei 207 % des Wertes vom 1. Jänner 2017. Gleichzeitig stiegen im Hinblick auf internationale Entwicklungen und die veränderte Bedrohungslage die Anforderungen an die DSN insgesamt und insbesondere auch im Bereich der Spionageabwehr deutlich. Dies kam u.a. auch durch den starken Anstieg der Auszahlungen für Mehrdienstleistungen zwischen 2017 und 2024 – insbesondere ab 2022 – auf 373 % des Ausgangswerts 2017 zum Ausdruck.

Anträge der DSN auf eine den gestiegenen Anforderungen entsprechende Personalaufstockung in allen Phänomenbereichen und im Konkreten auch im Phänomenbereich Spionage waren mit Stand Anfang 2025 noch nicht vollständig umgesetzt. Im Phänomenbereich Spionage betraf dies insbesondere die Tätigkeitsbereiche Informationsgewinnung und -auswertung sowie Ermittlung, Fahndung und Gefahrenabwehr.

Dem Innenministerium empfahl der RH, den personellen Ausbau der DSN, insbesondere im Bereich der Spionageabwehr, weiterhin voranzutreiben. Bei der Beantragung zusätzlicher Planstellen bzw. bewerteter Arbeitsplätze wäre dabei auf Basis regelmäßiger Bedarfsanalysen eine Priorisierung nach Dringlichkeit vorzunehmen.

Der RH empfahl der DSN, bis zur Umsetzung der Anträge zur Personalaufstockung sicherzustellen, dass ihr vorhandenes Personal entsprechend den laufenden Entwicklungen und der Bedrohungslage in den unterschiedlichen Phänomenbereichen flexibel eingesetzt werden kann.

7.3 Laut Stellungnahme des Innenministeriums werde der Empfehlung des RH, mehr personelle (und finanzielle) Ressourcen für die Spionageprävention bereitzustellen, seitens der DSN vollinhaltlich zugestimmt. Der Aufbau zusätzlicher Ressourcen sei notwendig, da in den letzten Jahren ein deutlicher Zuwachs im Phänomenbereich Spionage zu verzeichnen gewesen sei. Aufgrund der aktuellen geopolitischen Lage sei zudem zu erwarten, dass diese Bedrohungen weiter zunehmen werden. Daher sei es unerlässlich, die personellen (und finanziellen) Mittel der DSN zu verstärken, um den Herausforderungen der Zukunft gewachsen zu sein und die nationale Sicherheit nachhaltig zu gewährleisten.

Der personelle Ausbau der DSN sei trotz der angespannten budgetären Situation vorgesehen. Im Rahmen der laufenden Evaluierung erfolge eine Bedarfsanalyse für die jeweiligen Bereiche. Auch in der Spionageabwehr seien entsprechende Personalaufstockungen vorgesehen.

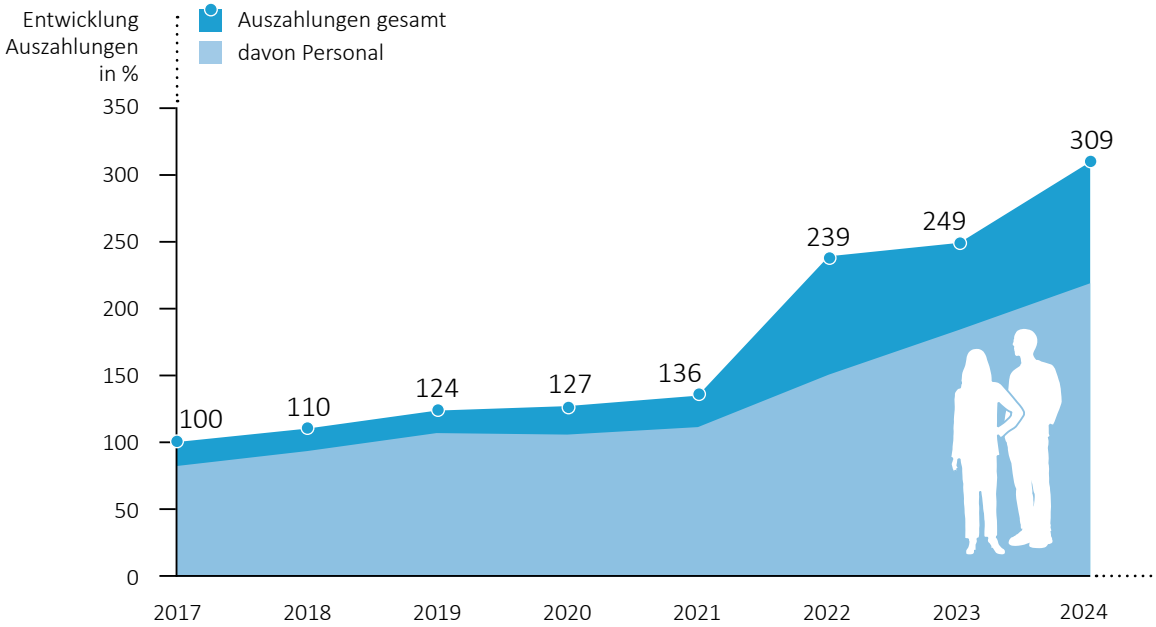
Im Bereich der Informationsgewinnung erfolge der Personaleinsatz bereits entsprechend identifizierter Prioritäten. Im Rahmen der Evaluierung der DSN würden auch die darüber hinausgehenden Möglichkeiten des anlassbezogenen, flexiblen Einsatzes der Mitarbeiterinnen und Mitarbeiter phänomenübergreifend innerhalb der DSN überprüft.

Finanzielle Ressourcen

8.1 Eigene finanzgesetzliche Ansätze (Budgets) für Staatsschutz und Nachrichtendienst (DSN bzw. Vorgängerorganisation BVT) bestanden nicht. Die tatsächlichen jährlichen Auszahlungen waren für den RH aber feststellbar. Der Aufgabenbereich der Spionageabwehr war in diesen Zahlen jeweils enthalten, eine gesonderte Auswertung bzw. getrennte Darstellung war nicht vorgesehen bzw. möglich.

Die Auszahlungen für das BVT (bis 2021) sowie für die DSN (ab 2022) insgesamt entwickelten sich – auf Basis des Jahres 2017 – gemäß einer Auswertung des RH aus der Haushaltsverrechnung des Bundes wie folgt:

Abbildung 3: Entwicklung der Auszahlungen für Staatsschutz und Nachrichtendienst sowie Anteil der Personalauszahlungen (DSN bzw. davor BVT)



1. Jänner 2017 bildet Basis von 100 %.

Quelle: BMI; Darstellung: RH

Die DSN wies ab dem Jahr 2022 – entsprechend den gesetzlichen Vorgaben – ihre jährlichen Gesamtauszahlungen in den Berichten gemäß § 17 Abs. 3 SNG an den Ständigen Unterausschuss aus. Die darin angeführten Werte stimmten mit den Werten gemäß den Auswertungen des RH aus der Haushaltsverrechnung des Bundes überein.

Die Auszahlungen für den Staatsschutz und den Nachrichtendienst stiegen von 2017 bis 2021 moderat und in der Folge ab 2022 stark. Insgesamt hatten sich die Auszahlungen von 2017 auf 2024 mehr als verdreifacht, der Anstieg bei den Personalauszahlungen war mit einem Plus von 183 % etwas geringer. Bis 2021 lag der Anteil der Personalauszahlungen an den gesamten Auszahlungen über 80 % (zwischen 82 % und 87 %), im Jahr 2022 lag er bei 63 %, 2023 und 2024 bei etwa 75 %. Der vergleichsweise hohe Anteil des Sachaufwands im Jahr 2022 war insbesondere auf IKT-Investitionen im Zusammenhang mit dem Aufbau der DSN zurückzuführen (IKT-Infrastruktur, Analyseplattform). Allgemein resultierte der höhere Anteil des Sachaufwands ab Einrichtung der DSN im Jahr 2022 vor allem aus nachhaltig höheren Mietaufwendungen und gestiegenen Auszahlungen für Verwaltungspraktikantinnen und -praktikanten – Letztere wurden als Sachaufwand verrechnet.

8.2 Der RH hielt fest, dass sich die Auszahlungen des Innenministeriums für den Aufgabenbereich Staatsschutz und Nachrichtendienst zwischen 2017 und 2024 mehr als verdreifachten. Der Bereich der Spionageabwehr war zwar nicht gesondert auswertbar, wegen des hohen Anteils der Personalauszahlungen – und analoger Entwicklung der Personalressourcen für Spionageabwehr – war diese Gesamtentwicklung aus Sicht des RH auf den Bereich der Spionageabwehr übertragbar und ein solcher Zuwachs auch plausibel.

Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung finanzieller Ressourcen zur Spionageprävention einzubeziehen.

Der RH empfahl daher dem Innenministerium, die finanziellen Ressourcen zur Spionageprävention entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen.

8.3 Laut Stellungnahme des Innenministeriums werde seitens der DSN auch dieser Empfehlung des RH vollinhaltlich zugestimmt. Der Aufbau zusätzlicher Ressourcen sei notwendig, da in den letzten Jahren ein deutlicher Zuwachs im Phänomenbereich Spionage zu verzeichnen gewesen sei. Aufgrund der aktuellen geopolitischen Lage sei zudem zu erwarten, dass diese Bedrohungen weiter zunehmen werden. Daher sei es unerlässlich, die (personellen und) finanziellen Mittel der DSN zu

verstärken, um den Herausforderungen der Zukunft gewachsen zu sein und die nationale Sicherheit nachhaltig zu gewährleisten.

Verteidigungsministerium

Personelle Ressourcen

9.1 (1) Die Aufgaben der Spionageabwehr im Verteidigungsministerium nahm im Wesentlichen das generell für die Abwehr von Gefahren für die militärische Sicherheit zuständige Abwehramt wahr. Dieses war – wie das für die Auslandsaufklärung zuständige Heeres-Nachrichtenamt – unmittelbar dem Chef des Generalstabs zugeordnet.

Maßgeblich für die personelle Ausstattung des Abwehramtes waren der Organisationsplan und seine organisatorische Gliederung. Der im Jahr 2017 geltende Organisationsplan war seit 2013 in Kraft. Im Jahr 2022 setzte das Verteidigungsministerium einen neuen Organisationsplan um, der mehr Arbeitsplätze im Abwehramt aufwies. Nach Angaben des Abwehramtes entsprach diese Erhöhung allerdings nicht ausreichend der gestiegenen Anzahl an Aufträgen.

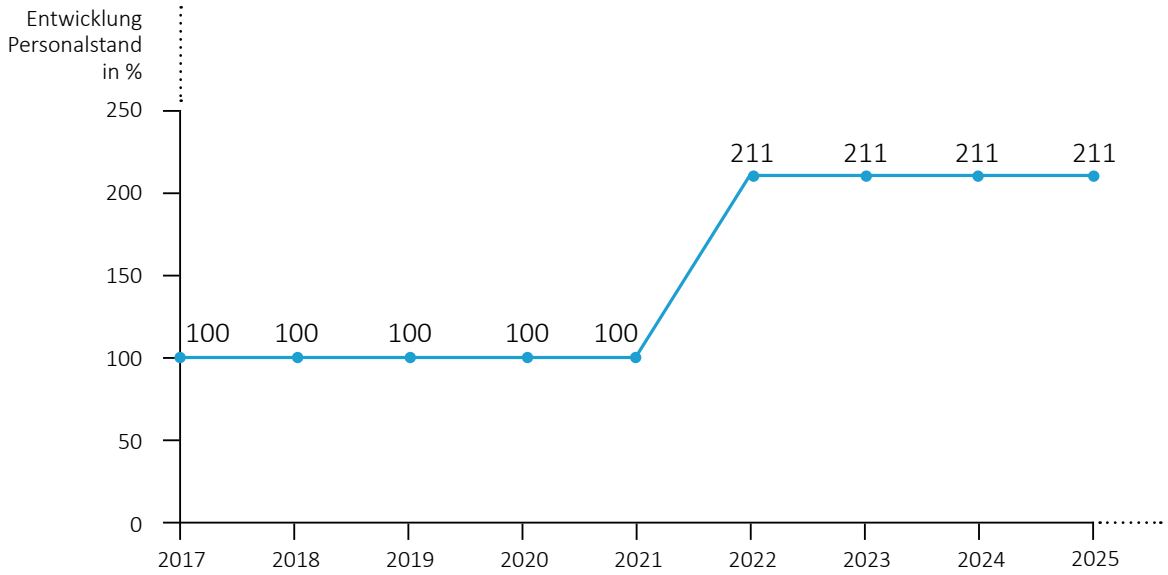
(2) Der RH identifizierte in Abstimmung mit dem Abwehramt die Organisationselemente, deren Hauptaufgaben im Bereich Spionageabwehr lagen:

- Militärische Sicherheit: Präventionsmaßnahmen gegen Wirtschafts- und Industriespionage im Zuge von Unternehmensprüfungen und Geheimschutzbetreuung, Verlässlichkeitsprüfungen;
- Operative Angelegenheiten: Fallbearbeitungen im Rahmen nachrichtendienstlicher Abwehr, operative Einsätze nach den Befugnissen des Militärbefugnisgesetzes, Fallauswertung und Maßnahmen der Prävention;
- Nachrichtendienstliche Cyber-Abwehr: nachrichtendienstliche IKT-Sicherheit, Auditierung von IKT-Systemen – Raumüberprüfungen, z.B. in Botschaften im Ausland.

Daneben leisteten bedarfsbezogen auch andere Bedienstete des Abwehramtes im Rahmen fallweiser Einteilungen bei der Planung und Durchführung nachrichtendienstlicher Operationen einen Beitrag zur Spionageabwehr.

Die Anzahl der im Abwehramt spezifisch im Bereich der Spionageabwehr eingesetzten Bediensteten veränderte sich im überprüften Zeitraum 2017 bis Anfang 2025 (jeweils Stichtag 1. Jänner) wie folgt:

Abbildung 4: Personal für Spionageabwehr beim Abwehramt



Personalstand 1. Jänner 2017 bildet Basis von 100 %.
Personalstand jeweils 1. Jänner

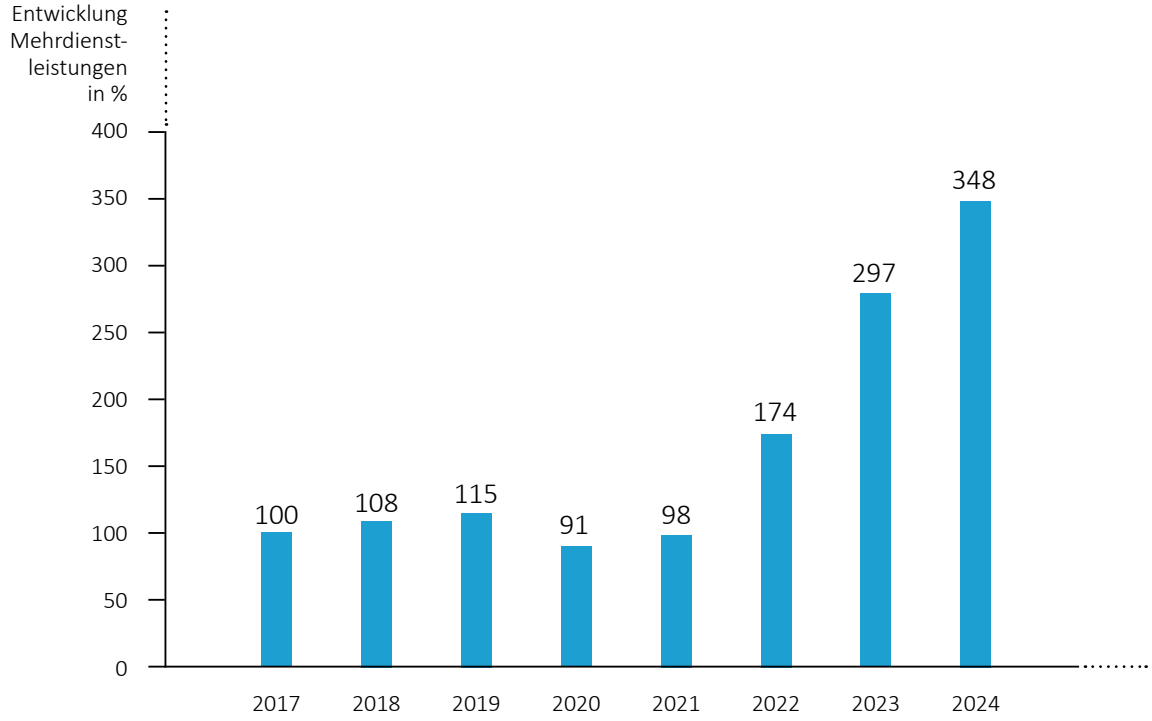
Quelle: BMLV; Darstellung: RH

Der Personalstand für den Bereich der Spionageabwehr hatte sich nach Angaben des Verteidigungsministeriums bereits zuvor seit zumindest 2008 nicht verändert. Die Umsetzung des neuen Organisationsplans mit 2022 ermöglichte dem Abwehramt eine Anpassung bzw. Aufstockung der personellen Ressourcen, insbesondere auch durch Umschichtungen zugunsten der Spionageabwehr.

Die für die Spionageabwehr vorgesehenen Arbeitsplätze waren zu den angegebenen Stichtagen vollständig besetzt, weil Rekrutierungen bzw. Nachbesetzungen aus Gründen der militärischen Sicherheit grundsätzlich unmittelbar intern – aus dem Personal des Abwehramtes – erfolgten. Der Anteil der Spionageabwehr am Gesamtpersonal des Abwehramtes lag Anfang 2025 bei 22 %.

(3) Die Auszahlungen für Mehrdienstleistungen der Bediensteten des Abwehramtes entwickelten sich im überprüften Zeitraum, gemessen am Jahr 2017, wie folgt:

Abbildung 5: Entwicklung Mehrdienstleistungen Abwehramt



Mehrdienstleistungen 1. Jänner 2017 bilden Basis von 100 %. Quelle: BMLV; Darstellung: RH

Die Auszahlungen für Mehrdienstleistungen blieben von 2017 bis 2021 nahezu unverändert, ab 2022 stiegen sie markant auf das Dreieinhalbfache im Jahr 2024. Nach Angaben des Abwehramtes war dafür vor allem der zeitintensive Personaleinsatz im Bereich der Spionageabwehr verantwortlich, der durch die veränderte internationale Bedrohungslage und verstärkte ausländische Spionagetätigkeiten besonders betroffen war. Demnach war insbesondere ab 2022 auch die Zahl der im Rahmen der Geheimschutzbetreuung erfassten Unternehmen (Folgeaufwand nach Ausstellung einer Sicherheitsbescheinigung für Unternehmen) deutlich gestiegen.

9.2 (1) Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung personeller Ressourcen zur Spionageprävention einzubeziehen.

Der RH empfahl daher dem Verteidigungsministerium, die personellen Ressourcen zur Spionageprävention entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen.

(2) Der RH hielt fest, dass das Verteidigungsministerium die im Abwehramt spezifisch für den Bereich der Spionageabwehr zur Verfügung stehenden Personalressourcen von 2017 bis 2024 mehr als verdoppelte; dies war im Wesentlichen mit der Umsetzung des neuen Organisationsplans im Jahr 2022 und internen Umschichtungen begründet.

Die seit 2022 durch die internationale Bedrohungslage – insbesondere infolge des Krieges in der Ukraine sowie verstärkter Spionagetätigkeit – gestiegenen Anforderungen an die militärische Spionageabwehr verursachten allerdings Bedarf an zusätzlichen personellen Ressourcen, was sich u.a. auch in einer deutlichen Steigerung der Auszahlungen für Mehrdienstleistungen in diesem Bereich zeigte.

Der RH empfahl daher dem Verteidigungsministerium, regelmäßig die personellen Ressourcen für die Spionageabwehr der internationalen Bedrohungslage anzupassen und den Organisationsplan des Abwehramtes in diesem Sinne zu überarbeiten.

9.3 Das Verteidigungsministerium teilte in seiner Stellungnahme mit, dass im Rahmen des Aufbauplans 2032+ ein Innovationsprozess zur Identifizierung verstärkter, zusätzlicher und neuer nachrichtendienstlicher Fähigkeiten sowie der erforderlichen Ressourcen und eine Überarbeitung des Organisationsplans des Abwehramtes stattgefunden hätten. Der überarbeitete Organisationsplan sehe vermehrte personelle Ressourcen für den Phänomenbereich Spionagebedrohungen vor. Der Entwurf des Organisationsplans sei Ende Jänner 2026 an das Bundeskanzleramt weitergeleitet worden.

Abhängig von der Bewertung bzw. innerministeriellen Umsetzung des überarbeiteten Organisationsplans benötige das Abwehramt die Zuweisung von Planstellen, um den Organisationsplan personell abzubilden.

Finanzielle Ressourcen

10.1 Entsprechend der organisatorischen Zuordnung (TZ 9) waren die militärischen Nachrichtendienste budgetär in den Generalstab integriert. Eine nähere Detaillierung und interne Kennzeichnung bestanden nicht. Eine strukturierte Auswertung und Zuordnung von Auszahlungen zum Abwehramt sowie im Besonderen zum Aufgabenbereich Spionageabwehr waren nicht möglich.

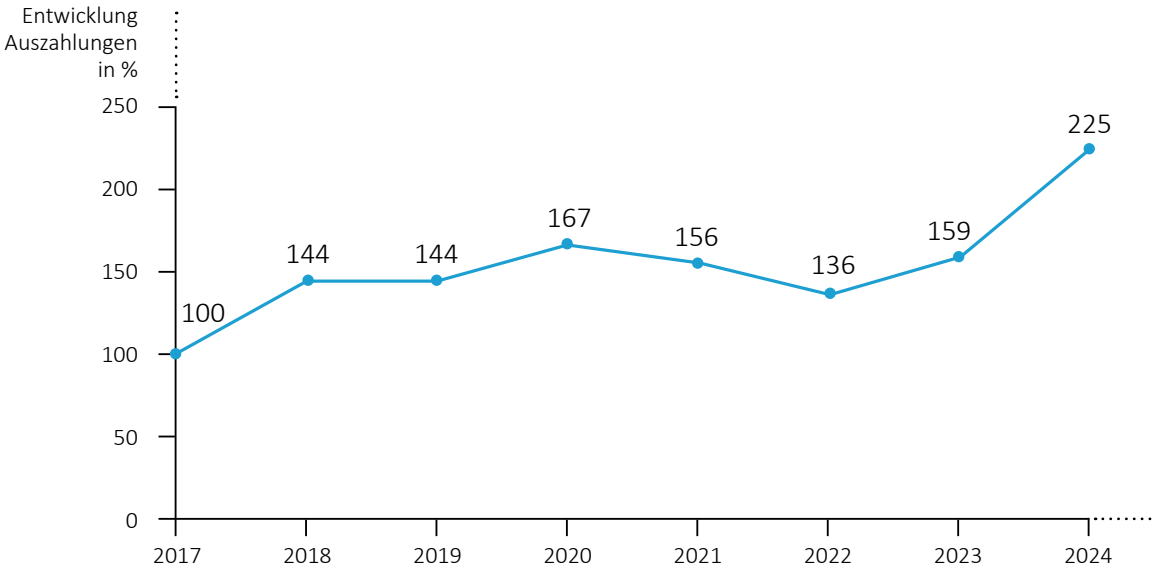
Eine Verpflichtung, den zur Kontrolle der Nachrichtendienste des Bundesheeres eingerichteten Ständigen Unterausschuss des Landesverteidigungsausschusses im Nationalrat über personelle und finanzielle Ressourcen zu informieren, sah das Militärbefugnisgesetz – anders als das SNG für die DSN – nicht vor.

Im überprüften Zeitraum waren die Auszahlungen für das Abwehramt von 2017 bis 2022 im Detailbudget erster Ebene (Generalstabsdirektion) enthalten. Nach einer im Jahr 2021 verfügten neuen Organisationsstruktur im Verteidigungsministerium, aus der auch wesentliche Änderungen in der Budgetstruktur resultierten, waren die Auszahlungen des Abwehramtes 2023 und 2024 dem Detailbudget zweiter Ebene (Generalstab) zugeordnet. Da die Inhalte dieser Detailbudgets nicht deckungsgleich waren, war auch auf übergeordneter Ebene keine Entwicklung über den gesamten überprüften Zeitraum darstellbar.

Auf Ersuchen des RH stellte die für das Budget des Generalstabs zuständige Leitung der Generalstabsabteilung den „Sachmittelaufwand“ für das Abwehramt in den Jahren 2017 bis 2024 zur Verfügung. Nicht enthalten waren darin insbesondere Auszahlungen für Investitionen oder den IKT-Bereich (z.B. Lizenzen, Hard- und Softwareanpassungen) sowie Mieten. Mangels gesonderter Kennzeichnung innerhalb des jeweiligen Detailbudgets konnte die Generalstabsabteilung auch keine Angaben zur Höhe der Personalauszahlungen im Abwehramt machen.

Ausgehend vom Jahr 2017 entwickelte sich der Sachmittelaufwand wie folgt:

Abbildung 6: Entwicklung des Sachmittelaufwands für das Abwehramt



1. Jänner 2017 bildet Basis von 100 %.

Quelle: BMLV; Darstellung: RH

Die Steigerung um 125 Prozentpunkte war insbesondere auf die deutliche Steigerung im Jahr 2024 zurückzuführen. Da wesentliche Sachaufwendungen sowie der Personalaufwand nicht enthalten waren, war die Aussagekraft darüber begrenzt, wie hoch die finanziellen Ressourcen waren, die dem Abwehramt zur Erfüllung seiner Aufgaben zur Verfügung standen.

Der Anteil des Personalaufwands im Detailbudget des Generalstabs lag im Zeitraum 2017 bis 2022 (alte Struktur) zwischen 72 % (2022) und 82 % (2019), in den Jahren 2023 und 2024 jeweils bei 92 %.

10.2 Der RH hielt fest, dass es wegen der fehlenden budgetären Zuordnung sowie der Änderung der Budgetstruktur im überprüften Zeitraum nicht möglich war, valide Zahlen zu den finanziellen Ressourcen zu erheben, die den Nachrichtendiensten des Bundesheeres und konkret dem Abwehramt insgesamt bzw. der Spionageabwehr zur Verfügung standen; auch war die Entwicklung der Auszahlungen in diesem Bereich nicht zuverlässig darstellbar. Aufgrund des hohen Anteils der Personalauszahlungen in den relevanten Budgetbereichen waren aus Sicht des RH aber die Entwicklungen der personellen Ressourcen für die Spionageabwehr (TZ 9) zumindest größenordnungsmäßig auf jene der finanziellen Ressourcen im Bereich der Spionageabwehr übertragbar.

Der RH empfahl dem Verteidigungsministerium, die Auszahlungen für die militärischen Nachrichtendienste im Budgetvollzug im Sinne einer effizienten Steuerungsmöglichkeit intern zu kennzeichnen.

Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung finanzieller Ressourcen zur Spionageprävention einzubeziehen.

Der RH empfahl daher dem Verteidigungsministerium, die finanziellen Ressourcen zur Spionageprävention entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen.

10.3 Laut Stellungnahme des Verteidigungsministeriums werde, nach der Reorganisation, durch neue budgetäre Zuordnungen hinkünftig ein besserer Nachweis des Budgetvollzugs ermöglicht. Aus Sicherheitsinteressen werde das Verteidigungsministerium keine weitere Unterteilung (z.B. für Spionageprävention) vornehmen, aus der Rückschlüsse auf die Strukturen und Fähigkeiten ableitbar wären.

Außenministerium

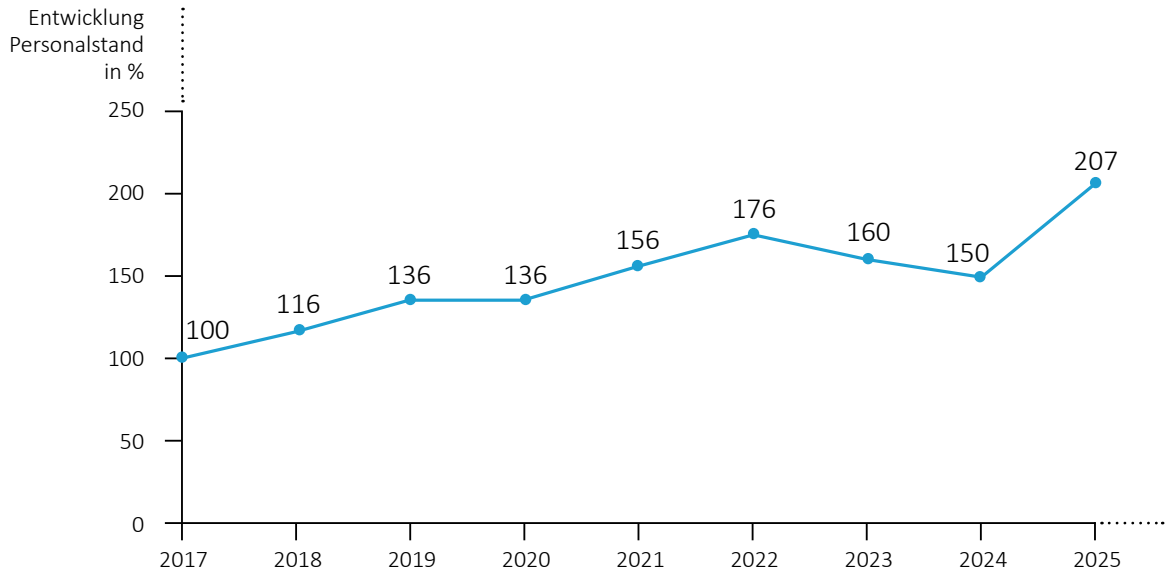
Personelle Ressourcen

11.1 Im Außenministerium war keine spezifische Organisationseinheit für Spionageabwehr (bzw. Spionageprävention) zuständig. Nach Angabe des Außenministeriums waren die unterschiedlichen Aspekte der Spionageprävention als umfassender Aufgabenbereich zu sehen, an dem mehrere Organisationseinheiten des Ministeriums mitwirkten. Insbesondere waren folgende Abteilungen mit dem Thema befasst:

- Sicherheitsangelegenheiten: Fragen der personellen und physischen Sicherheit sowie ressortweite Belange der Informationssicherheit einschließlich IKT-Sicherheit,
- Sicherheitspolitische Angelegenheiten: militärische, zivile und hybride Bedrohungen, Einbindung in innerstaatlichen und internationalen Informationsaustausch zu Aspekten nachrichtendienstlicher Tätigkeiten fremder Staaten,
- IKT-Sicherheit: operative Sicherheit der IT-Netzwerke, Security Operation Center.

Im überprüften Zeitraum entwickelte sich der Personalstand (VBÄ) in den mit Spionageabwehr befassten Organisationseinheiten des Außenministeriums – ausgehend vom 1. Jänner 2017 – wie folgt:[23]

Abbildung 7: Personal Spionageprävention Außenministerium



Personalstand 1. Jänner 2017 bildet Basis von 100 %.
Personalstand jeweils 1. Jänner

Quelle: BMEIA; Darstellung: RH

[23] Aus der Abteilung IKT-Sicherheit ist lediglich das Personal des Security Operation Centers berücksichtigt, daneben war eine Reihe von Bediensteten bei Sicherheitsthemen mitbefasst.

Der personelle Zuwachs war insbesondere auf die Abteilung Sicherheitspolitische Angelegenheiten zurückzuführen.

11.2 Der RH hielt fest, dass im Außenministerium keine spezifische Organisationseinheit für Spionageabwehr zuständig war, entsprechende Aufgaben waren auf mehrere Abteilungen verteilt. Zwischen 1. Jänner 2017 und 1. Jänner 2025 stieg der Personalstand in den primär mit dem Aufgabenbereich befassten Abteilungen auf knapp mehr als das Doppelte.

Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung personeller Ressourcen zur Spionageprävention einzubeziehen.

Der RH empfahl daher dem Außenministerium, die personellen Ressourcen zur Spionageprävention entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen.

11.3 Laut Stellungnahme des Außenministeriums werde es die Empfehlung nach Maßgabe der budgetären Möglichkeiten umsetzen.

Finanzielle Ressourcen

12.1 Budgetmittel für den Aufgabenbereich Spionageabwehr bzw. -prävention waren im Außenministerium nicht gesondert veranschlagt oder ausgewiesen. Nach Angaben des Außenministeriums habe es im überprüften Zeitraum Beschaffungen zur Abwehr von Bedrohungen anlassbezogen sowie im Rahmen von routinemäßigen operativen Sicherheitsmaßnahmen durchgeführt. So sei etwa zur konkreten Abwehr von Cyber-Angriffen im Jahr 2020 ein externer Dienstleister mit Expertise für solche Vorfälle – mit Kosten von rd. 1,70 Mio. EUR – beauftragt worden. Weitere Beschaffungen zur anlassbezogenen Cyber-Abwehr habe das Ministerium 2022 und 2023 (Kosten jeweils rd. 0,30 Mio. EUR) durchgeführt. Der RH verwies in diesem Zusammenhang auf die Ergebnisse seiner Überprüfung zur Koordination der Cyber-Sicherheit (Reihe Bund 2022/13, TZ 24 ff.).

Laut Außenministerium liege der Anteil für Sicherheit am IT-Gesamtbudget im Durchschnitt bei 15 % bis 20 %. Gemäß der Haushaltsverrechnung des Bundes stiegen die jährlichen IT-Auszahlungen des Außenministeriums zwischen 2017 und 2024 auf mehr als das Fünffache.

12.2 Der RH hielt fest, dass Daten zum Einsatz finanzieller Ressourcen im Außenministerium für dessen Aufgabenerfüllung vorlagen. Die Spionageprävention war keine explizite Aufgabe des Außenministeriums. Finanzielle Ressourcen im Zusammenhang mit Spionageprävention waren daher nicht gesondert ausgewiesen.

Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung finanzieller Ressourcen zur Spionageprävention einzubeziehen.

Der RH empfahl daher dem Außenministerium, die finanziellen Ressourcen zur Spionageprävention entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen.

12.3 Laut Stellungnahme des Außenministeriums werde es auch diese Empfehlung nach Maßgabe der budgetären Möglichkeiten umsetzen.

Spionageprävention im Internen Kontrollsystem

Kontrollbereiche der Spionageprävention

13 Das IKS ist ein in die Arbeits- und Betriebsabläufe einer Organisation eingebetteter Prozess, der von den Führungskräften sowie den Mitarbeiterinnen und Mitarbeitern durchgeführt wird, um bestehende Risiken zu erfassen und zu steuern und um mit ausreichender Gewähr sicherstellen zu können, dass die Organisation im Rahmen der Erfüllung ihrer Aufgaben ihre Ziele erreicht. Das IKS muss auf eine Minimierung dieser Risiken im laufenden Geschäftsprozess mittels angemessener organisatorischer und technischer Maßnahmen ausgerichtet sein.

Die Gebarungsüberprüfung umfasste – dem Antrag entsprechend – jene Teile des IKS der überprüften Bundesministerien, die zur Verhinderung von Spionage und zur Identifizierung von Spionagenetzwerken eingerichtet waren.

Ausgangspunkte der Gebarungsüberprüfung waren daher der Geheimschutz (Umgang mit Informationen, die einer besonderen Geheimhaltung unterliegen (TZ 15)) und die Kontrollsysteme zur Hintanhaltung definierter Risiken im Zusammenhang mit Spionage.

Risikoidentifikation und organisatorische Ausgestaltung des Internen Kontrollsystems

14.1 (1) Das Innen-, das Verteidigungs- und das Außenministerium identifizierten als Risiken im Zusammenhang mit Spionage den Geheimschutz (z.B. Informationsabfluss), Schutz von Rechtsgütern (z.B. Zutritt Unberechtigter) und den Schutz des eigenen Personals (z.B. vor Anwerbungsversuchen).

(a) Im Innenministerium oblag das Risikomanagement den einzelnen Organisationseinheiten. Die Direktorin bzw. der Direktor der DSN hatte aufgrund von § 2 Abs. 9 SNG ein System zur Qualitätssicherung für die Bewertung wahrscheinlicher Gefährdungen sowie der damit verbundenen Maßnahmen einzurichten. So erkannte die DSN u.a. Risiken in Bezug auf Spionage durch die nachrichtendienstliche Tätigkeit anderer Staaten und durch die Lieferkette von technischem Equipment sowie den Informationsabfluss durch Externe, Bedienstete und behördliche Maßnahmen.

(b) Risiken hinsichtlich Spionage bewerteten im Verteidigungsministerium das Abwehramt und das Heeres-Nachrichtenamt. Das Abwehramt beurteilte periodisch (quartalsmäßig) die möglichen Bedrohungen sowie die konkreten Gefährdungen auf ihre Eintrittswahrscheinlichkeiten. Das Heeres-Nachrichtenamt beurteilte Risiken anhand eines Gefahrenkatalogs. Als Risiken sah das Verteidigungsministerium beispielsweise die Weitergabe von Informationen, die Ausspähung militärischer Rechtsgüter, unbefugten Zutritt und Personen- und Sachschäden. Auch Anwerbung von Personal durch fremde Nachrichtendienste war ein Risiko.

(c) Das Risikomanagement des Außenministeriums führte als Risiken im Hinblick auf Spionage u.a. den Informationsabfluss (sowohl durch Dienstleister und andere Externe als auch durch Bedienstete des Ministeriums), Sabotage an Objekten und technischen Systemen sowie Lieferketten von technischem Equipment an.

(2) Das Innenministerium hatte keine zentralen Vorgaben an ein IKS für den Bereich der Spionageprävention.

Das BVT war bis 2018 in vier, danach in sechs Abteilungen ohne Trennung von Staatsschutz und Nachrichtendienst gegliedert. Die Direktorin bzw. der Direktor des BVT war gleichzeitig die bzw. der Informationssicherheitsbeauftragte des Innenministeriums. Nach dem 1. Oktober 2018 war das Referat „Interne Sicherheit“ bei der stellvertretenden Direktorin bzw. beim stellvertretenden Direktor des BVT angesiedelt. Daneben waren noch zwei Abteilungen mit Aufgaben im Geheimschutz betraut.

Die DSN war – wie auch schon das BVT – eine Teilorganisation der Generaldirektion für die öffentliche Sicherheit. Sie war nicht als Dienstbehörde erster Instanz und Personalstelle eingerichtet. Die Dienstrechtsangelegenheiten nahm daher der Innenminister wahr. Die DSN war organisatorisch in drei Teile gegliedert, den Bereich Direktion sowie die Aufgabenbereiche Staatsschutz und Nachrichtendienst. Ihr stand eine Direktorin bzw. ein Direktor vor, zwei stellvertretende Direktorinnen bzw. Direktoren leiteten jeweils einen Aufgabenbereich. Im Bereich Direktion war ein gemeinsames Informations- und Lagezentrum als Informationsschnittstelle zur Koordinierung des Staatsschutzes und Nachrichtendienstes eingerichtet. Aufgaben im IKS zum Geheimschutz waren in der Direktion im Rechtsbüro und im Büro „Interne Sicherheit“ angesiedelt. Die Leitung des Rechtsbüros war gleichzeitig die bzw. der Informationssicherheitsbeauftragte des Innenministeriums. Sie bzw. er nahm an Sitzungen der Informationssicherheitskommission teil und gestaltete Schulungsunterlagen sowie Leitlinien. Das Büro „Interne Sicherheit“ führte Kontrollen und Durchsuchungen sowie die Vertrauenswürdigkeitsprüfungen von Bediensteten der DSN operativ durch.

Zur Zeit der Gebarungsüberprüfung hatte der Direktor das Büro „Interne Sicherheit“ mittels Dienstanweisung ermächtigt, DSN-weite Anordnungen zu erteilen und Informationen über sicherheitsrelevante Umstände einzuholen. Zwischen dem Rechtsbüro, dem Büro „Interne Sicherheit“ und anderen den Geheimschutz umsetzenden Organisationseinheiten fand ein bedarfsorientierter, nicht regelmäßiger Austausch statt, z.B. bei gemeinsamen Projekten oder Informationssicherheitsvorfällen.

(3) Zentrale Vorgaben an die Ausgestaltung des IKS speziell für den Bereich Spionageprävention bestanden auch im Verteidigungsministerium nicht. Die Geschäftseinteilung des Verteidigungsministeriums wies die Angelegenheiten der militärischen Sicherheit und der bzw. des Sicherheits- und Informationssicherheitsbeauftragten der nachrichtendienstlichen Abwehr zu. Der Leiter des Abwehramtes nahm die Aufgaben des Sicherheits- und Informationssicherheitsbeauftragten wahr. Ebenso war er für die Angelegenheiten der nachrichtendienstlichen Abwehr ressortweit zuständig. Die Verantwortung für Regelungen des IKS zur Spionageprävention war bei der nachrichtendienstlichen Abwehr zentralisiert. Die Aufgaben umfassten den Schutz militärischer Rechtsgüter.

(4) Im Außenministerium bestand gemäß Geschäftseinteilung keine spezifische IKS-Zuständigkeit zur Spionageprävention. Die Umsetzung von IKS-Maßnahmen erfolgte in jeder Organisationseinheit. Es gab interne Vorgaben, Dokumente und Prozesse, die Teil des IKS waren und mehrere Abteilungen umfassten.

Die für Sicherheitsangelegenheiten zuständige Abteilung nahm Aufgaben der Spionageprävention wahr. In ihrem Zuständigkeitsbereich lagen Fragen der personellen und physischen Sicherheit sowie ressortweite Belange der Informationssicherheit

und der Umsetzung der Informationssicherheitspolitik einschließlich der Sicherheit im Bereich der IKT. Eine verpflichtende Einbindung der für Sicherheitsangelegenheiten zuständigen Abteilung in IKS-relevante Vorfälle im Außenministerium bestand nicht.

Ein eigens im Außenministerium eingerichtetes Informationssicherheitsmanagement-Team (ISM-T) koordinierte sämtliche Fragen auf dem Gebiet der Informationssicherheit; die Leitung oblag dem Büro des Generalsekretärs. Weiters gehörten ihm Vertreter des Generalinspektorats sowie der Abteilungen für Sicherheitsangelegenheiten und IKT an. Die Aufgaben umfassten die Festlegung von Richtlinien im Bereich der Informationssicherheitspolitik, die Festlegung von IKT-Sicherheitskonzepten im In- und Ausland sowie die Kontrolle der Umsetzung der beschlossenen Maßnahmen.

Das Außenministerium gab 2021 eine GAP-Analyse (Herausarbeitung der Lücke zwischen Soll- und Ist-Stand) in Auftrag, deren Ergebnis als Grundlage für den Aufbau eines Informationssicherheitsmanagementsystems (**ISMS**) dienen sollte. Seit 2023 arbeitete das Außenministerium unter der Leitung der für Sicherheitsangelegenheiten zuständigen Abteilung sowohl für den Bereich der Zentralstelle als auch für die Vertretungsbehörden an der Implementierung eines ISMS. Ziel war die Verstärkung der Mechanismen des Internen Kontrollsystems. Das Außenministerium ging von einem zweijährigen Umsetzungszeitraum aus. Durch das Projekt waren auch Anforderungen der NIS-2-Richtlinie[24] hinsichtlich Implementierung einer Governance sowie geeigneter Risikomanagementmaßnahmen adressiert. Dies erforderte die Definition von Prozessen und Rollen mit klaren Verantwortungs- und Berichtswegen.[25] Die Digitalisierung von Mitarbeiterrichtlinien war ebenso Bestandteil des Projekts wie den Bereich der Sicherheitsschulungen (auch in Bezug auf „Umgang mit klassifizierten Informationen“) mittels E-Learning-Modulen zu intensivieren und auszubauen.

14.2 (1) Der RH hielt fest, dass in den überprüften Bundesministerien der Bereich Spionageprävention kein eigener oder vom allgemeinen IKS getrennter Bestandteil war. Vielmehr war das IKS so ausgelegt, dass nicht explizit auf die Spionageprävention und -abwehr ausgelegte IKS-Elemente im Zusammenspiel auch das Spionagerisiko reduzieren.

[24] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie).

[25] Der RH verwies auf die Ergebnisse der im August 2025 von Bundesministerin Mag.ª Beate Meinl-Reisinger, MES eingesetzten unabhängigen, multidisziplinären Untersuchungskommission gemäß § 8 Bundesministeriengesetz unter dem Vorsitz von Bundesminister a.D. Mag. Thomas Starlinger. Der Bericht der Untersuchungskommission „Sicherheit und Prozesse“ vom Oktober 2025 führte in diesem Zusammenhang aus, dass es keinen „Chief Information Security Officer“ (CISO) als Stabsstelle und keine direkte, regelmäßige Berichtspflicht an den Generalsekretär gab.

(2) Der RH stellte fest, dass in der DSN – im Gegensatz zum BVT – die Aufgabenbereiche Staatsschutz und Nachrichtendienst organisatorisch getrennt waren und jeweils unter der Leitung einer stellvertretenden Direktorin bzw. eines stellvertretenden Direktors standen. Zum Informationsaustausch und zur Abstimmung dieser Arbeitsbereiche war das gemeinsame Informations- und Lagezentrum eingerichtet.

Weiters merkte der RH an, dass es in der DSN zwar ein bedarfsorientiertes, aber kein regelmäßiges Austauschformat zwischen Rechtsbüro, dem Büro „Interne Sicherheit" und anderen, den Geheimschutz umsetzenden Organisationseinheiten gab. Der RH hielt ein formelles regelmäßiges Austauschformat zwischen diesen Organisationseinheiten für zweckmäßig, um den Informations- und Erfahrungsaustausch zu gewährleisten und die Maßnahmen im IKS besser zu koordinieren.

Der RH empfahl der DSN, ein formelles regelmäßiges Austauschformat zwischen allen im Geheimschutz tätigen Organisationseinheiten in der DSN aufzubauen.

(3) Der RH hob die Bedeutung der Umsetzung eines ISMS und die damit einhergehende Stärkung von Governance und Risikomanagementmaßnahmen im Außenministerium hervor. In diesem Zusammenhang wies er – insbesondere aufgrund der Dislozierung der Vertretungsbehörden des Außenministeriums – auf das verbundene Potenzial zur Verbesserung des IKS sowie den damit einhergehenden Ausbau und die Intensivierung der Schulungsmaßnahmen.

Der RH empfahl dem Außenministerium, zur Stärkung des IKS die Implementierung des ISMS priorisiert abzuschließen und entsprechende Prozesse und Rollen unter Einbeziehung von Gesichtspunkten der Spionageprävention zu definieren.

Weiters empfahl er dem Außenministerium die Umsetzung ressortweiter standardisierter und verbindlicher Schulungs- und Awarenessmaßnahmen mit anschließender Wissensüberprüfung, in deren Fokus auch das Thema Spionageprävention steht.

Der RH hielt kritisch fest, dass im Außenministerium nicht vorgesehen war, die für Sicherheitsangelegenheiten zuständige Abteilung in die Aufarbeitung IKS-relevanter Vorfälle (z.B. Disziplinarverfahren) routinemäßig einzubinden.

Er empfahl dem Außenministerium, die für Sicherheitsangelegenheiten zuständige Abteilung über staatssicherheitsrelevante Vorfälle zu informieren.

14.3 (1) Laut Stellungnahme des Innenministeriums bestehe bereits ein bedarfsorientiertes Austauschformat zwischen den im Geheimschutz tätigen Organisationseinheiten in der Direktion Staatsschutz und Nachrichtendienst. Der Empfehlung des RH folgend werde dieses Austauschformat künftig formalisiert und regelmäßig abgehalten.

(2) Das Außenministerium führte in seiner Stellungnahme aus, dass die Standardprozesse für die Untersuchung von möglicherweise disziplinarrechtlich oder IKS-relevanten Vorwürfen und Hinweisen überarbeitet worden seien. Die Standardprozesse sähen nun die Einbindung der für Sicherheitsangelegenheiten zuständigen Abteilung bereits in der Phase der Erstevaluierung eines Sachverhalts vor.

Das Außenministerium habe sein ISMS mit Anfang 2026 in Betrieb genommen und sämtliche damit zusammenhängende Dokumente per Runderlass allen Bediensteten des Außenministeriums zur Kenntnis gebracht. Den Empfehlungen der Untersuchungskommission „Sicherheit und Prozesse" folgend strebe das Außenministerium eine Zertifizierung nach ISO 27001:2022 an.

Wesentliches Element des ISMS sei das Risikomanagement, wobei sich der Bogen von der Identifizierung und Analyse bis zur Behandlung oder Akzeptanz von Risiken spanne. Das ISMS unterstütze das Außenministerium bei der Risikoerkennung, -vermeidung, -verminderung oder -bewältigung (dies umfasse auch Spionageprävention) und schaffe strukturierte und aussagekräftige Entscheidungsgrundlagen für die Leitungsebene.

Im Rahmen des ISMS sei auch ein entsprechender Ausbau der Schulungsmaßnahmen vorgesehen (auch IT-gestützt und für Lokalbedienstete an den Vertretungsbehörden).

Das Außenministerium erarbeite derzeit auch neue standardisierte Schulungs- und Awarenessmaßnahmen mit anschließender Wissensprüfung zur Stärkung der bereits bisher durchgeführten Schulungen.

Geheimschutz – rechtliche Grundlagen

15.1 (1) Das Informationssicherheitsgesetz (**InfoSiG**)[26] und die Informationssicherheitsverordnung[27] regelten den Umgang mit Informationen, die einer besonderen Geheimhaltung unterliegen (klassifizierte Informationen) und die Österreich im Einklang mit völkerrechtlichen Regelungen erhält („internationaler Geheimschutz"). Der Umgang mit klassifizierten Informationen außerhalb des Anwendungsbereichs des InfoSiG („nationaler Geheimschutz") war in der Geheimschutzordnung des Bundes geregelt. Diese war ein – nicht öffentlich zugänglicher – Beschluss des Ministerrates vom Jänner 2008 und von den Bundesministerinnen und -ministern per Weisung für das jeweilige Bundesministerium in Kraft zu setzen. Als eine generelle interne Anordnung begründete sie im Außenverhältnis keine Rechte und Pflichten.

[26] BGBl. I 23/2002 i.d.g.F.

[27] BGBl. II 548/2003 i.d.g.F.

Das Innenministerium, das Verteidigungsministerium und das Außenministerium setzten die Geheimschutzordnung in ihren Wirkungsbereichen um.

(2) Der internationale und nationale Geheimschutz sahen u.a. in folgenden Bereichen unterschiedliche Regelungen vor:

- Schutzstandards klassifizierter Informationen: Die Informationssicherheitskommission hatte in einem Bericht 2020 auf die Risiken unterschiedlicher Regelungen hingewiesen. Der RH hatte in seinem Bericht „Management der IT-Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 6) unter Hinweis auf diese Unterschiede empfohlen, eine Regierungsvorlage zu erarbeiten, die ein einheitliches Regelungssystem zur elektronischen Verarbeitung klassifizierter Informationen für den internationalen und nationalen Geheimschutz schafft. In seinem Bericht „Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium“ (Reihe Bund 2024/16, TZ 8) hatte der RH festgestellt, dass im Juni 2023 eine entsprechende Regierungsvorlage oder ein Gesetzesbeschluss nicht vorlag, und empfohlen, die Vorbereitung der Regierungsvorlage für ein novelliertes InfoSiG in der Informationssicherheitskommission sowie im Abstimmungsprozess mit den Bundesministerien zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen.
- Sanktionierung von Verstößen: Das InfoSiG definierte für den internationalen Bereich Tatbestände für Verwaltungsübertretungen und gerichtlich strafbare Handlungen; bei Verstößen sah es Sanktionen vor, sofern die Taten nicht nach anderen Bundesgesetzen mit strengerer Strafe bedroht waren. Solche Regelungen konnte der nationale Geheimschutz wegen der rechtlichen Qualität der Geheimschutzordnung nicht enthalten.
- Koordinierungs- und Beratungsaufgaben sowie Berichtspflichten: Nach dem InfoSiG war in jedem Bundesministerium eine Informationssicherheitsbeauftragte bzw. ein Informationssicherheitsbeauftragter zu bestellen. Ihr bzw. ihm oblagen u.a. die Überwachung der Einhaltung des internationalen Geheimschutzes und die Überprüfung der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen im Ministerium. Überdies war die Informationssicherheitskommission – unter dem Vorsitz der bzw. des Informationssicherheitsbeauftragten des Bundeskanzleramts – einzurichten, der die Informationssicherheitsbeauftragten aller Bundesministerien angehörten. Ihre Aufgabe war u.a., auf die „bundesweite Einheitlichkeit von Schutzmaßnahmen und deren Koordination im Bereich der Bundesverwaltung hinzuwirken“ und regelmäßig an die Bundesregierung zu berichten sowie Vorschläge zur Verbesserung der Informationssicherheit zu erstatten (§ 8 Abs. 1 InfoSiG). Die Geheimschutzordnung enthielt keine allgemeinen Koordinierungs- und Beratungsaufgaben sowie Berichtspflichten der Informationssicherheitskommission; zu den Informationssicherheitsbeauftragten enthielt sie keine Ausführungen.

(3) Im Jahr 2024 arbeitete das Bundeskanzleramt an einem Entwurf für das „InfoSiG neu“, mit dem Ziel, die Behandlung nationaler und internationaler klassifizierter Informationen gleichzustellen und in einem Gesetz zu regeln.

15.2 Der RH hielt fest, dass die in seinem Bericht „Management der IT-Sicherheit in der Verwaltung ausgewählter Bundesministerien“ (Reihe Bund 2021/31, TZ 6) aufgezeigten Unterschiede in den rechtlichen Grundlagen für die elektronische Verarbeitung klassifizierter Informationen weiterhin bestanden und damit auch das aus den Unterschieden resultierende, von der Informationssicherheitskommission identifizierte Sicherheitsrisiko.

Darüber hinaus stellte der RH Unterschiede bei der Sanktionierung von Verstößen im internationalen und nationalen Geheimschutz fest. Während das InfoSiG sowohl verwaltungsstrafrechtliche als auch strafrechtliche Tatbestände enthielt, konnte die Geheimschutzordnung solche aufgrund ihrer reinen Innenwirkung nicht enthalten. Weiters hatte die nach dem InfoSiG eingerichtete Informationssicherheitskommission im internationalen Geheimschutz nicht die gleichen Koordinierungs- und Beratungsaufgaben sowie Berichtspflichten wie im nationalen Geheimschutz. Die Informationssicherheitsbeauftragten waren mit den ihnen im nationalen Geheimschutz übertragenen Aufgaben in der Geheimschutzordnung nicht vorgesehen. Der RH hielt eine Harmonisierung auch in diesen Bereichen für wichtig, um den Schutzstandard im Geheimschutz durch einheitliche Sanktionen und einheitliche Aufgabenbesorgung sicherzustellen.

Der RH empfahl dem Innen-, dem Verteidigungs- und dem Außenministerium, die Vorbereitung der Regierungsvorlage für das „InfoSiG neu“ in der Informationssicherheitskommission sowie im Abstimmungsprozess mit sämtlichen Bundesministerien zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen.

15.3 (1) Laut Stellungnahme des Innenministeriums befinde sich die Empfehlung in der Umsetzungsphase, indem unter Federführung des Bundeskanzleramts ein Entwurf für eine Novelle des InfoSiG unter Einbindung des Innenministeriums ausgearbeitet werde; der Entwurf befinde sich in der politischen Abstimmung. Gemäß dem Entwurf sollten u.a. die Rechtsgrundlagen für klassifizierte Informationen harmonisiert werden.

(2) Das Verteidigungsministerium teilte in seiner Stellungnahme mit, dass die Empfehlung des RH sachgerecht erscheine und ein Entwurf für eine Novelle des InfoSiG einen harmonisierten Umgang mit international klassifizierten und national klassifizierten Informationen vorsehe.

(3) Das Außenministerium hielt in seiner Stellungnahme fest, dass die für Sicherheitsangelegenheiten zuständige Abteilung im laufenden Austausch mit dem Bundeskanzleramt stehe und die Empfehlung in Umsetzung sei.

Interne Kontrollsysteme zum Geheimschutz

Klassifizierte Informationen

16.1 (1) Klassifizierte Informationen sind materielle und immaterielle Informationen, unabhängig von Darstellungsform und Datenträger, die aufgrund ihres Inhalts einer besonderen Geheimhaltung bedürfen. Sie waren daher nur für einen begrenzten Personenkreis zugänglich und besonders gegen Kenntnisnahme und Zugriff durch Unbefugte geschützt. Internationaler und nationaler Geheimschutz sahen ein nach den Auswirkungen eines Missbrauchs der Information abgestuftes Klassifizierungssystem (Klassifizierungsstufen) vor:

Tabelle 1: Voraussetzungen für die Zuordnung zu den Klassifizierungsstufen im internationalen und nationalen Geheimschutz

Klassifizierungsstufen	internationaler Geheimschutz § 2 Abs. 2 InfoSiG, § 3 Abs. 1 InfoSiV	nationaler Geheimschutz § 3 Abs. 2 GehSO
eine Information ist **EINGESCHRÄNKT**,[1]	wenn die unbefugte Weitergabe der Informationen den Geheimschutzinteressen[2] zuwiderlaufen würde	wenn die unbefugte Weitergabe der Informationen den Geheimschutzinteressen[2] zuwiderlaufen würde und die Informationen eines über die bloße Amtsverschwiegenheit hinausgehenden Schutzes bedürfen
eine Information ist **VERTRAULICH**,[1]	wenn die Informationen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist	wenn die Informationen eingeschränkt sind und die Preisgabe der Informationen die Gefahr einer Schädigung der Geheimschutzinteressen[2] schaffen würde
eine Information ist **GEHEIM**,	wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der Geheimschutzinteressen[2] schaffen würde	wenn die Informationen vertraulich sind und ihre Preisgabe die Gefahr einer erheblichen Schädigung der Geheimschutzinteressen[2] schaffen würde
eine Information ist **STRENG GEHEIM**,	wenn die Informationen geheim sind und überdies ihr Bekanntwerden eine schwere Schädigung der Geheimschutzinteressen[2] wahrscheinlich machen würde	wenn die Informationen geheim sind und überdies ihr Bekanntwerden eine schwere Schädigung der Geheimschutzinteressen[2] wahrscheinlich machen würde

InfoSiG = Informationssicherheitsgesetz
InfoSiV = Informationssicherheitsverordnung
GehSO = Geheimschutzordnung des Bundes

Quellen: InfoSiG; InfoSiV; GehSO; Zusammenstellung: RH

[1] Die Unterschiede in den Klassifizierungsstufen „EINGESCHRÄNKT“ und „VERTRAULICH“ blieben aufgrund der Herkunft der Information ohne Folgen. Im internationalen Geheimschutz übermittelte eine Partnerorganisation die bereits klassifizierten Informationen und der Empfänger übernahm diese. Für die Erstellung von klassifizierten Informationen war ausschließlich der nationale Geheimschutz von Bedeutung.

[2] Als Geheimschutzinteressen werden die im vormaligen Art. 20 Abs. 3 Bundes-Verfassungsgesetz i.d.F. BGBl. I 141/2022 genannten Interessen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung oder der auswärtigen Beziehungen, der wirtschaftlichen Interessen einer Körperschaft des öffentlichen Rechts, der Vorbereitung einer Entscheidung oder der überwiegenden Interessen der Parteien bezeichnet. Das InfoSiG und die InfoSiV verwiesen bis Ende August 2025 auf Art. 20 Abs. 3 Bundes-Verfassungsgesetz i.d.F. BGBl. I 141/2022, während die Geheimschutzordnung die Interessen tatbestandsmäßig explizit anführt.

Bedienstete, die eine klassifizierte Information erstellten, mussten sie anhand der in der Tabelle angeführten Voraussetzungen gemäß § 3 Abs. 2 Geheimschutzordnung den Klassifizierungsstufen zuordnen. Eine konkretere Definition dieser Voraussetzungen gab es in der Geheimschutzordnung nicht. Die Informationssicherheitskommission arbeitete im Rahmen der Novelle des InfoSiG (TZ 15) an einer Klassifizierungsrichtlinie, die eine Hilfestellung für Bedienstete bieten, Einheitlichkeit erzielen und Über- oder Unterklassifizierung vermeiden soll.

(2) Das Innenministerium setzte Regelungen zum Geheimschutz um. Zusätzlich zu den Klassifizierungsstufen verwendete es die Kennzeichnungen „VERSCHLUSS“ und „VERSCHLUSS SENSIBEL“. Sie sollten die Vertraulichkeit einer Information unterhalb der Klassifizierungsstufen verdeutlichen. Eine Definition und Voraussetzungen, wann eine Information mit diesen Kennzeichnungen versehen werden sollte, waren in der „Richtlinie zur Anwendung der Geheimschutzordnung des Bundes“ nicht festgelegt.

(3) Das Verteidigungsministerium setzte Regelungen zum Geheimschutz um. Die Leiter des Heeres-Nachrichtenamtes und des Abwehramtes legten für ihren Wirkungsbereich den Verkehr mit klassifizierten Informationen nach den besonderen Erfordernissen des militärischen Nachrichtendienstes fest.

(4) Das Außenministerium setzte Regelungen zum Geheimschutz mittels Dienstzettel bzw. Runderlass an alle österreichischen Berufsvertretungsbehörden[28] vom Mai 2012 um. Zeitgleich aktualisierte das Außenministerium den entsprechenden Paragrafen im Handbuch für den Auswärtigen Dienst, der die Klassifizierung von internen Schriftstücken regelte.

16.2 Der RH hielt fest, dass die Vorschriften zur Klassifizierung in der Geheimschutzordnung einen erheblichen Interpretationsspielraum offenließen. Daher erachtete er die Bestrebungen der Informationssicherheitskommission für zweckmäßig, eine Klassifizierungsrichtlinie als Hilfestellung für Bedienstete zu erstellen.

Der RH hielt kritisch fest, dass das Innenministerium die eigenen Kennzeichnungen in der Richtlinie zur Anwendung der Geheimschutzordnung weder definierte noch Voraussetzungen festlegte.

Der RH empfahl dem Innen-, dem Verteidigungs- und dem Außenministerium, die Arbeiten in der Informationssicherheitskommission an einer Klassifizierungsrichtlinie voranzutreiben, die die Bediensteten bei der Klassifizierung von Informationen unterstützen und die Einheitlichkeit fördern soll.

[28] Botschaften und Honorarkonsulate

16.3 (1) Das Innenministerium führte in seiner Stellungnahme aus, dass die Empfehlung des RH sehr zu begrüßen sei. Im Entwurf zur Novelle des InfoSiG sei auch vorgesehen, in weiterer Folge Vorgaben zur Erstellung von Klassifizierungsrichtlinien in der Informationssicherheitsverordnung zu regeln.

(2) Das Verteidigungsministerium teilte in seiner Stellungnahme im Zusammenhang mit dem Entwurf zur Novelle des InfoSiG mit, dass eine Zuordnung von schutzwürdigen Informationen zu einer bestimmten Klassifizierungsstufe aufgrund klarerer Zuordnungskriterien im Vergleich zur geltenden Rechtslage wohl leichter möglich sei. Ein gewisser Interpretationsspielraum sei aber weiterhin verblieben.

(3) Laut Stellungnahme des Außenministeriums stehe die für Sicherheitsangelegenheiten zuständige Abteilung im laufenden Austausch mit dem Bundeskanzleramt; die Empfehlung sei in Umsetzung.

Aufbewahrung, Bearbeitung und Kommunikation

17.1 (1) Das InfoSiG gemeinsam mit der Informationssicherheitsverordnung und die Geheimschutzordnung legten Mindeststandards für den Schutz von klassifizierten Informationen fest. Diese waren von den betroffenen Organisationseinheiten durch Maßnahmen zu konkretisieren. Die Anforderungen an Kennzeichnung, Verarbeitung, Kommunikation, Vervielfältigung und Vernichtung von klassifizierten Informationen stiegen mit der Klassifizierungsstufe.

(2) Die DSN gab gegenüber dem RH an, im Rahmen der Konkretisierung der Mindeststandards bei Unterschieden zwischen internationalem und nationalem Geheimschutz den höheren Standard anzuwenden. Das war auch in einzelnen internen Dienstanweisungen abgebildet.

Eine interne Dienstanweisung der DSN regelte die Erstellung von Informationen für die Ressortleitung und die Generaldirektion für die öffentliche Sicherheit und legte entsprechende Prozesse fest. Die Informationen durften für die Ressortleitung keine klassifizierten Dokumente und für die Generaldirektion für die öffentliche Sicherheit nur solche bis zur Klassifizierungsstufe „EINGESCHRÄNKT“ enthalten. In beiden Fällen gab die Direktorin bzw. der Direktor der DSN die Informationsweitergabe frei.

Im Innenministerium bestanden schriftliche Vorgaben zur Vergabe bzw. Handhabung von Zugriffsrechten, die entweder für das Innenministerium gesamt, für einzelne Abteilungen oder spezifisch für die DSN galten. Die DSN regelte außerdem für die eigenen Anwendungen und Laufwerke die Grundlagen und Prozesse zur Vergabe und zum Entzug von Zugriffsberechtigungen für unterschiedliche dienstliche Szenarien (z.B. Eintritt, Austritt, Dienstzuteilung). So waren z.B. auch bei tempo-

rären Unterbrechungen (z.B. Krankenstand, Karenzierung) die Berechtigungen zu entziehen bzw. zu deaktivieren, ebenso bei Suspendierung.

Benutzerrechte waren nach dem Need-to-know-Prinzip zu vergeben. Bei der Beantragung und Vergabe der Zugriffsrechte für Bedienstete der DSN waren das Vier-Augen-Prinzip einzuhalten und gegebenenfalls weitere IKS-Maßnahmen vorgesehen (zusätzliche Faktoren, Einbindung weiterer Stellen, kein Kopieren und Übernehmen von Zugriffsrechten). Verantwortlichkeiten für die Kontrolle der Zugriffsrechte und um deren Aktualität sicherzustellen, waren festgelegt. Die Führungskraft war verantwortlich, dass Rechte aktuell waren, und konnte zur Überprüfung Übersichtslisten anfordern.

Die Zugriffe der Bediensteten auf die Systeme der DSN wurden elektronisch protokolliert; die in der DSN dafür zuständigen Stellen kontrollierten die Zugriffe aller Bediensteten gemäß Dienstanweisung vom Juni 2024.

Neben der technischen Beschränkung der Zugriffsmöglichkeiten sahen das Innenministerium und die DSN auch Sensibilisierungsgespräche zum sicheren Umgang mit den IT-Systemen sowie Melderoutinen bei Gefährdung für die Integrität der IT-Infrastruktur vor. Dokumente ab der Klassifizierungsstufe „VERTRAULICH“ durften nur auf Geräten ohne externe Vernetzung verarbeitet werden. Führungskräfte waren für die Einhaltung der IT-Sicherheitsrichtlinien verantwortlich. Zur Absicherung des IT-Sicherheitsniveaus im Innenministerium legte dieses darüber hinaus im Rahmen einer „Sicherheitsorganisationsstruktur“ für ausgewählte Bedienstete spezifische Verantwortlichkeiten fest, z.B. als IT-Sicherheitsbeauftragte oder IT-Sicherheitsvertrauenspersonen. Es bestanden außerdem Regelungen zur Verwendung von wechselbaren Datenträgern (z.B. USB-Sticks) allgemein und zur Beschränkungen von Transfer, Transport und Verarbeitung klassifizierter Daten auf Datenträgern im Speziellen.

(3) Auch das Verteidigungsministerium gab an, im Rahmen der Konkretisierung der Mindeststandards bei Unterschieden zwischen internationalem und nationalem Geheimschutz den höheren Standard anzuwenden.

Im Verteidigungsministerium bestanden schriftliche Vorgaben zur Vergabe bzw. Handhabung von Zugriffsrechten, die entweder für das Verteidigungsministerium gesamt, für einzelne Abteilungen oder spezifisch für das Abwehramt galten.

Die Büroordnung des Abwehramtes regelte den Umgang mit elektronischen Akten und Papierakten. Die Verwaltung von Akten und die Speicherung von nachrichtendienstlichen (operativen) Daten waren voneinander getrennt und erfolgten in unterschiedlichen Systemen. Die Vergabe von Rechten dafür hatte durch den Leiter des Abwehramtes (mit eingeschränkter Delegationsmöglichkeit) nach dem Need-to-

know-Prinzip zu erfolgen. Im System wurden die Zugriffe auf einzelne Datensätze technisch protokolliert.

Im Netzwerk des Abwehramtes war eine Verarbeitung von klassifizierten Informationen bis zur Stufe „GEHEIM“ möglich. Das Abwehramt verfügte über einen vom Verteidigungsministerium getrennten ELAK.

Im Abwehramt standen technische Lösungen für die Sprachkommunikation über klassifizierte Informationen zur Verfügung. Beispielsweise konnten Informationen der Stufe „EINGESCHRÄNKT“ über eine zugelassene Lösung mit Mobiltelefonen besprochen werden.

Eine eigene Regelung bestand für die Vorlage von Geschäftsstücken an die Ressortleitung, das Kabinett und das Generalsekretariat. Die Vorlage erfolgte grundsätzlich im Wege der Generalstabsabteilung oder unter gleichzeitiger Information des Chefs des Generalstabes.

(4) Im Außenministerium gab es Vorgaben und Dienstanweisungen, um eine sichere Kommunikation im Zusammenhang mit Informationen zu eingeschränkten Inhalten (inklusive Klassifizierungsstufe „EINGESCHRÄNKT“) gewährleisten zu können. Das Außenministerium verfügte über technische Möglichkeiten, um auch telefonisch über Informationen zu eingeschränkten Inhalten kommunizieren zu können.

17.2 (1) Der RH hielt fest, dass im Innen-, im Verteidigungs- und im Außenministerium Vorschriften zur Aufbewahrung, Bearbeitung und Kommunikation von klassifizierten Informationen vorhanden waren.

(2) Der RH verwies auf seine Feststellungen und seine Empfehlung in TZ 15, die Vorbereitung der Regierungsvorlage für das „InfoSiG neu“ zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen.

(3) Im Zusammenhang mit der Errichtung der DSN hielt der RH fest,

- dass das Innenministerium und die DSN für die IT-Nutzung und bei der Vergabe und Handhabung von Zugriffsrechten IKS-Standards berücksichtigten,
- dass die Zugriffe der Bediensteten auf die Systeme der DSN protokolliert sowie regelmäßig kontrolliert wurden,
- dass das Innenministerium und die DSN neben technischen Maßnahmen auch persönlich an die Bediensteten gerichtete Maßnahmen vorsahen, wie Sensibilisierungsgespräche, Regeln zur Nutzung von Datenträgern und Melderoutinen bei Gefährdungen.

(4) Der RH hob hervor, dass es für die Weitergabe von Informationen im Weisungsweg an die Ressortleitungen für die DSN und das Abwehramt gesonderte Vorschriften gab. Die Freigabe der Informationsweitergabe erfolgte in der DSN durch die Direktorin bzw. den Direktor. Die Weitergabe von Informationen aus dem Abwehramt hatte im Verteidigungsministerium im Wege der Generalstabsabteilung zu erfolgen. Der RH hielt fest, dass in beiden Fällen das Vier-Augen-Prinzip zur Anwendung kam.

Laufende Überprüfungen und Kontrollen

18.1 (1) Der internationale und der nationale Geheimschutz[29] sahen übereinstimmend nachweisliche jährliche Überprüfungen der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen vor. Dabei waren insbesondere die Vollständigkeit der Aufzeichnungen, die Sicherheit der Behältnisse, das Schlüsselsystem und die Sicherungsmaßnahmen von Kommunikations- und Informationssystemen zu kontrollieren.

(2) Das Büro „Interne Sicherheit“ der DSN führte diese jährlichen Überprüfungen durch und kontrollierte auch nach Zufallsprinzip und stichprobenartig die Einhaltung der Geheimschutzvorgaben. Die Anzahl dieser Überprüfungen, deren Ergebnisse und allfällige daraus resultierende Maßnahmen berichtete das Büro der Direktorin bzw. dem Direktor der DSN.

(3) Im Verteidigungsministerium war der Zugang zu klassifizierten Informationen der Klassifizierungsstufen „VERTRAULICH“, „GEHEIM“, „STRENG GEHEIM“ zu dokumentieren. Bei Zugang zu klassifizierten elektronischen Informationen war sicherzustellen, dass alle Zugriffe unveränderbar dokumentiert wurden.

Das Geheimschutzpersonal im Verteidigungsministerium musste über eine gültige Prüfbescheinigung (Verlässlichkeitsprüfung) verfügen. Zum Geheimschutzpersonal zählten die bzw. der Informationssicherheitsbeauftragte, die Geheimschutzbeauftragten und die Sicherheitsbeauftragten, jeweils mit ihren Stellvertretungen. Das System des Geheimschutzes war durch die Sicherheitsbeauftragten jährlich zu überprüfen („GEHEIM“ und „STRENG GEHEIM“ vollständig, „VERTRAULICH“ stichprobenartig). Das Überprüfungsergebnis legten die Sicherheitsbeauftragten dem Abwehramt im Dienstweg vor.

Gesonderte Regelungen bestanden für die Einteilung und Aufgabenerfüllung für Organe der militärischen Sicherheit.

[29] Informationssicherheitsgesetz und Geheimschutzordnung

(4) Im Außenministerium überprüfte die Interne Revision (Generalinspektorat) regelmäßig die Vertretungen im Ausland sowie alle Organisationseinheiten im Ressort, auch hinsichtlich der Einhaltung der Sicherheitsvorgaben. Im Zuge dieser Revisionen prüfte sie die Sicherheit von Amt und Residenz, Zutrittsregelungen (Schlüsselvormerk) – insbesondere auch in Bezug auf den Serverraum –, Zugriffsberechtigungen, Sicherheitsvorkehrungen der Vertretung, Sicherheitsbehältnisse sowie die Einhaltung der Compliance-Vorschriften.

Weitere regelmäßige Vor-Ort-Kontrollen der Register des Außenministeriums (EU, MTCR[30], OPCW[31]), der Österreichischen Vertretung in Brüssel und der Österreichischen Vertretung NATO in Brüssel (im Sinne der Einhaltung des Systems der Informationssicherheit gemäß § 17 Informationssicherheitsverordnung) erfolgten durch die Informationssicherheitsbeauftragte bzw. den Informationssicherheitsbeauftragten des Außenministeriums.

18.2 Der RH hielt fest, dass im Innen-, im Verteidigungs- und im Außenministerium Vorschriften für die jährlichen Überprüfungen der Sicherheitsvorkehrungen zum Schutz von klassifizierten Informationen vorhanden waren.

Überprüfung von Personen

Allgemeines

19 In den überprüften Bundesministerien waren personenbezogene Überprüfungen eine Aufnahmevoraussetzung und Voraussetzung für den Zugang zu Informationen. Die Ministerien konnten diese Überprüfungen je nach Erfordernis des Geheimschutzes für den Zugang zu Informationen abgestuft für den jeweiligen Einsatzbereich anwenden. Abhängig von der Verwendung der Bediensteten waren die personenbezogenen Überprüfungen in regelmäßigen Abständen (drei, fünf oder zehn Jahre) zu erneuern.

Im Innenministerium und in der DSN kamen Vertrauenswürdigkeitsprüfungen und Sicherheitsüberprüfungen (TZ 20) zur Anwendung. Sicherheitsüberprüfungen veranlasste auch das Außenministerium für sein Personal. Gesonderte Regelungen für eine Verlässlichkeitsprüfung (TZ 21) bestanden im Verteidigungsministerium.

[30] Missile Technology Control Regime

[31] Organization for the Prohibition of Chemical Weapons (Organisation für das Verbot von Chemiewaffen)

Vertrauenswürdigkeitsprüfung und Sicherheitsüberprüfung

20.1 (1) Die Vertrauenswürdigkeitsprüfung war in § 2a SNG geregelt. Der Gesetzgeber hatte sie im Rahmen der Neugestaltung des Verfassungsschutzes eingeführt, weil sich die bestehende Sicherheitsüberprüfung laut Gesetzesmaterialien als unzureichend erwiesen hatte, um den Schutz klassifizierter Informationen zu gewährleisten. Die Anpassung an internationale Standards trug der sensiblen Tätigkeit der Bediensteten des Verfassungsschutzes Rechnung. Die Sicherheitsüberprüfung bestand weiterhin unverändert fort und war in §§ 55 ff. Sicherheitspolizeigesetz geregelt. Diese Personenüberprüfungen oblagen der DSN (§ 4 Z 3 SNG), intern waren die Zuständigkeiten dafür organisatorisch getrennt.

(2) (a) Die Vertrauenswürdigkeitsprüfung diente der Abklärung der Vertrauenswürdigkeit einer Person anhand personenbezogener Daten, die Aufschluss über allfällige Anhaltspunkte dafür gaben, ob von dieser Person ein Risiko für den Verfassungsschutz ausging. Die Prüfung bestand aus den Angaben in der Vertrauenswürdigkeitserklärung und der Überprüfung der darin enthaltenen Informationen einschließlich einer mündlichen Erörterung mit der überprüften Person. Darüber hinaus waren volljährige Personen, die mit der überprüften Person im gemeinsamen Haushalt lebten, einer Sicherheitsüberprüfung zu unterziehen.

(b) Die Themen der Vertrauenswürdigkeitsprüfung legte die Vertrauenswürdigkeitsprüfungs-Verordnung[32] fest: Angaben zur Person (Name, Wohnsitz, Familienstand etc.), Vermögensverhältnisse und finanzielle Verbindlichkeiten, öffentlich sichtbare Nutzung von Online-Diensten[33], Kontakte zu Nachrichten- und Geheimdiensten, Aufenthalte in oder Beziehungen zu fremden Staaten, sofern das für das Gebiet des Staatsschutzes relevant war. Die Angaben der Vertrauenswürdigkeitserklärung überprüfte die DSN mit Registerabfragen und Open Source Intelligence (**OSINT**)[34], sie holte Auskünfte von Behörden und anderen Dienststellen und Körperschaften ein und befragte Referenzpersonen, die die überprüfte Person anzugeben hatte. Das abschließende mündliche Gespräch mit der überprüften Person bot die Möglichkeit, etwaige Widersprüche zwischen den Angaben der Vertrauenswürdigkeitserklärung und den Überprüfungen aufzuklären oder allfällige Anhaltspunkte für ein Risiko für den Verfassungsschutz auszuräumen.

32 BGBl. II 402/2020 i.d.g.F.

33 Das betraf insbesondere Social-Media-Plattformen, Internet-Foren oder eigene Websites.

34 Open Source Intelligence (OSINT) befasst sich mit der Gewinnung von Informationen, die über offene Quellen frei verfügbar im Internet zu finden sind. Diese Daten werden für weitere Ermittlungen und Analysen herangezogen, um gezielte Erkenntnisse daraus herzuleiten (siehe dazu Bundesministerium für Inneres, Cybercrime Report 2023, Lagebericht über die Entwicklung von Cybercrime, S. 75).

(c) Das Ergebnis der Vertrauenswürdigkeitsprüfung war eine Prognose aufgrund bestimmter Tatsachen und ihrer Wertung und konnte entweder „positiv“ (vertrauenswürdig) oder „negativ“ (nicht vertrauenswürdig) sein. Bedienstete galten jedenfalls als nicht vertrauenswürdig, wenn sie nicht oder unzureichend an der Vertrauenswürdigkeitsprüfung mitwirkten und so eine Feststellung des maßgeblichen Sachverhalts nicht möglich war oder sie diese verweigerten (§ 2a Abs. 2 SNG). Anders als das Militärbefugnisgesetz (für die Verlässlichkeitsprüfung) enthielt das SNG keine weiteren Gründe für eine „negative“ Vertrauenswürdigkeitsprüfung oder Kriterien für Anhaltspunkte, ob von dieser Person ein Risiko für den Verfassungsschutz ausging.

(d) Vor Beginn der Tätigkeit in der DSN mussten sich künftige Bedienstete gemäß § 2a Abs. 1 SNG einer Vertrauenswürdigkeitsprüfung für den Verfassungsschutz unterziehen. Danach hatten Bedienstete der DSN alle drei Jahre abwechselnd eine Sicherheitsüberprüfung für den Zugang zu streng geheimer Information und eine Vertrauenswürdigkeitsprüfung zu wiederholen. Die Einhaltung dieser Intervalle stellte die DSN durch ein internes Monitoringsystem sicher. Die Vertrauenswürdigkeitsprüfung war unverzüglich zu wiederholen, wenn Anhaltspunkte vorlagen, wonach eine Bedienstete oder ein Bediensteter nicht mehr vertrauenswürdig sein könnte. Zusätzlich verankerte die DSN intern Meldepflichten für Umstände, die geeignet waren, die Vertrauenswürdigkeit infrage zu stellen.

Weiters war eine Vertrauenswürdigkeitsprüfung eine gesetzlich vorgesehene Voraussetzung für

- Bedienstete der für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen,
- Mitglieder und Bedienstete der Kontrollkommission sowie
- sonstige Bedienstete des Innenministeriums, die mit dem Aufbau oder Betrieb der technischen Infrastruktur der DSN betraut waren.

(e) Der Rechtsschutzbeauftragte und seine Stellvertretungen (bis 30. September 2025)[35] sowie Verwaltungsbedienstete, die im Rahmen ihrer Kontrollbefugnisse umfangreiche Einblicke in operative Angelegenheiten der DSN erhielten, waren nicht verpflichtet, sich einer Vertrauenswürdigkeitsprüfung zu unterziehen. Das traf auch auf andere Verwaltungsbedienstete im Innenministerium zu, die – mit Kenntnissen über Aufbau oder Betrieb der technischen Infrastruktur vergleichbare – sensible Informationen zur DSN hatten, wie z.B. die für die DSN zuständigen Verwaltungsbediensteten der Dienstbehörde oder Personalstelle.

[35] Mit der Änderung des § 91b Sicherheitspolizeigesetz (BGBl. I 2025/54 vom 29. September 2025) hatten sich auch der Rechtsschutzbeauftragte und seine Stellvertretung vor Beginn der Tätigkeit einer Vertrauenswürdigkeitsprüfung (§ 2a SNG) zu unterziehen.

(3) (a) Die Sicherheitsüberprüfung diente der Abklärung der Vertrauenswürdigkeit einer Person anhand personenbezogener Daten, die Aufschluss über allfällige Anhaltspunkte dafür geben, ob die Person gefährliche Angriffe begehen werde. Nähere Regelungen dazu, wann solche Anhaltspunkte vorlagen, enthielt das Sicherheitspolizeigesetz nicht.

(b) Die Sicherheitsüberprüfung war nach den Regelungen des Geheimschutzes Voraussetzung für den Zugang zu klassifizierten Informationen ab der Stufe „VERTRAULICH“ (§ 3 Abs. 1 Z 1 lit. c InfoSiG und § 6 Abs. 1 Z 3 Geheimschutzordnung). Korrespondierend dazu sah das Sicherheitspolizeigesetz die Möglichkeit einer Sicherheitsüberprüfung zur Sicherung der Geheimhaltung vertraulicher Information und eine Verpflichtung bei Zugang zu klassifizierten Informationen ab der Stufe „VERTRAULICH“ vor.

Für den Zugang zu Informationen der Stufe „STRENG GEHEIM“ waren auch Bezugspersonen zu überprüfen. Das waren volljährige Personen, die mit der oder dem Bediensteten in einem gemeinsamen Haushalt lebten.

Lagen die Voraussetzungen für eine Sicherheitsüberprüfung vor, konnte sie alle drei Jahre wiederholt werden. Auch war es möglich, bei Zustimmung der bzw. des Betroffenen oder wenn Anhaltspunkte vorlagen, dass eine Person nicht mehr vertrauenswürdig war, diese anlassfallbezogen durchzuführen.

(c) Basis einer Sicherheitsüberprüfung war die Sicherheitserklärung. Ihr Umfang war in der Sicherheitserklärungs-Verordnung[36] geregelt; er richtete sich nach der Klassifizierungsstufe der Information, die geschützt oder zu der Zugang erlangt werden sollte. Die Sicherheitserklärung für die Stufe „STRENG GEHEIM“ umfasste etwa Angaben zur Person, zu straf- und verwaltungsstrafrechtlichen Verfahren, zu Beziehungen zu extremistischen oder gewaltbereiten Gruppen oder Organisationen und Nachrichtendiensten (Geheimdiensten) sowie zur finanziellen und gesundheitlichen Situation.

Die Anhänge zur Sicherheitserklärungs-Verordnung enthielten vier Musterformulare für die Sicherheitserklärung. Auf Grundlage der ausgefüllten und unterschriebenen, analogen Sicherheitserklärung führte die DSN die Sicherheitsüberprüfung durch. Wie bei der Vertrauenswürdigkeitsprüfung überprüfte die DSN die Angaben der Sicherheitserklärung. Dabei war sie auf die darin enthaltenen Informationen beschränkt und durfte keine Recherche mit OSINT über die öffentlich sichtbare Nutzung von Online-Diensten durchführen.

[36] BGBl. II 114/2000 i.d.g.F.

Der oder dem Bediensteten war abschließend die Gelegenheit zu geben, sich zu den Feststellungen der Sicherheitsüberprüfung zu äußern.

(d) Das Ergebnis der Sicherheitsüberprüfung enthielt Feststellungen darüber, ob Anhaltspunkte vorlagen, dass die Person gefährliche Angriffe begehen könnte. Eine Beurteilung in den Kategorien „positiv" oder „negativ" – wie bei der Vertrauenswürdigkeitsprüfung – war nicht vorgesehen. Die Feststellungen der Sicherheitsüberprüfung der DSN entfalteten keine bindende Wirkung für die anfordernde Stelle. Ergab eine Sicherheitsüberprüfung bei Bediensteten der DSN Anhaltspunkte, dass die bzw. der Bedienstete gefährliche Angriffe (z.B. Spionageaktivitäten) begehen könnte, war eine anlassfallbezogene Vertrauenswürdigkeitsprüfung durchzuführen.

20.2 Der RH stellte fest, dass die Überprüfung künftiger und bestehender Bediensteter der DSN im Rahmen der Vertrauenswürdigkeitsprüfung umfassender und tiefgehender war als bei der Sicherheitsüberprüfung. Erstere umfasste u.a. auch Aufenthalte in oder Beziehungen zu fremden Staaten, eine Recherche mittels OSINT über die öffentlich sichtbare Nutzung von Online-Diensten sowie die Befragung von Referenzpersonen. Darüber hinaus war die Vertrauenswürdigkeitsprüfung an festgelegte Themenbereiche (z.B. Vermögensverhältnisse und finanzielle Verbindlichkeiten) gebunden, was eine höhere Flexibilität im Vergleich zur Sicherheitsüberprüfung gewährleistete.

Die Überprüfung von Personen im Rahmen von Vertrauenswürdigkeitsprüfungen war eine wichtige präventive Schutzmaßnahme insbesondere zum Schutz vor Spionage. Obwohl der Gesetzgeber in den Gesetzesmaterialien zur Einführung der Vertrauenswürdigkeitsprüfung die Sicherheitsüberprüfung für die Gewährleistung des Schutzes von klassifizierten Informationen für unzureichend hielt, blieben die gesetzlichen Grundlagen seitdem unverändert. Aus Sicht des RH sollte die Überprüfung von Personen flexibel an geänderte Bedrohungslagen angepasst werden können und sich in der Beurteilung auf objektive Maßstäbe stützen. In der Abwicklung sollten die Potenziale der Vernetzung und Digitalisierung unter Berücksichtigung des Datenschutzes genutzt werden.

Der RH empfahl dem Innenministerium, unter Einbindung der wesentlichen Bedarfs- und Interessensträger die rechtlichen, organisatorischen und prozessualen Grundlagen der Vertrauenswürdigkeits- und Sicherheitsüberprüfung zu analysieren. Dies mit dem Ziel, eine flexible, zeitgemäße, effektive und effiziente Durchführung der Prüfung zu gewährleisten. Die Ergebnisse wären in geeigneter Weise umzusetzen.

Das Militärbefugnisgesetz enthielt gesetzliche Ausschlussgründe, bei deren Vorliegen Betroffene als nicht „verlässlich" galten und dadurch ex lege von der Ausübung einer entsprechenden Tätigkeit ausgeschlossen waren. Eine vergleichbare Regelung sah weder das SNG – ausgenommen die Verweigerung und die mangelnde Mitwir-

kung – noch das Sicherheitspolizeigesetz vor. Ausschlussgründe könnten u.a. eine rechtskräftige Verurteilung wegen bestimmter Straftaten oder eine bereits negativ absolvierte Vertrauenswürdigkeits- oder Sicherheitsüberprüfung in der Vergangenheit sein. Der RH erachtete eine solche Regelung als zweckmäßig. Das würde eine schonendere Ressourcennutzung ermöglichen, ohne den präventiven Eigenschutz zu beeinträchtigen.

Der RH empfahl dem Innenministerium, analog zum Militärbefugnisgesetz auch im SNG und Sicherheitspolizeigesetz für die Vertrauenswürdigkeits- und Sicherheitsüberprüfung eine Regelung im Nationalrat zu initiieren, die Gründe für eine ex lege negativ zu beurteilende Überprüfung festlegt.

Der RH merkte an, dass Verwaltungspersonal, das durch seine Kontroll- und Dienstleistungsaufgaben insbesondere im Rahmen seiner Tätigkeit für die Dienstbehörde oder Personalstelle und den Rechtsschutzbeauftragten (bis 30. September 2025) umfangreiche Einblicke in sensible Bereiche des Verfassungsschutzes erhielt, keine Vertrauenswürdigkeitsprüfung durchlaufen musste.

Er empfahl dem Innenministerium, analog zu den bestehenden Regelungen im SNG zu den Personen, die einer Vertrauenswürdigkeitsprüfung unterzogen werden, eine gesetzliche Regelung im Nationalrat zu initiieren, die Verwaltungspersonal mit vergleichbarem Einblick in die sensible Tätigkeit des Verfassungsschutzes in die Vertrauenswürdigkeitsprüfung einbezieht.

20.3 Laut Stellungnahme des Innenministeriums sei im Regierungsprogramm 2025–2029 festgelegt, dass das Sicherheitspolizeigesetz zur Professionalisierung der Sicherheitsüberprüfungen von natürlichen und juristischen Personen novelliert werden solle. Die konkrete Ausgestaltung (z.B. Gründe für eine ex lege negativ zu beurteilende Überprüfung) müsse erst ausgearbeitet werden.

Bei einer SNG-Novellierung würden auch die gesetzlichen Regelungen der Vertrauenswürdigkeitsprüfung geprüft und gegebenenfalls adaptiert.

Die Einbeziehung von Verwaltungspersonal mit Einblick in die sensible Tätigkeit des Verfassungsschutzes in die Vertrauenswürdigkeitsprüfung werde im Rahmen der Evaluierung des SNG berücksichtigt; entsprechend den neu hinzugekommenen Aufgaben bedürfe es eines Personalzuwachses in der Vertrauenswürdigkeitsprüfung.

Verlässlichkeitsprüfung

21.1 (1) Die Verlässlichkeitsprüfung war in §§ 23 und 24 Militärbefugnisgesetz geregelt, nähere Bestimmungen über die Verlässlichkeitserklärung gemäß § 24 Abs. 1 leg. cit. in einer Verordnung des Bundesministers für Landesverteidigung[37]. Die Verlässlichkeitsprüfung diente der Abklärung der Verlässlichkeit einer Person anhand von Daten, die Aufschluss über allfällige Anhaltspunkte geben, ob von dieser Person eine Gefahr für die militärische Sicherheit ausgeht.

Die Verlässlichkeitsprüfung war die Voraussetzung für die Aufnahme in ein Dienstverhältnis zum Verteidigungsministerium, in einer reduzierten Form war sie Voraussetzung für den selbstständigen Zutritt zu militärischen Liegenschaften. Darüber hinaus war sie – neben den Verpflichtungen zum Geheimschutz – Voraussetzung für den Zugang zu klassifizierten Informationen ab der Stufe „VERTRAULICH" und zur Dienstverwendung in sicherheitsrelevanten Bereichen.

(2) Basis der Verlässlichkeitsprüfung war eine Verlässlichkeitserklärung der zu überprüfenden Person. Das Verteidigungsministerium unterschied – nach Maßgabe der Gefahr für die militärische Sicherheit – zwischen einer einfachen und erweiterten Verlässlichkeitserklärung.

- Die einfache Verlässlichkeitserklärung umfasste Angaben zur Person und zum persönlichen und familiären Umfeld, zu Kontakten mit verfassungsfeindlichen Gruppen oder zu ausländischen Nachrichten- und Sicherheitsdiensten, zu Wehrdienstleistungen im Ausland sowie Wehrersatzdienstleistungen im In- und Ausland. Mit Relevanz für die militärische Sicherheit waren Angaben zu straf- und verwaltungsstrafrechtlichen Verfahren, Ausbildung und Erwerbstätigkeit, Mitgliedschaften und zu finanziellen Verbindlichkeiten erforderlich.
- Die erweiterte Verlässlichkeitserklärung umfasste zusätzlich gesundheitliche und finanzielle Aspekte sowie nähere Auskünfte zum familiären Umfeld (z.B. Staatsbürgerschaft, Beruf und Wohnsitz der Eltern) und zu beruflichen Tätigkeiten.

(3) Die Kommandantinnen und Kommandanten bzw. Leiterinnen und Leiter der Organisationseinheiten des Verteidigungsministeriums waren – nach Abfrage des Vorliegens einer aufrechten Verlässlichkeitsprüfung und des tatsächlichen Bedarfs einer Prüfung – für die Einleitung einer Verlässlichkeitsprüfung des Personals verantwortlich. Die Durchführung der Verlässlichkeitsprüfungen oblag den mit der nachrichtendienstlichen Abwehr betrauten Dienststellen des Verteidigungsministeriums (Abwehramt und teilweise Heeres-Nachrichtenamt)[38]. Wenn Ermittlungsergebnisse

[37] Verordnung des Bundesministers für Landesverteidigung über die Verlässlichkeitserklärung, BGBl. II 195/2001

[38] § 23 Militärbefugnisgesetz

der Verlässlichkeitsprüfungen von den Angaben in der Verlässlichkeitserklärung abwichen, bestand die Möglichkeit zur Stellungnahme.[39]

(4) Den Abschluss einer Verlässlichkeitsprüfung bildete die Beurteilung, ob Anhaltspunkte dafür bestanden, dass von der überprüften Person eine Gefahr für die militärische Sicherheit ausging oder nicht. Ein Katalog an Risikofaktoren lag im Verteidigungsministerium vor. Keine Beurteilung erfolgte bei fehlender Überprüfbarkeit von Daten (z.B. lange Auslandsaufenthalte, im Ausland begangene gerichtlich strafbare Handlungen). Dies wurde beim Abschluss vermerkt. Zu den Ausschlussgründen gemäß § 23 Abs. 2 Militärbefugnisgesetz – die Person galt dann als nicht verlässlich – zählten u.a. Verurteilungen durch ein inländisches Gericht wegen Straftaten nach dem Militärstrafgesetz[40] und Strafgesetzbuch (z.B. Hochverrat, Angriffe gegen den Staat oder auf oberste Staatsorgane, Landesverrat) oder falls aus von der überprüften Person zu vertretenden Gründen eine Feststellung des für die Verlässlichkeit maßgeblichen Sachverhalts nicht möglich war.

Positive Beurteilungen der Verlässlichkeit endeten in einer Prüfbescheinigung für die jeweilige Zulassungsgruppe (von Zutrittsberechtigungen bis zum Zugang zu streng geheimen Informationen). Die Ergebnisse waren in einer Datenbank hinterlegt. Die Gültigkeitsdauer lag zwischen fünf und zehn Jahren je nach Zulassungsgruppe, Dienstzugehörigkeit und -verwendung.

21.2 Der RH hielt fest, dass das Verteidigungsministerium mit der Verlässlichkeitsprüfung über die Möglichkeit zur Überprüfung künftiger und bestehender Bediensteter verfügte. Die Verlässlichkeitsprüfung konnte – je nach Zulassungsgruppe – abgestuft auf Basis der einfachen oder erweiterten Verlässlichkeitserklärung durchgeführt werden.

[39] gemäß § 24 Abs. 3 Militärbefugnisgesetz

[40] BGBl. 344/1970 i.d.g.F.

Personenbezogene Interne Kontrollsysteme

Personalaufnahme

22.1 (1) Die Gestaltung des Bewerbungsprozesses oblag der im Innenministerium für Personalangelegenheiten zuständigen Organisationseinheit. Personen, die eine Tätigkeit in der DSN anstrebten, mussten zunächst ein dreiteiliges Auswahlverfahren durchlaufen: eine computerunterstützte psychologische Testung, ein psychologisches Interview und ein Fachgespräch. Hier stand insbesondere das in der Ausschreibung beschriebene Anforderungsprofil im Vordergrund, nicht ein allfälliges Risiko für den Verfassungsschutz. Dieses musste im Rahmen der Vertrauenswürdigkeitsprüfung festgestellt werden (TZ 20).

(2) Eine Voraussetzung für die Aufnahme in ein Dienstverhältnis zum Verteidigungsministerium war die Verlässlichkeitsprüfung. Zusätzlich hatten Personen, die eine Tätigkeit im Abwehramt anstrebten, ein mehrstufiges Auswahlverfahren zu durchlaufen. Dazu zählten neben der allgemeinen Erfüllung des Anforderungsprofils eine persönliche Auswahl der Personen, ein psychologisches Screening, eine erweiterte Verlässlichkeitsprüfung (TZ 21), ein Hearing und ein Assessment für Auslandseinsätze. Nach einer positiven Beurteilung erfolgten die Aufnahme und Ausbildung.

(3) Das Außenministerium veranlasste vor der Aufnahme einer Bewerberin bzw. eines Bewerbers sowie bei Versetzungen als Sicherheitsmaßnahme u.a. eine Sicherheitsüberprüfung. Vor der Aufnahme wurden alle Bediensteten, auch jene des Kabinetts, einer Sicherheitsüberprüfung durch die DSN unterzogen. Eine erneute Überprüfung erfolgte jedenfalls alle zehn Jahre bzw. anlassbezogen sowie stets bei Übernahme einer Funktion mit einer höheren Sicherheitseinstufung.

Eine den örtlichen Verhältnissen angepasste Vorgehensweise sah das Außenministerium für die österreichischen Vertretungsbehörden vor.

Unabhängig von der Sicherheitsüberprüfung unterzog das Außenministerium Bewerberinnen und Bewerber einem mehrteiligen Auswahlverfahren mit Online-Test, schriftlichem Test, Beurteilung in einem Assessment Center[41] und einer kommissionellen mündlichen Prüfung.[42]

22.2 Der RH hielt fest, das im Innen-, im Verteidigungs- und im Außenministerium im Zuge der Personalaufnahme personenbezogene Überprüfungen als Aufnahmevor-

[41] Dieses dauerte einen Tag, wurde durch die Arbeitspsychologin des Außenministeriums in Zusammenarbeit mit Psychologinnen und Psychologen des Verteidigungsministeriums durchgeführt und beinhaltete Gruppenübungen, computerunterstützte Tests und ein psychologisches Einzelgespräch.

[42] Bei dieser Prüfung stand neben anderen Aspekten insbesondere die Eignung für die ausgeschriebene Karriere im Vordergrund.

aussetzung bestanden. Grundsätzlich konnten die Bundesministerien diese Überprüfungen je nach Erfordernis des Geheimschutzes für den Zugang zu Informationen abgestuft für den jeweiligen Einsatzbereich anwenden.

Personalausbildung und -entwicklung

23.1 (1) Neue Bedienstete der DSN mussten in der ersten Woche ihrer Tätigkeit die E-Learning-Module zu den Themen Verfassungsschutz und klassifizierte Informationen absolvieren. Danach waren innerhalb der ersten drei Monate neben einer Einführungsveranstaltung weitere Schulungen und E-Learning-Module abzuschließen. Das E-Learning-Modul „Klassifizierte Informationen" galt gleichzeitig als Unterweisung für den Zugang zu klassifizierten Informationen gemäß InfoSiG und Geheimschutzordnung. Es war danach von den Bediensteten der DSN jährlich zu wiederholen.

Gemäß § 2 Abs. 7 SNG hatten Bedienstete der DSN einen speziellen Grundausbildungslehrgang Verfassungsschutz an der Sicherheitsakademie zu absolvieren. In zehn Wochen vermittelt er soziale und fachliche Kompetenzen für den Verfassungsschutz (z.B. Informationssicherheit, Sicherheitslücke Mensch und Interne Sicherheit). Im Jahr 2024 fanden drei Lehrgänge statt.

Weiters war für Bedienstete bestimmter Verwendungsgruppen der Fachhochschullehrgang Verfassungsschutz vorgesehen. Er deckte u.a. die Schwerpunkte Entwicklung und Aufgaben des Verfassungsschutzes, Management, Führung und Recht im Verfassungsschutz, Sicherheitsaspekte und Bedrohungen im Bereich Verfassungsschutz sowie Grundsätze und Methoden staatspolizeilicher und nachrichtendienstlicher Arbeit ab.

Abseits des Aus- und Weiterbildungsangebots führte die DSN regelmäßig und anlassbezogen Awareness-Maßnahmen zu Sicherheitsthemen, insbesondere im Bereich des Geheimschutzes, mittels Aushang in den Gebäuden und auf der Intranetstartseite durch. Auch bot sie verfassungsschutzrelevante Beratungen und allgemeine Sicherheitsberatungen für die obersten Organe der Vollziehung an.

(2) Im Verteidigungsministerium mussten alle Bediensteten jährlich IKT-Sicherheitsbelehrungen und Geheimschutzbelehrungen absolvieren. Für Schlüsselpersonal und Ressortangehörige waren auch Datenschutzbelehrungen verpflichtend. Die IKT-Sicherheitsbelehrung konnte im Rahmen eines E-Learning-Moduls mit integriertem Leistungsnachweis absolviert werden. Die Weiterentwicklung des Sicherheits- und Zutrittsinformationssystems ermöglichte seit 2020 eine automatische Speicherung des positiven Abschlusses des E-Learning-Moduls.

Die erfolgreiche Personalaufnahme im Abwehramt bildete den Beginn für eine mehrstufige Basisausbildung (z.B. Eigenschutz, Gesprächsführung, OSINT-Recherche) und Speziallehrgänge (z.B. Observationen). Die Curricula der Ausbildung waren unabhängig von Vorbildung und -verwendung sowie von Funktion und Dienstgrad. Jährlich verpflichtend waren zudem Kaderfortbildungen und anlassbezogene Schulungen sowie die IKT-Sicherheitsbelehrungen und Geheimschutzbelehrungen.

Das Abwehramt gestaltete auch für externe Personen Sensibilisierungs- und Informationsvorträge. Dazu zählten – neben Teilen der Bundesregierung – die Generalsekretärinnen und Generalsekretäre, die Präsidentschaftskanzlei und Militärangehörige außerhalb des Abwehramtes.

(3) Die Grundausbildung im Außenministerium umfasste auch eine Schulung zum Thema Informationssicherheit und Umgang mit klassifizierten Informationen. Das Absolvieren dieser Schulung war für die Bediensteten erforderlich, um gemäß InfoSiG (und auch gemäß Geheimschutzordnung) Zugang zu klassifizierten Informationen zu erhalten.

Die im Rahmen der Grundausbildung[43] zu absolvierende Einweisung in Sicherheitsthemen[44] war anlässlich jeder (Auslands-)Versetzung zu wiederholen bzw. zu ergänzen. Im Zuge dessen vermittelte die zuständige Abteilung I.2 in einer Sicherheitsunterweisung den Bediensteten die Pflichten – und die Folgen von Verstößen – gemäß InfoSiG, Informationssicherheitsverordnung und internen Runderlässen. Die unterwiesenen Personen erhielten alle relevanten Dokumente (Gesetze, Runderlässe, Merkblätter) und hatten den Erhalt dieser sowie die Durchführung der Unterweisung durch persönliche Unterfertigung zu bestätigen.

Im Rahmen von Auslandsbesuchen an österreichischen Vertretungsbehörden oder von Veranstaltungen des Ministeriums (etwa der jährlichen Botschafterkonferenz sowie der jährlichen Konsularkonferenz) führten Bedienstete der zuständigen Abteilung der Zentralstelle[45] Veranstaltungen zur Bewusstseinsbildung durch, die auch Aspekte der Spionageabwehr bzw. -prävention behandelten. Das Außenministerium band dabei auch Mitarbeiterinnen und Mitarbeiter der DSN bzw. des Heeres-Nachrichtenamts oder des Abwehramtes ein.

Gemäß § 19 Abs. 1 Bundesgesetz über Aufgaben und Organisation des auswärtigen Dienstes-Statut[46] (in der Folge: **Statut für den auswärtigen Dienst**) waren Dienststellenleitungen angehalten, insbesondere Sicherheitsaspekten prioritäre Bedeu-

43 bereits ab dem Onboarding

44 die auch Spionageprävention umfasste

45 Abteilung I.2 Sicherheitsangelegenheiten

46 BGBl. I 129/1999 i.d.g.F.

tung zukommen zu lassen. Alle Bediensteten des Außenministeriums hatten daher vor ihrer Auslandsverwendung ein Sicherheitsgespräch mit der zuständigen Fachabteilung zu absolvieren. Für Dienstverwendungen an Vertretungsbehörden mit besonders herausfordernden Sicherheitsbedingungen waren darüber hinaus Zusatzausbildungen vor Beginn der Auslandsverwendung zu absolvieren.

23.2 Der RH stellte fest,

- dass die Aus- und Weiterbildungsprogramme der DSN Inhalte über Spionage, Spionageprävention und -abwehr enthielten. Diese Inhalte waren darüber hinaus auch Gegenstand von regelmäßigen und anlassbezogenen Awareness-Maßnahmen.
- dass auch die Aus- und Weiterbildungsprogramme des Verteidigungsministeriums, insbesondere des Abwehramtes, Inhalte über Spionage, Spionageprävention und -abwehr umfassten. Das Abwehramt gestaltete auch Sensibilisierungs- und Informationsvorträge für Militärangehörige und externe Personen.
- dass die Aus- und Weiterbildungsprogramme des Außenministeriums die Themen Informationsschutz, Eigenschutz und anlassbezogene Awareness-Maßnahmen abdeckten. Auch im Zusammenhang mit der wechselnden Auslandsverwendung setzte das Außenministerium Maßnahmen, etwa durch Sicherheitsgespräche vor Versetzungen oder die Nutzung von Tagungen auch für Fortbildung.

Nebenbeschäftigungen

24.1 (1) (a) Im Jahr 2016 erließ die damalige Innenministerin[47] die Nebenbeschäftigungsverordnung – Inneres.[48] Diese Verordnung legte gemäß § 56 Abs. 7 Beamten-Dienstrechtsgesetz 1979 fest, welche Nebenbeschäftigungen für Bedienstete des Innenministeriums jedenfalls unzulässig waren.

Die Interne Revision des Innenministeriums prüfte in den Jahren 2020 und 2021 das Thema Nebenbeschäftigungen. Sie stellte fest, dass die damalige Nebenbeschäftigungsverordnung – Inneres sensible Bereiche mit besonderem Schutzbedarf der Informationen und des Spezialwissens der Bediensteten (wie das BVT) nicht in besonderer Weise berücksichtigte. Daher empfahl sie, zu prüfen, ob die Nebenbeschäftigungsverordnung – Inneres diesem besonderen Schutzbedarf Rechnung trug. Aus diesem Anlass novellierte 2024 der Innenminister[49] die Nebenbeschäftigungsverordnung – Inneres und erweiterte die Aufzählung jedenfalls unzulässiger Nebenbeschäftigungen u.a. um die Vermittlung von spezifischen sicherheits- und kriminalpolizeilichen Kenntnissen und Fertigkeiten außerhalb tertiärer Bildungseinrichtungen in Konkurrenz zu Angeboten der Sicherheitsakademie.

47 Mag.ª Johanna Mikl-Leitner

48 BGBl. II 84/2016 i.d.g.F.

49 Mag. Gerhard Karner

(b) Der Direktorin bzw. dem Direktor und den stellvertretenden Direktorinnen bzw. Direktoren der DSN war die Ausübung jeder Nebenbeschäftigung mit Ausnahme von Tätigkeiten im Bereich der Lehre und mit Ausnahme von unentgeltlichen sonstigen Nebenbeschäftigungen untersagt. Unentgeltliche sonstige Nebenbeschäftigungen unterlagen einer Ausnahmebewilligung durch die Dienstbehörde (§ 2 Abs. 5 SNG).

Im Gegensatz zu den genannten Leitungsfunktionen waren für sonstige Bedienstete der DSN entgeltliche Nebenbeschäftigungen abseits der Lehre nicht generell unzulässig, sondern sie bedurften gemäß § 2 Abs. 6 SNG der Genehmigung durch die Dienstbehörde. Nebenbeschäftigungen im Bereich der Lehre waren meldepflichtig, sofern sie zu nennenswerten Einkünften führten. Im Rahmen der Meldung hatten Bedienstete die Inhalte der Vortragstätigkeit auch ihren Vorgesetzten und dem Büro „Interne Sicherheit" zur Durchsicht vorzulegen. Im Verfahren über die Genehmigung der Nebenbeschäftigung hatte die Dienstbehörde eine Stellungnahme der Direktorin bzw. des Direktors der DSN einzuholen.[50] Auch dabei waren die unmittelbar Vorgesetzten sowie das Büro „Interne Sicherheit" eingebunden. Neben den allgemeinen Zulässigkeitskriterien des § 56 Beamten-Dienstrechtsgesetz 1979 hatten sie das sich aus dem Verfassungsschutz ergebende dienstliche Interesse bei der Beurteilung zu berücksichtigen.

(2) Im Jahr 2011 erließ der damalige Verteidigungsminister[51] eine Verordnung über unzulässige Nebenbeschäftigungen.[52] Die Verordnung enthielt für militärische Organe mit Aufgaben der nachrichtendienstlichen Aufklärung und Abwehr jene Bereiche (z.B. Sicherheitsgewerbe, Kommunikationselektronik, Auskunfteien), in denen die Ausübung einer Nebenbeschäftigung jedenfalls unzulässig war. Darüber hinaus enthielt sie Einschränkungen von Nebenbeschäftigungen für Bedienstete, die Einfluss auf die Vergabe von Fördermitteln und Vergabeverfahren hatten.

Die Interne Revision des Verteidigungsministeriums legte im Jahr 2021 einen Bericht über die Prüfung zum Thema Nebenbeschäftigungen vor. Sie stellte fest, dass bei Einzelfällen zur Wahrung der Dienstgeberinteressen auch ein präventiver Handlungsbedarf bestand. Daher empfahl sie, eine Risikoanalyse durchzuführen, um Problembereiche für den Dienstgeber zu erkennen, und darauf basierend die Verordnung über unzulässige Nebenbeschäftigungen zu analysieren und gegebenenfalls zu überarbeiten.

50 Im Falle der Direktorin bzw. des Direktors der DSN war eine Stellungnahme der Generaldirektorin bzw. des Generaldirektors für die öffentliche Sicherheit erforderlich.

51 Mag. Norbert Darabos

52 Verordnung des Bundesministers für Landesverteidigung und Sport über unzulässige Nebenbeschäftigungen, BGBl. II 100/2011

(3) Für Bedienstete des Außenministeriums waren § 24 des Statuts für den auswärtigen Dienst, § 56 Beamten-Dienstrechtsgesetz 1979, § 5 Abs. 1 Vertragsbedienstetengesetz 1948 sowie § 515 des Handbuchs für den Auswärtigen Dienst die Rechtsgrundlage in Bezug auf Nebenbeschäftigungen. Die Bediensteten hatten der zuständigen Abteilung unverzüglich jede Aufnahme und Änderung einer erwerbsmäßigen Nebenbeschäftigung im Inland sowie jede Aufnahme und Änderung einer erwerbsmäßigen und einer nicht erwerbsmäßigen Nebenbeschäftigung im Ausland zu melden. Begründet wurde die Meldung auch nicht erwerbsmäßiger Nebenbeschäftigungen im Ausland mit den im Wiener Übereinkommen und in ähnlichen Abkommen angeführten starken Einschränkungen der Tätigkeit der Mitglieder von diplomatischen und konsularischen Vertretungen im Empfangsstaat. Deshalb müsse es der Dienstbehörde möglich sein, jede Nebenbeschäftigung zu untersagen, die im Empfangsstaat Zweifel an ihrer Vereinbarkeit mit der offiziellen Funktion des Bediensteten begründen könnte.[53]

Gemäß § 25 des Statuts für den auswärtigen Dienst[54] hatten Bedienstete einer Dienststelle im Ausland der zuständigen Abteilung die Aufnahme oder Beendigung einer im Ausland ausgeübten Erwerbstätigkeit eines mit ihnen im gemeinsamen Haushalt lebenden Familienangehörigen unverzüglich zu melden. Die Dienststellenleitung im Ausland hatte zusätzlich einmal im Jahr zu erheben, ob Nebenbeschäftigungen von Angehörigen vorliegen und ob diese auch an die Zentrale gemeldet wurden.

24.2 (1) Der RH stellte fest, dass Nebenbeschäftigungen für Leitungsfunktionen und Bedienstete der DSN entweder gesetzlich untersagt waren oder unter Genehmigungsvorbehalt der Dienstbehörde standen. Davon ausgenommen waren Tätigkeiten in der Lehre. Diese Ausnahme war bei der Vermittlung von spezifischen sicherheits- und kriminalpolizeilichen Kenntnissen und Fertigkeiten außerhalb von tertiären Bildungseinrichtungen auf Bereiche beschränkt, die nicht in Konkurrenz zu Angeboten der Sicherheitsakademie standen. Die Einbindung des Büros „Interne Sicherheit“ im Rahmen der Beurteilung von Nebenbeschäftigungen war für den RH mit Blick auf Spionageprävention und -abwehr zweckmäßig.

(2) Der RH hob hervor, dass ein restriktiver Umgang mit Nebenbeschäftigungen geeignet war, um im Sinne der Spionageprävention zu wirken. Er verwies – insbesondere im Zusammenhang mit der Erhöhung der Bedrohungslage durch Spionage – auf den von der Internen Revision im Verteidigungsministerium hervorgehobenen präventiven Handlungsbedarf zur Wahrung von Dienstgeberinteressen.

[53] vgl. ErläutRV 1852 BlgNR 20. GP 14

[54] in Verbindung mit § 515 des Handbuchs für den Auswärtigen Dienst

Der RH empfahl daher dem Verteidigungsministerium, basierend auf den Empfehlungen der Internen Revision eine Risikoanalyse im Bereich der Nebenbeschäftigungen durchzuführen. Dies mit dem Ziel, Problembereiche für den Dienstgeber zu erkennen und gegebenenfalls die Verordnung über unzulässige Nebenbeschäftigungen zu überarbeiten.

(3) Der RH stellte fest, dass sowohl für erwerbsmäßige als auch für nicht erwerbsmäßige Nebenbeschäftigungen im Außenministerium Meldevorschriften bestanden. Zweifel an der Vereinbarkeit mit der offiziellen Funktion im Empfangsstaat führten zur Untersagung. Dies betraf bei Auslandsverwendungen auch die im gemeinsamen Haushalt lebenden Familienangehörigen.

Zutrittsregelung

25.1 (1) Das Innenministerium verfügte über schriftliche Vorgaben betreffend den Zutritt zu den Standorten oder spezifischen Räumlichkeiten auf Ebene des Innenministeriums gesamt, einzelner Abteilungen oder spezifisch für die DSN.

Bei Besuchen Externer regelten die Vorgaben z.B. die Vergabe von Zutrittsberechtigungen für Wartungstätigkeiten im Zusammenhang mit IT-Services und IT-Produkten, den Umfang der Sicherheitsüberprüfung der Mitarbeiterinnen und Mitarbeiter externer Dienstleister und den Umgang mit Externen beim Zutritt sowie während ihrer Anwesenheit bei der DSN. Für Ressortfremde war die Einfahrt in die DSN-Liegenschaft verboten.

Für Bedienstete der DSN wurden die Zutrittsrechte zentral verwaltet. Je nach Räumlichkeit (Zone) innerhalb der DSN und dem diesbezüglichen Sicherheitsbedarf gab es unterschiedliche Zutrittssysteme und mussten eine oder mehrere Sicherheitsvoraussetzungen für den Zutritt erfüllt sein. Beim Betreten und Verlassen des Gebäudes wurden die Bediensteten der DSN (gegebenenfalls stichprobenartig) kontrolliert, klassifizierte Informationen durften ausschließlich in dafür bestimmten Räumlichkeiten unter speziellen, strengeren Sicherheitsvorkehrungen bearbeitet werden. Geregelt waren außerdem Verantwortlichkeiten in den Abteilungen und Büros für Objektsicherheit und Zutrittsmanagement, Dokumentations- und Meldepflichten bei Sicherheitsvorfällen oder für den Umgang mit privaten und dienstlichen elektronischen Geräten beim Zutritt zu und während des Aufenthalts in den Räumlichkeiten der DSN.

(2) Im Verteidigungsministerium bestanden für den Objektschutz schriftliche Vorgaben, die den Zutritt zu den Liegenschaften, spezifischen Gebäuden oder einzelnen Anlagen regelten. Besondere Vorschriften gab es für die nachrichtendienstlich genutzten Objekte. Die Regelungen verfolgten das Ziel, den Schutz militärischer

Rechtsgüter bereits im täglichen Betrieb, ohne zusätzliche Absicherungsmaßnahmen, sicherzustellen.

Geschützte Bereiche waren u.a. durch die Bestimmungen zum Geheimschutz oder bi- und multilaterale Vorgaben definiert. Die daraus abgeleiteten abgestuften Objektschutzkategorien sahen u.a. vor, ob darin von klassifizierten Informationen Kenntnis erlangt werden konnte und welche Art von Schutzmaßnahmen (z.B. äußere Abgrenzung, Perimeterschutz, Bewachung) erforderlich war. Besondere Anforderungen betrafen abhörsichere und abhörgeschützte Bereiche, in denen Besprechungen über klassifizierte Unterlagen stattfinden durften.

Den Objektschutzkategorien folgten abgestufte Zutrittsregelungen. Dienststellenfremde Personen mussten zum Teil ständig begleitet werden, eine gültige Prüfbescheinigung (Verlässlichkeitsprüfung) besitzen und vor Eintritt einer Sicherheitsbelehrung unterzogen werden.

Der Zutritt zum Abwehramt war grundsätzlich nur aus dienstlichen Gründen zulässig und bedurfte einer Genehmigung durch einen (zahlenmäßig engen) Kreis von Genehmigungsberechtigten. Die Zutritte waren zu protokollieren, elektronische Geräte (z.B. Mobiltelefone, Smartwatches, Laptops) von ressortfremden Personen versperrt zu deponieren und ausgegebene Erkennungszeichen sichtbar zu tragen. Darüber hinaus war der Umgang mit Notfällen und externen Dienstleistern geregelt.

(3) Im Außenministerium wurden technische bzw. bauliche Schutzmaßnahmen und Kontrollsysteme ergänzt um Regelungen betreffend den Zutritt nur für sicherheitsüberprüftes Personal (weiter eingeschränkt beispielsweise für besonders sensible Bereiche wie den Serverraum), die Verwendung elektronischer Zutrittssysteme in der Zentralstelle sowie das verpflichtende Führen von Verzeichnissen für Schlüssel (Schlüsselvormerke).

Mitarbeiterinnen und Mitarbeiter externer Dienstleister, die Zutritt für Standorte oder Dienste des Außenministeriums benötigten, wurden entweder gemäß §§ 55 f. Sicherheitspolizeigesetz sicherheitsüberprüft oder von sicherheitsüberprüften Personen begleitet. Das Außenministerium hielt fest, dass es in der Vergangenheit von Dienstleistungen durch Personal externer Dienstleister Abstand genommen habe, wenn es bei diesem zu Sicherheitsbedenken gekommen war. Eine Sicherheitsüberprüfung betreffe konkret stets nur jene Person, die die Dienstleistung erbringen sollte, da für eine generelle Unternehmensüberprüfung die Rechtsgrundlage fehle.

25.2 (1) Der RH hielt fest, dass in den überprüften Bundesministerien generell Zutrittsbeschränkungen bestanden. Diese waren durch bauliche (z.B. äußere Abgrenzungen, Lage von Räumlichkeiten) und technische (z.B. Zutrittskarten) sowie zusätzlich durch

organisatorische (z.B. Begleitung externer Personen) Maßnahmen geregelt. Im Innen- und Verteidigungsministerium gab es zum Teil strengere Maßnahmen.

(2) Der RH vermerkte, dass das Innenministerium und die DSN Zutrittsregelungen für die eigenen Räumlichkeiten schriftlich und je nach Sicherheitsbedarf der Räumlichkeit – mit unterschiedlichen Zutrittsvoraussetzungen im Sinne eines IKS – festgelegt hatten. Er hob hervor, dass das Innenministerium und die DSN Zuständigkeiten im Bereich des Zutrittsmanagements regelten und dass für den Zugang zu klassifizierten Informationen strengere Sicherheitsvorkehrungen galten.

(3) Der RH hielt fest, dass das Verteidigungsministerium abgestufte Objektschutzkategorien und Zutrittsregelungen je nach Schutzbedarf der militärischen Rechtsgüter und Informationen als IKS-Maßnahmen implementiert hatte.

Personal Offboarding

26.1 (1) Verließen Bedienstete die DSN dauerhaft, durchliefen sie einen sogenannten „Auscheckprozess“. Dieser beinhaltete die Abgabe aller elektronischen Geräte, die Sperre von Zugängen und Aufklärungsgespräche über Geheimhaltungspflichten.

Auch Personen, bei denen das Ergebnis der Vertrauenswürdigkeitsprüfung gegen eine (Weiter-)Beschäftigung bei der DSN sprach, durchliefen diesen Prozess. Zwischen 1. Jänner 2022 und 18. Jänner 2025 führten 38 Vertrauenswürdigkeitsprüfungen von (potenziellen) Bediensteten der DSN zu keinem positiven Ergebnis. Zum Stand Jänner 2025 war keine dieser Personen bei der DSN in Verwendung; zwei Betroffene waren anderen Organisationseinheiten des Innenministeriums zugeteilt, die anderen wurden z.B. (dauerhaft) versetzt, gekündigt oder nicht aufgenommen. In solchen Fällen war es das Ziel der DSN, schon bei der DSN beschäftigte betroffene Personen möglichst zeitnah nicht mehr in der DSN einzusetzen. Wenn keine dienstrechtliche Möglichkeit zur Auflösung des Dienstverhältnisses bestand, wurden Betroffene – nach etwaiger vorübergehender Dienstzuteilung, Dienstfreistellung oder Konsumation von Urlaub – in andere Bereiche des Innenministeriums versetzt. Dabei war es in allen Fällen notwendig, das Innenministerium als Dienstbehörde einzubinden und sich mit den aufnehmenden Stellen abzustimmen. Besondere Herausforderungen bei der alternativen Verwendung im Innenministerium bestanden nach Auskunft der DSN bei sehr DSN-spezifischen Berufsbildern.

(2) Das Abwehramt arbeitete zur Zeit der Gebarungsüberprüfung an einem Offboarding-Prozess für den eigenen Wirkungsbereich der militärischen Nachrichtendienste und erstellte in diesem Zusammenhang eine Risikobeurteilung. Die Beendigung von Dienstverhältnissen war beispielsweise mit dem Risiko eines Informationsabflusses verbunden. Die Sicherheitsüberlegungen des Abwehramtes umfassten einen risikoorientierten Offboarding-Prozess mit abgestuften Maßnahmen.

(3) Die internen Vorschriften des Außenministeriums – u.a. Runderlässe[55] und das Handbuch für den Auswärtigen Dienst – enthielten Regelungen für die Beendigung von Dienstverhältnissen. Im Handbuch fanden sich konkrete Handlungsanleitungen für die endgültige Beendigung der Tätigkeit einer Dienststellenleiterin bzw. eines Dienststellenleiters, etwa zum Umgang mit dem Amtssiegel, zur unverzüglichen Rückstellung des Diplomatenpasses und zur korrekten Amtsübergabe. Ebenso enthielt es Vorgaben[56] zur Vorgehensweise bei der Beendigung der „Dienstleistung in der Zentrale“ (infolge Pensionierung oder Auflösung des Dienstverhältnisses, Auslandsversetzung, Karenzierung). Das Handbuch verwies auf die zu verwendenden elektronischen Formulare. Neben der Vorgehensweise bei der Zurückstellung von Ausweisen und Zutrittskarten wies es auch ausdrücklich auf die Einhaltung des Datengeheimnisses nach Beendigung des Dienstverhältnisses hin.

26.2 (1) Der RH hielt fest,

- dass Bedienstete, die die DSN dauerhaft verließen, einen Offboarding-Prozess durchliefen
- und dass die DSN Personen, bei denen das Ergebnis der Vertrauenswürdigkeitsprüfung gegen eine Weiterbeschäftigung bei der DSN sprach, nicht mehr in der DSN einsetzte.

Um das Risiko schädlicher Handlungen durch betroffene Personen zu minimieren, beurteilte der RH es als zweckmäßig, diese Personen möglichst zeitnah in anderen Bereichen des Innenministeriums einzusetzen, sofern keine Kündigung möglich und die Interessen der aufnehmenden Stelle nicht gefährdet waren.

(2) Der RH hob die Bedeutung eines risikoorientierten Ansatzes für einen Offboarding-Prozess der militärischen Nachrichtendienste hervor. Er erachtete die Festschreibung eines Offboarding-Prozesses im Hinblick auf die Prozessdokumentation eines IKS für zweckmäßig.

Der RH empfahl dem Verteidigungsministerium, die Erstellung des Offboarding-Prozesses für die militärischen Nachrichtendienste ehestmöglich abzuschließen; darin wäre die Dokumentation der einzelnen Schritte des Prozesses (etwa in Form einer Checkliste) vorzusehen.

(3) Der RH hielt fest, dass das Außenministerium über Regelungen für einen Offboarding-Prozess verfügte, der auch die Besonderheiten der dislozierten Aufgabenerfüllung in den Vertretungsbehörden berücksichtigte.

[55] z.B. bezüglich IT-An- und -Abmeldungen (GZ 2022-0.756.634)

[56] Diese Regelungen umfassten auch Versetzungen, Verwendungsänderungen innerhalb der Zentrale etc.

26.3 Das Verteidigungsministerium hielt in seiner Stellungnahme fest, dass im Rahmen der Personalbetreuung des Abwehramtes die Sicherstellung notwendiger Maßnahmen im Zuge der Beendigung von Dienstverhältnissen erfolge. Die Erstellung des Offboarding-Prozesses im Abwehramt werde mit Nachdruck verfolgt.

Beschaffungen

27.1 (1) Für öffentliche Auftragsvergaben war das Bundesvergabegesetz in der jeweils geltenden Fassung maßgebend.[57] Handelte es sich beim Leistungsgegenstand um die Beschaffung bestimmter Leistungen des Verteidigungs- und Sicherheitsbereichs, war das Bundesvergabegesetz Verteidigung und Sicherheit 2012[58] anzuwenden. Dieses enthielt aufgrund der im Verteidigungs- und Sicherheitsbereich erhöhten Geheimhaltungs- und Versorgungsinteressen besondere Regelungen zur Informations- und Versorgungssicherheit.

Beide Vergabegesetze enthielten Ausnahmen, etwa zu Aufträgen, auf die die Ausnahmebestimmung in Art. 346 des Vertrags über die Arbeitsweise der Europäischen Union (**AEUV**)[59] Anwendung fand. Demnach unterlagen Maßnahmen, die für die Wahrung der wesentlichen Sicherheitsinteressen des Mitgliedstaates erforderlich waren, nicht den Vergabegesetzen.

(2) Die DSN übernahm mit Dezember 2021 die Aufgaben des BVT. Um ihre Aufgaben im gesetzlichen Umfang wahrnehmen zu können und den von internationalen Partnern vorgegebenen Rahmenbedingungen zu entsprechen, benötigte sie ein entsprechendes IT-System. Zur Unterstützung der Umsetzung von Hochsicherheitsnetzwerken sollten externe Leistungen zugekauft werden. Laut Einstufung durch das Innenministerium betraf die Auftragsvergabe wesentliche Sicherheitsinteressen des Bundes. Das Innenministerium vergab die Leistung im Oktober 2021 selbst, ohne Einbindung der Bundesbeschaffung GmbH (**BBG**), unter Heranziehung der Ausnahme (Schutz wesentlicher Interessen der Staatssicherheit) nach § 3 Abs. 1 Z 1 BBG-Gesetz (Bundesgesetz über die Errichtung der BBG)[60].

Bei der Vergabe der Leistungen zum Hochsicherheitsnetzwerk der DSN berief sich das Innenministerium auf die Ausnahmen des Art. 346 AEUV bzw. des § 9 Abs. 1 Z 5 Bundesvergabegesetz Verteidigung und Sicherheit 2012; die Vergabe erfolgte sohin außerhalb des Vergaberechts. Die Auswahl fiel auf ein Unternehmen, das aufgrund seiner bisherigen Tätigkeiten über eingehende Kenntnisse der österreichi-

[57] zur Zeit der Gebarungsüberprüfung: Bundesvergabegesetz 2018, BGBl. I 65/2018 i.d.g.F.

[58] BGBl. I 10/2012 i.d.g.F.

[59] BGBl. III 86/1999

[60] BGBl. I 39/2001

schen Verwaltung und insbesondere auch des Innenministeriums verfügte. Die Gesamtkosten für die Beschaffung betrugen 1,25 Mio. EUR.

Im Juni 2022 berichtete eine deutsche Mediengesellschaft über die Beauftragungen durch das Innenministerium im Zusammenhang mit einem IKT-Projekt für die DSN, über Verbindungen des beauftragten Unternehmens zu einem ehemaligen Geschäftsführer eines deutschen Zahlungsdienstleisters sowie über mögliche, damit zusammenhängende Verbindungen zur Russischen Föderation.

Infolge dieser Berichterstattung nahm die DSN von der Umsetzung des Hochsicherheitsnetzwerks durch externe Unternehmen Abstand. Das Konzept des externen Unternehmens kam nicht zur Anwendung. Potenzielle Auswirkungen der medialen Vorhalte auf andere Projekte des Unternehmens für die Republik Österreich untersuchte weder das Innenministerium noch die DSN. Eine Information an andere Bundesministerien unterblieb. Die DSN gab an, über keine Möglichkeiten zur Überprüfung von Unternehmen zu verfügen.

(3) Das Abwehramt war für die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen zuständig.[61] Ein Unternehmen benötigte eine solche Bescheinigung, wenn für die Teilnahme an industriellen Tätigkeiten und Forschungstätigkeiten sowie zur Erlangung von Aufträgen klassifizierte Informationen erforderlich waren. Die Überprüfung durch das Abwehramt umfasste u.a. Integrität und Beeinflussbarkeit des Unternehmens, die Ausgestaltung der Sicherheitssysteme für den Schutz klassifizierter Informationen sowie Verlässlichkeitsprüfungen (TZ 21). Erforderlichenfalls waren Sicherheitsüberprüfungen durchzuführen (TZ 20).

Das Abwehramt überprüfte Anfang 2021 – unabhängig von der Beauftragung durch das Innenministerium – das mit der Unterstützung zur Erstellung des Hochsicherheitsnetzwerks beauftragte Unternehmen. Eine Sicherheitsunbedenklichkeitsbescheinigung stellte das Abwehramt im Februar 2021 aus.

27.2 Der RH hielt fest, dass die Vergabe zur Unterstützung der Umsetzung von Hochsicherheitsnetzwerken der DSN wesentliche Sicherheitsinteressen des Bundes betraf. Auch wenn die von einer deutschen Mediengesellschaft aufgezeigten Geschäftsverbindungen nicht gerichtlich verwertbar waren, hielt es der RH unter dem Gesichtspunkt der Spionageprävention für zweckmäßig, von der Verwertung der beauftragten Leistung Abstand zu nehmen.

Kritisch sah der RH aus dem Blickwinkel der Gebarungskontrolle die aufgelaufenen Kosten von 1,25 Mio. EUR. Auch beurteilte er es als kritisch, dass weder das Innenministerium noch die DSN im Sinne der Spionageprävention Auswirkungen auf

[61] gemäß §§ 11 bis 13 InfoSiG

andere Projekte des Unternehmens für die Republik Österreich weiter untersuchte. Ein Austausch mit anderen Bundesministerien unterblieb.

Der RH empfahl dem Innenministerium, gegebenenfalls andere Bundesministerien über jene sicherheitsrelevanten Umstände zu informieren, aufgrund derer das Innenministerium von der Nutzung der vertraglichen Leistungen im eigenen Bereich Abstand nimmt.

Der RH hob hervor, dass die rechtliche Grundlage der Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen auf eine sichere Verwendung klassifizierter Informationen abstellte. Spezifische Aspekte der Spionageprävention waren davon nicht umfasst. Die personenbezogenen Überprüfungshandlungen (Sicherheitsüberprüfung, Verlässlichkeitsprüfung) beruhten auf einer Selbstauskunft der überprüften Personen. Mangels gesetzlicher Grundlage war es bei diesen Überprüfungen nicht möglich, nachrichtendienstliche Informationen heranzuziehen sowie zivile und militärische Informationen zu Unternehmen auszutauschen.

Der RH empfahl dem Innen- und dem Verteidigungsministerium, für Beschaffungen, die wesentliche Sicherheitsinteressen des Bundes betreffen und die damit für eine Ausnahme von den Bundesvergabegesetzen zugänglich sind, auf eine gesetzliche Regelung hinzuwirken, die eine Überprüfung von Unternehmen vor Beauftragung (im Rahmen der Eignungsprüfung) unter Heranziehung nachrichtendienstlicher Erkenntnisse ermöglicht.

27.3 (1) Laut Stellungnahme des Innenministeriums finde auf bilateraler Basis ein Austausch (über sicherheitsrelevante Umstände) statt, eine standardisierte Informationsweitergabe wäre im Rahmen einer interministeriellen Vereinbarung anzudenken. Eine formale Austauschplattform über alle Ministerien müsse den Sicherheitsanforderungen entsprechen.

Im Entwurf zur Novelle des InfoSiG sei vorgesehen, dass Unternehmen, die im Zuge von Aufträgen Zugang zu klassifizierten Informationen erhielten, eine Sicherheitsunbedenklichkeitsbescheinigung benötigten. Bisher sei das nur für international klassifizierte Informationen nötig. Bei der Beauftragung von Dienstleistern oder sonstigen Auftragnehmern solle grundsätzlich eine Prüfung auf Sicherheitsrisiken für den Verfassungsschutz möglich sein.

(2) Das Verteidigungsministerium teilte in seiner Stellungnahme mit, dass bei Vorliegen von Sicherheitsinteressen des Bundes der Ausnahmetatbestand des Art. 346 AEUV erfüllt sein könne. Vergaberechtliche Vorschriften seien diesfalls nicht anzuwenden, allfällige Sicherheitsüberprüfungen bedürften einer Rechtsgrundlage.

Ein Überprüfungszeitpunkt „vor Beauftragung“ sollte nicht der Zeitpunkt unmittelbar vor Zuschlagserteilung sein. Es bestehe sonst die Gefahr, dass Mitbewerbern ohne vorherige Sicherheitsüberprüfung bereits Zugang zu sensiblen und sicherheitsrelevanten Informationen gewährt würde. Das Verteidigungsministerium regte einen vorgelagerten Zeitpunkt an, sodass erst nach erfolgter Sicherheitsüberprüfung entschieden werden könne, welche Unternehmen für eine Teilnahme am weiteren Verfahren in Betracht kämen (Sicherheitsüberprüfung im Rahmen der Eignungsprüfung). Hierfür könne es erforderlich sein, eine ausdrückliche gesetzliche Grundlage für die Durchführung derartiger Unternehmensprüfungen in diesem frühen Stadium zu schaffen.

27.4 Der RH wies gegenüber dem Verteidigungsministerium darauf hin, dass die Empfehlung im vom Verteidigungsministerium beschriebenen Sinne intendiert war und präzisierte dementsprechend den Wortlaut der Empfehlung.

28.1 (1) Der RH erhob im Innen-, im Verteidigungs- und im Außenministerium Beschaffungen im Zusammenhang mit der IT-Sicherheitsinfrastruktur (etwa Server, Netzwerkkomponenten, unterbrechungsfreie Stromversorgungen, Komponenten zur verschlüsselten Kommunikation).

Folgende Tabelle zeigt die Aufteilung der Auftragsabwicklung der von den drei überprüften Ministerien im Zeitraum 2017 bis 2024 beschafften IT-Sicherheitsinfrastruktur und wie viel sie anteilsmäßig über die BBG bzw. selbst beschafften:

Tabelle 2: Beschaffungen IT-Sicherheitsinfrastruktur in den drei überprüften Ministerien; 2017 bis 2024

	Einbeziehung der BBG	durch das Ministerium selbst	BVergGVS und Ausnahmen zu Vergabegesetzen
	Abwicklung des Auftragsvolumens		
	in %		
Innenministerium (für DSN)	58	42	0
Verteidigungsministerium (für Abwehramt)	89	2	9
Außenministerium	70	14	16

BBG = Bundesbeschaffung GmbH
BVergGVS = Bundesvergabegesetz Verteidigung und Sicherheit 2012

Quellen: BMI; BMLV; BMEIA; Auswertung: RH

(2) Im Innenministerium war für Beschaffungen ein Standardprozess etabliert. Je nach Leistungsgegenstand waren definierte Abteilungen zentral zuständig. Wenn die DSN als Bedarfsträger es z.B. aus Gründen der Informationssicherheit für notwendig erachtete, konnte sie Vergaben auch selbst, d.h. ohne Einbindung von Stellen außerhalb der DSN, durchführen. Das Bundesvergabegesetz 2018 und das

Bundesvergabegesetz Verteidigung und Sicherheit 2012 sahen Ausnahmen für Beschaffungen im Sicherheitsbereich bzw. für Zwecke nachrichtendienstlicher Tätigkeiten vor.[62] Die DSN orientierte sich bei Beschaffungen nach eigenen Angaben an international (in Nachrichtendiensten) bewährten Vorgehensweisen. Sie griff bei der Vorselektion der Hersteller und Produkte auf internationale nachrichtendienstliche Erkenntnisse, Umfeldanalysen sowie Marktforschung in offenen Quellen zum Renommee der Produkte und der Hersteller bzw. Lieferanten zurück. Eine darüber hinausgehende (verpflichtende) Überprüfung der Unternehmen war rechtlich nicht vorgesehen bzw. möglich. Relevante Personen konnten sicherheitsüberprüft werden, wenn sie Zugang zu klassifizierten Informationen erhalten sollten. Das Thema „Lieferkette technischen Equipments" war im internen Risikomanagement der DSN berücksichtigt.

(3) Im Verteidigungsministerium fielen Beschaffungen für die militärischen Nachrichtendienste in den Aufgabenbereich der Vergabeabteilung. Die Zuordnung von Beschaffungen (IT-Beschaffungen) zu Zwecken der Spionageprävention war nicht möglich, weil die Bedarfsbegründungen der antragstellenden Organisationseinheiten keine Rückschlüsse darauf zuließen. Nachrichtendienstliche Anforderungen waren bereits bei der Einleitung von Beschaffungsvorgängen zu berücksichtigen.

Im Bereich der nachrichtendienstlichen Abwehr führte das Abwehramt Beschaffungen in geringem Umfang durch, die der Informationsgewinnung, dem Eigenschutz sowie der Abwehr von Gefahren zuzurechnen waren. So beschaffte das Abwehramt beispielsweise Abhörschutzboxen für mobile Telefone.

Die Einbindung von externem Personal in einen Beschaffungsprozess unterlag vertraglichen Regelungen. Erforderte der Einsatz externen Personals Zugang zu sicherheitsrelevanten oder klassifizierten Informationen oder Zutritt zu Sicherheitsbereichen, wandte das Verteidigungsministerium die Geheimschutzvorschriften an. Die erforderlichen Sicherheitsüberprüfungen waren durchzuführen (z.B. Verlässlichkeitsprüfung).

(4) Das Außenministerium beschaffte IT-Leistungen vorrangig über die BBG. Ministeriumsintern gab es darüber hinaus Vorgaben für Beschaffungen im Wege der Direktvergabe sowie zur Kerndatenmeldung vergebener Aufträge gemäß §§ 61 ff. Bundesvergabegesetz 2018. Diese Vorgaben wiesen auf Ausnahmen von der Bekanntgabeverpflichtung hin und die Abteilung VI.6 sensibilisierte anlassbezogen in Vergabeprozessen hinsichtlich der Ausnahme zur Bekanntgabe „bestimmter Angaben". Bei Auftragswerten oberhalb der Direktvergabegrenze war jedenfalls die Sektion VI zu befassen.

[62] insbesondere § 9 Abs. 1 Z 1, 4 und 5 Bundesvergabegesetz 2018 und § 9 Abs. 1 Z 5 und 6 Bundesvergabegesetz Verteidigung und Sicherheit 2012

Der für eine konkrete IT-Beschaffung zuständigen Organisationseinheit oblag die Erstbeurteilung, ob Aspekte der Spionageabwehr bzw. -prävention vorlagen. In Abstimmung mit den zuständigen Fachabteilungen war sodann eine vergaberechtlich zulässige Vorgangsweise zu erarbeiten.

Vor Einleitung einer IT-Beschaffung waren bestehende bzw. anlassbezogen erstellte Sicherheitskonzepte Grundlage für die Leistungsdefinition. Risikomanagement, das Erkennen von IT-Sicherheitsrisiken sowie die Beachtung von allfällig verbleibenden Restrisiken erfolgten bei Bedarf in Abstimmung mit den entsprechenden Organisationen. Bei Bedarf wurden Beschaffungen bzw. deren Konzepte auch einem Penetrationstest durch unabhängige externe Unternehmen unterzogen.

28.2 (1) Der RH hielt fest, dass die DSN Vergaben bei Bedarf ohne Einbindung anderer Stellen im Innenministerium selbst durchführen konnte. Er erachtete es dabei als zweckmäßig, möglichst wenige Personen – insbesondere außerhalb der DSN – in den Beschaffungsprozess einzubinden, um das Risiko eines unbefugten Eingriffs in den Liefer- bzw. Leistungsprozess und die Anzahl an Angriffspunkten für Spionagetätigkeiten zu minimieren. Er erachtete es ebenfalls als zweckmäßig, dass die DSN die potenziell in die Liefer- bzw. Leistungskette involvierten Unternehmen und handelnden Personen vor der Beauftragung im Rahmen der gesetzlichen Möglichkeiten und auf Basis nachrichtendienstlicher Erkenntnisse hinsichtlich deren Renommee überprüfte.

Der RH empfahl der DSN, für rechtliche Fragen des Vergabeverfahrens – unter Wahrung der Sicherheitsinteressen – die Expertise von zentralen, für Beschaffungen zuständigen Abteilungen des Innenministeriums heranzuziehen.

(2) Der RH hielt fest, dass im Verteidigungsministerium Beschaffungen für die militärischen Nachrichtendienste in den Aufgabenbereich der Vergabeabteilung fielen. Das Abwehramt konnte zu Zwecken der Informationsgewinnung, des Eigenschutzes sowie der Abwehr von Gefahren selbst Beschaffungen in geringem Umfang durchführen.

(3) Der RH verwies darauf, dass das Außenministerium Beschaffungen im Wege der BBG durchführte. Das Außenministerium führte 16 % seiner Beschaffungen unter Heranziehung der Ausnahmen für Beschaffungen im Sicherheitsbereich gemäß Bundesvergabegesetz Verteidigung und Sicherheit 2012 durch.

28.3 Das Innenministerium verwies in seiner Stellungnahme auf seine Abteilung (Vergabe), bei der bei Bedarf Nachfragen durch anfordernde Stellen jederzeit möglich seien, bzw. darauf, dass ab der vorgeschriebenen Höhe des Beschaffungsbetrags die Zentralstelle verpflichtend einzubinden sei.

Zusammenfassung Kontrollbereiche

29.1 Ein IKS soll sicherstellen, dass sich niemand in der Organisation fehlerhaft verhält, dass Prozesse eingehalten und Pflichtwidrigkeiten aufgedeckt werden können; es soll letztlich auch dazu beitragen, Spionage hintanzuhalten. Der Schutz von Vermögen und Informationen, die Ordnungsmäßigkeit und die Rechtmäßigkeit der Handlungen sollen sichergestellt werden. Prinzipien wie Funktionstrennung, Mindestinformation und Vier-Augen-Prinzip sind daraus ableitbar.

Nachstehende Tabelle gibt einen zusammenfassenden Überblick über die allgemeinen Prinzipien eines IKS mit Fokus auf die Ausprägung Spionageprävention und über ihre Umsetzung in den überprüften Bundesministerien:

Tabelle 3: Allgemeine Kontrollprinzipien des IKS bezogen auf Spionageprävention

Kontrollprinzip	Beschreibung – allgemein	Spionageprävention (beispielhaft)	BMI	BMLV	BMEIA
Funktionstrennung	keine Alleinverantwortung für den gesamten Prozess; konsequente Trennung von entscheidender, ausführender und kontrollierender Funktion	• Antrag und Vergabe Zugriffsrechte • Protokollierung der Zugriffe und Kontrolle; Auditierung der Kontrolle	x	x	x
Vier-Augen-Prinzip	Kontrollen im Prozessablauf durch Implementierung des Vier-Augen-Prinzips	• Antrag und Vergabe Zugriffsrechte	x	x	x
Kontrollautomatik	systematischer Einbau von Kontrollen im Arbeitsablauf, z.B. IT-gestützt (automatisierte Systemkontrollen)	• Kontrolle der Zugriffsrechte • Melderoutinen bei Sicherheitsvorfällen	x	x	x
Mindestinformation	Bereitstellung nur jener Informationen an Management sowie Mitarbeiterinnen und Mitarbeiter, die zur Erfüllung der Aufgaben notwendig sind	• Geheimschutz • abgestufte personenbezogene Überprüfungen	x	x	x
minimale Rechte	adäquate Beschränkung von Zugangs- und Zugriffsberechtigungen (z.B. zu IT-Systemen); Einräumung nur jener Berechtigungen zu sensiblen Daten, die zur Erfüllung der Aufgaben unbedingt erforderlich sind	• Zutrittskontrollen und Zutrittsbeschränkungen • Zugriff auf Systeme nur nach IKT-Sicherheitsbelehrung • Zugriffsrechte nach Need-to-know-Prinzip • abgestufte personenbezogene Überprüfungen	x	x	x
Transparenz und Nachvollziehbarkeit	klare, detaillierte und transparente Regelung der Arbeitsabläufe in schriftlicher Form; nachvollziehbare Dokumentation von Unterlagen und Abläufen	• Dienstvorschriften und -anweisungen	x	x	x

Quelle: RH

In den überprüften Bundesministerien waren – bezogen auf die Kontrollprinzipien – Dienstvorschriften und Dienstanweisungen, Richtlinien und Erlässe vorhanden. Ebenso waren die Erteilung und Dokumentation von Zugang zu und Zugriff auf Informationen vorhanden sowie diesbezügliche Kontrollen nachvollziehbar. Für Zutritte zu Gebäuden oder Liegenschaften bestanden Genehmigungsverfahren.

29.2 Der RH hielt fest, dass die überprüften Ressorts jeweils über ein IKS mit Elementen zur Spionageprävention verfügten. Regelungen und Maßnahmen waren in Dienstvorschriften dokumentiert, Bedienstete wurden darin unterwiesen und regelmäßig fortgebildet. In den vom RH stichprobenhaft überprüften Fällen konnten Vorbereitungshandlungen und die Einhaltung der IKS-Elemente festgestellt werden.

Der RH wies darauf hin, dass seine Feststellungen nur auf den Zeitpunkt der Überprüfung zutrafen. Eine darüber hinausgehende Beurteilung der Wirksamkeit der Kontrollmaßnahmen konnte der RH nicht vornehmen. Der RH hielt fest, dass die Überwachung der Einhaltung der Regelungen des IKS eine Management- bzw. Führungsaufgabe darstellt, die von den jeweiligen Vorgesetzten wahrzunehmen ist. Nur im Rahmen regelmäßiger Kontrollen kann das erwartete Schutzniveau aufrechterhalten werden.

Der RH empfahl daher dem Innen-, Verteidigungs- und Außenministerium, der Wahrnehmung der Management- und Führungsaufgaben – zum Erhalt des Schutzniveaus des IKS – hohe Aufmerksamkeit zu schenken.

29.3 (1) Das Innenministerium hielt in seiner Stellungnahme fest, dass den Management- und Führungsaufgaben im Bereich der Informationssicherheit hohe Aufmerksamkeit geschenkt werde. Die gesetzlich vorgesehenen Kontrollaufgaben, die auch Spionageprävention mitumfassten, nähmen die zuständigen Stellen entsprechend den rechtlichen Vorgaben wahr. Über das Risikomanagement würden Spionagerisiken und Gegenmaßnahmen in einem iterativen Prozess unter Einbeziehung der Geschäftsführung durchgeführt.

(2) Das Verteidigungsministerium hob in seiner Stellungnahme die Verbesserung der bereits bestehenden Instrumente und Prozesse im Rahmen des Innovationsprozesses des Abwehramtes hervor. Der überarbeitete Organisationsplan sehe zusätzliche, strukturierte Elemente zur Stärkung des IKS vor.

(3) Laut Stellungnahme des Außenministeriums seien im Rahmen des ISMS-Prozesses die Einbindung und Aufmerksamkeit des Managements systematisch gewährleistet. Mit der Dienstrechtsnovelle 2025 sei eine verpflichtende Führungskräfteausbildung (Management-Training) im Bundesdienst eingeführt worden. Das Außenministerium werde diese Empfehlung daher auch in diesem Rahmen umsetzen.

29.4 Der RH entgegnete dem Außenministerium, dass die von ihm angesprochene Führungskräfteausbildung (Management-Training) nicht für alle bestehenden Leitungsfunktionen galt. Die verpflichtende Führungskräfteausbildung erfasste Ernennungen oder dauernde Betrauungen frühestens ab 1. Jänner 2022 (gemäß § 284 Abs. 118 Z 6 Beamten-Dienstrechtsgesetz 1979). Der RH betonte nochmals, dass der Wahrnehmung von Management- und Führungsaufgaben im Sinne des IKS hohe Aufmerksamkeit zu schenken ist.

Interministerielle Zusammenarbeit und präventive Maßnahmen

Allgemeines

30 Die Grundlagen für die interministerielle Zusammenarbeit und den nationalen Informationsaustausch zwischen dem Innen-, dem Verteidigungs- und dem Außenministerium waren in den einschlägigen Gesetzen (z.B. SNG, Militärbefugnisgesetz, Sicherheitspolizeigesetz) definiert. Für den Austausch mit Partnerdiensten im Ausland waren § 4 Z 5 SNG und das Polizeikooperationsgesetz[63] wesentlich. Auf EU-Ebene kamen unterschiedliche Geheimschutzvorschriften und Geheimhaltungsgrade zum Tragen. Im Rahmen der Spionageprävention arbeiteten die Ressorts auf mehreren Ebenen (sicherheitspolitisch, strategisch und operativ) zusammen und tauschten Informationen aus.

Laufende Zusammenarbeit zwischen den Bundesministerien

31.1 (1) In den Bundesministerien gab es verschiedene Formate des Informationsaustauschs. Nach Angaben des Außenministeriums fand im Rahmen der innerstaatlichen Formate Nationaler Sicherheitsrat, Arbeitsgruppe Hybride Bedrohungen, Kerngruppe Desinformation sowie in den Gremien gemäß Bundes-Krisensicherheitsgesetz[64] anlassbezogen und regelmäßig ein Informationsaustausch zu Aspekten der nachrichtendienstlichen Tätigkeit fremder Staaten statt. Die Bundesministerien tauschten im „Inneren Kreis der Operativen Koordinationsstruktur“ (IKDOK)[65] für den Cyberraum spionagerelevante Informationen aus.

63 BGBl. I 104/1997 i.d.g.F.

64 BGBl. I 89/2023 i.d.g.F.

65 zu IKDOK siehe den RH-Bericht „Koordination der Cyber-Sicherheit“ (Reihe Bund 2022/13)

Spionage war zudem im Rahmen der EU ein Thema im Kontext der hybriden Bedrohungen. Für die Analyse und den Informationsaustausch unter den EU-Mitgliedstaaten war im Lagezentrum der EU[66] die „Hybrid Fusion Cell" eingerichtet. Seit 2018 fanden halbjährlich Treffen der Nationalen Kontaktpunkte der EU-Mitgliedstaaten im Rahmen der Hybrid Fusion Cell statt. Die Leitung der Abteilung II.2 im Außenministerium nahm die Funktion des Nationalen Kontaktpunkts für Österreich wahr. Für die Vor- und Nachbereitung der halbjährlichen Kontaktpunkte-Treffen tauschte das Außenministerium Informationen mit den Bundesministerien und Nachrichtendiensten aus; es koordinierte ebenso die Erstellung des österreichischen Beitrags (erstmalig 2022) zur EU Hybrid Trends Analysis. Das Innen- und das Verteidigungsministerium arbeiteten zudem in der „Kooperationsstelle der Nachrichtendienste" zusammen. In dieser waren die DSN, das Abwehramt und das Heeres-Nachrichtenamt vertreten.

(2) Für die laufende und operative Zusammenarbeit der Bundesministerien waren je nach Art bzw. Klassifizierung der Informationen unterschiedliche Organisationseinheiten (bzw. Organisationsebenen) zuständig. Die DSN, das Abwehramt und das Außenministerium hatten Prozesse definiert, die dem RH in Interviews erläutert wurden:

- Die DSN hatte Prozesse zur Informationsanalyse, -aufbereitung und -weitergabe innerhalb der DSN bzw. des Innenministeriums, zur Informationsweitergabe zum Abwehramt und Heeres-Nachrichtenamt, zu anderen Ressorts und zu Partnerdiensten im Ausland definiert (TZ 17).
- Das Abwehramt bereitete nach eigenen Angaben bei Kenntnissen aus fremden oder eigenen Ermittlungen, die eine Einbindung anderer Dienststellen bzw. Bundesministerien notwendig machten, nach Vor- und Freigabe durch die Leitungsebene entsprechende Informationen auf. Diese übermittelte es entweder schriftlich oder mündlich an die externen Bedarfsträger.
- Das Außenministerium nahm auf die Geschäftseinteilung und die darin festgelegten Agenden Bezug.

Die Bundesministerien tauschten Informationen je nach Art bzw. Klassifizierung im Wege der Amtshilfe[67], über gesicherte Datenleitungen oder persönlich aus.

Das Innen- und das Verteidigungsministerium schlossen 2010 und 2014 Verwaltungsübereinkommen über die Zusammenarbeit zwischen dem damaligen BVT, dem Abwehramt sowie dem Heeres-Nachrichtenamt. Damit sollte die Grundlage für eine

66 EU Intelligence and Situation Centre (INTCEN)

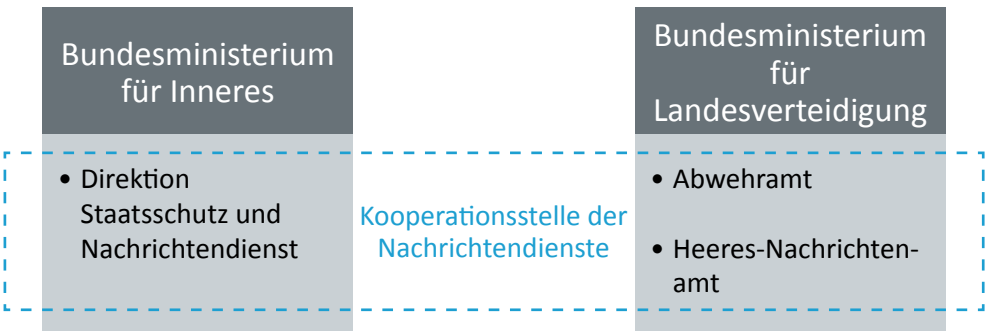
67 Art. 22 Bundes-Verfassungsgesetz

effiziente und professionelle Zusammenarbeit der drei Nachrichtendienste geschaffen werden. Gegenstand des Übereinkommens waren

- die Organisation von Fachgesprächen,
- die Koordinierung von Themen einer abgestimmten Berichtslegung,
- Informationsaustausch und Übermittlung operativer sowie analytischer Ergebnisse in den Bereichen Extremismus und Terrorismus, Nachrichtendienst, Proliferation und Cyber,
- Informationsaustausch und Übermittlung analytischer Ergebnisse zur Einschätzung von Gefährdungslagen,
- Informationsaustausch im Zusammenhang mit Verlässlichkeitsprüfungen und Sicherheitsüberprüfungen,
- der Austausch personenbezogener Informationen im Rahmen des rechtlich Zulässigen, soweit dies für die Aufgabenerfüllung erforderlich war,
- Informationsaustausch zu Strategien im internationalen Bereich,
- gemeinsame Vorbereitung und Abstimmung von Verhandlungen mit internationalen Partnern, soweit zweckmäßig,
- Informationsaustausch und Unterstützung beim Kontaktaufbau zu ausländischen Diensten,
- Informationsaustausch bei beabsichtigten Gesetzesanträgen mit sicherheits- und nachrichtendienstlichem Bezug.

Diese Zusammenarbeit nahm u.a. die „Kooperationsstelle der Nachrichtendienste“ wahr. Die Kooperationsstelle bestand aus einem Executive Board (Direktoren bzw. Leiter der Nachrichtendienste), dem Senior Board (leitende Bedienstete) und einer fixen Personeneinteilung. Der Vorsitz rotierte alle sechs Monate. Im Jahr 2021 unterzeichneten die Leiter des damaligen BVT, des Abwehramtes sowie des Heeres-Nachrichtenamtes einen Letter of Intent.

Abbildung 8: Zusammenarbeit der Nachrichtendienste



Quellen: BMI; BMLV; Darstellung: RH

(3) In Österreich – insbesondere in Wien – haben zahlreiche diplomatische Vertretungen sowie internationale Organisationen ihren Sitz. Das Wiener Übereinkommen regelt die Rahmenbedingungen für die diplomatischen Beziehungen zwischen Staaten. Vorbehaltlich der Art. 5, 8, 9 und 11 des Wiener Übereinkommens konnte der Entsendestaat die Mitglieder des Personals seiner Mission nach freiem Ermessen ernennen.[68]

Das Außenministerium befasste die relevanten Bundesministerien und Nachrichtendienste u.a. in allen Agrémentverfahren[69] – diese betrafen bilaterale Botschafterinnen und Botschafter und Militärattachés – sowie in einigen Fällen vor der Erteilung von Dienstantrittsvisa für andere Personen. Die DSN erhielt vom Außenministerium auf Anfrage Daten über einzelne in Österreich akkreditierte Diplomatinnen und Diplomaten, deren Angehörige, sonstige Missionsangehörige sowie Mitarbeiterinnen und Mitarbeiter internationaler Organisationen oder Personengruppen.

Die folgende Tabelle gibt die Anzahl des in Österreich akkreditierten diplomatischen Personals (sogenannte Hauptberechtigte) bei wesentlichen Einrichtungen mit Stand 1. März 2025 wieder, gegliedert nach wesentlichen Personengruppen; nicht enthalten sind weitere 3.776 Familienangehörige der Hauptberechtigten, sogenannte Nebenberechtigte:

Tabelle 4: Diplomatisches Personal in Österreich

Einrichtungen	Diplomatinnen und Diplomaten	technisch-administratives Personal	Hauspersonal	Summe
	Anzahl zum 1. März 2025			
Botschaften	1.363	340	66	**1.769**
Ständige Vertretungen	350	71	9	**430**
Generalkonsulate	2[1]	11	2	**15**
Ständige Vertretungen bei der OSZE Wien	179	18	1	**198**
internationale Organisationen in Wien	170	1.481	3	**1.654**
Ständige Beobachtermissionen bei den internationalen Organisationen in Wien	51	12	1	**64**
Sonderorganisationen der Vereinten Nationen in Wien	512	3.543[2]	14	**4.069**
Summe	**2.627**	**5.476**	**96**	**8.199**

OSZE = Organisation für Sicherheit und Zusammenarbeit in Europa Quelle: BMEIA

[1] zusätzlich 32 Berufskonsuln
[2] Davon umfasst sind alle Bediensteten internationaler Organisationen in Wien, die nicht in leitender Funktion tätig sind.

[68] Allerdings konnte gemäß Art. 11 des Wiener Übereinkommens bei Fehlen einer ausdrücklichen Vereinbarung über den Personalbestand der Mission der Empfangsstaat verlangen, dass dieser Personalbestand in jenen Grenzen gehalten wird, die er in Anbetracht der bei ihm vorliegenden Umstände und Verhältnisse sowie der Bedürfnisse der Mission für angemessen und normal hält.

[69] Agrément bezeichnet die völkerrechtliche Zustimmung des Empfangsstaates, Vertreterinnen und Vertreter des Entsendestaates für eine diplomatische oder sonstige Mission zu empfangen.

Nach Art. 9 des Wiener Übereinkommens konnte ein Empfangsstaat dem Entsendestaat jederzeit ohne Angabe von Gründen notifizieren, dass der Missionschef oder ein Mitglied des diplomatischen Personals der Mission persona non grata war oder dass ein anderes Mitglied des Personals der Mission ihm nicht genehm war. In diesen Fällen hatte der Entsendestaat die betreffende Person entweder abzuberufen oder ihre Tätigkeit bei der Mission zu beenden. Eine Person konnte als non grata oder nicht genehm erklärt werden, bevor sie im Hoheitsgebiet des Empfangsstaats eintraf.

Sachverhalte und Informationen, die zu einer Ausweisung führen konnten, übermittelten der Direktor der DSN sowie der Leiter des Abwehramtes nach übereinstimmenden Angaben der Bundesministerien ausschließlich persönlich und mündlich den zuständigen Personen im Außenministerium. Schriftliche Unterlagen dazu übermittelten sie grundsätzlich nicht. Das Außenministerium gab an, dass – sobald Hinweise auf nicht mit dem Wiener Übereinkommen vereinbare nachrichtendienstliche Tätigkeiten vorgelegt wurden – diese mit den betroffenen Bundesministerien und Nachrichtendiensten erläutert und geprüft wurden. Waren ausreichend Hinweise für ein Fehlverhalten einer Diplomatin bzw. eines Diplomaten vorhanden, wurde nach Beteiligung aller betroffenen Bundesministerien über etwaige Ausweisungen entschieden. Im Falle multilateral akkreditierter Diplomatinnen und Diplomaten erfolgte die im jeweiligen Amtssitzabkommen vorgesehene Konsultation mit der betroffenen internationalen Organisation.

Österreich erklärte seit Beginn des Krieges in der Ukraine im Februar 2022 elf Personen zu personae non gratae und wies sie aus. Dies betraf ausschließlich diplomatisches Personal der Russischen Föderation. Innerhalb der EU[70] lag Österreich mit dieser Zahl im hinteren Feld.

(4) Im Zuge der Gebarungsüberprüfung durch den RH bewerteten die Bundesministerien die übergreifende Zusammenarbeit und den Informationsaustausch als positiv und gut funktionierend. Nach Angaben der DSN waren aber teils widerstrebende Interessenslagen im Hinblick auf Ausweisungen diplomatischen Personals erkennbar.

31.2 Der RH erachtete die Zusammenarbeit und den Informationsaustausch zwischen den Bundesministerien und auf EU-Ebene als wesentlich für eine effektive und effiziente Spionageprävention. In diesem Sinne hielt er es für zweckmäßig, dass das Innen-, das Verteidigungs- und das Außenministerium auf sicherheitspolitischer, strategischer und operativer Ebene zusammenarbeiteten und relevante Informationen austauschten. Die zwischen den Nachrichtendiensten auf Basis des Verwaltungsübereinkommens eingerichtete „Kooperationsstelle der Nachrichtendienste“

[70] Tschechien wies z.B. im Jahr 2021 18 Staatsangehörige der Russischen Föderation mit diplomatischem Status aus.

sowie deren Zusammenarbeit auf multinationaler, operativer, technischer und rechtlicher Ebene wertete er positiv.

Im Hinblick auf geopolitische Entwicklungen und Gefährdungslagen war ein abgestimmtes, von gesamtstaatlichen Interessen getragenes Vorgehen der Bundesministerien bei nachrichtendienstlichen Tätigkeiten fremder Staaten erforderlich. Treffsichere Maßnahmen, z.B. Ausweisungen und eine effektive Zusammenarbeit, waren geeignet, einen generalpräventiven Nutzen zu erzielen.

In diesem Zusammenhang hielt der RH fest, dass das Innen-, das Verteidigungs- und das Außenministerium die interministerielle Zusammenarbeit als positiv und gut funktionierend darstellten. Er wies allerdings auf mögliche widerstrebende Interessenslagen der Ressorts hin.

31.3 Das Außenministerium führte in seiner Stellungnahme aus, dass die Erklärung zur persona non grata nur in beschränktem Maße als Präventionsmaßnahme einsetzbar sei. Sie diene vor allem als Sanktion (ultima ratio) bei bereits festgestelltem rechtswidrigem Verhalten von Diplomatinnen und Diplomaten, darunter auch Spionagetätigkeiten. Präventiv würden hingegen Maßnahmen wie die Verweigerung der Einreise bzw. der Akkreditierung von Diplomatinnen und Diplomaten wirken, von denen aufgrund nachrichtendienstlicher Erkenntnisse erwartet werden könne, dass sie nach Dienstantritt in Österreich rechtswidrigen Tätigkeiten (z.B. Spionage) nachgingen. Diese Maßnahme werde, auf Basis der Erkenntnis von und in enger Abstimmung mit den Nachrichtendiensten, in mehreren Dutzend Fällen jährlich eingesetzt. Auch die formelle Vorladung von Missionschefinnen und -chefs zur Klarstellung der Rechtslage könne als Präventivmaßnahme eingesetzt werden.

31.4 Der RH teilte grundsätzlich die Einschätzung des Außenministeriums, hielt jedoch fest, dass auch die Erklärung zur persona non grata eine präventive Wirkung in anderen Staaten entfalten konnte.

Ressortübergreifende präventive Maßnahmen

32.1 Prävention ist kein klar definierter Begriff, unterschiedliche Maßnahmen konnten präventiven Charakter haben. Innerhalb der Bundesministerien trugen u.a. Maßnahmen des IKS, die Schulung der Bediensteten sowie technische Sicherheitsvorkehrungen zur Spionageprävention bei. Ressortübergreifend hatte die DSN nach §§ 7 und 8 Abs. 2 SNG die Aufgabe, verfassungsschutzrelevante (d.h. Staatsschutz und Nachrichtendienst betreffende) Beratungen vorzunehmen und die obersten Organe der Vollziehung zu unterrichten.

Das Abwehramt hielt Sensibilisierungsvorträge in den Generalsekretariaten der Bundesministerien im Jahr 2023 sowie im Rahmen der „Kooperationsstelle der Nachrichtendienste“. Die Vorträge beinhalteten Länder und deren wichtigste Nachrichtendienste, die eine Bedrohung im Phänomenbereich Spionage für Österreich darstellten, sowie die Beschreibung ihrer Methoden zur Informationsbeschaffung anhand praktischer Fallbeispiele.

32.2 Der RH erachtete die Sensibilisierung der Bediensteten in den Bundesministerien, vor allem der Funktions- und Entscheidungsträgerinnen und -träger, als wesentliche Präventionsmaßnahme. Er hielt fest, dass die DSN und das Abwehramt durch ressortübergreifende Beratungen und Sensibilisierungsmaßnahmen zur Spionageprävention beitrugen.

Fragenbeantwortung

33 Der RH überprüfte gemäß Art. 126b Abs. 4 Bundes-Verfassungsgesetz aufgrund eines Antrags gemäß § 99 Abs. 2 Geschäftsordnungsgesetz 1975 des Abgeordneten Douglas Hoyos-Trauttmansdorff und weiterer Abgeordneter vom 15. Mai 2024 (4017/A BlgNR 27. GP) die Gebarung des Innenministeriums, des Verteidigungsministeriums sowie des Außenministeriums hinsichtlich des Präventionsmechanismus, um Spionagevorfälle zu verhindern. Das Verlangen zur Durchführung der Gebarungsüberprüfung umfasste einen Katalog von sechs Fragen, deren Beantwortung die Überprüfung insbesondere umfassen sollte:

1.a. Welche internen Kontrollsysteme bestehen im jeweiligen Ministerium, um Spionage zu verhindern und etwaige Spionagenetzwerke zu identifizieren – einerseits rechtlich?

(1) (a) Im Innenministerium waren Gefahrenerforschung und -abwehr im Bereich Spionage von Anfang 2017 bis Ende November 2021 im damaligen BVT angesiedelt. Mit Einrichtung der DSN mit Dezember 2021 gingen die Aufgaben auf diese über. Die DSN war in die Bereiche Staatsschutz und Nachrichtendienst getrennt. (TZ 6)

Der Bereich Staatsschutz umfasste insbesondere den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen, Fallkonferenzen sowie sicherheits- und kriminalpolizeiliche Aufgaben im Zusammenhang mit verfassungsgefährdenden Angriffen[71]. (TZ 6)

Der Bereich Nachrichtendienst diente der erweiterten Gefahrenerforschung (§ 6 Abs. 1 SNG) sowie der Gewinnung und Analyse von Informationen hinsichtlich der Zwecke des Verfassungsschutzes (§ 8 Abs. 1 SNG) und somit insbesondere der Spionageabwehr und -prävention. (TZ 6)

Eine weitere zentrale Aufgabe lag im Bereich der Prävention, sohin der Koordination, Steuerung und Förderung der gesamtstaatlichen Zusammenarbeit. Dies umfasste die Erarbeitung von Strategien und Handlungsempfehlungen sowie die Koordination und Durchführung von entsprechenden Maßnahmen. Zudem sollten Nachrichtendienste im regelmäßigen Kommunikations- und Informationsaustausch mit anderen Diensten stehen und mit sicherheitsrelevanten Akteuren, jeweils im In- und Ausland, kooperieren. Zum Aufgabenbereich gehörte auch der besondere Schutz von sensiblen Informationen und Geheimnissen, Cyber-Sicherheit sowie die Abwehr von Cyber-Spionage[72]. (TZ 6)

[71] Die Aufgaben der Gefahrenabwehr und die damit verbundenen Befugnisse waren im Sicherheitspolizeigesetz geregelt, sofern das SNG nichts Besonderes regelte (§ 5 SNG).

[72] vgl. https://www.dsn.gv.at/104/ (abgerufen am 5. März 2025)

Mit Maßnahmen im Bereich der Spionageprävention waren zudem zahlreiche Organisationseinheiten in der Zentralstelle des Innenministeriums betraut, weiters die Sicherheitsakademie, die Unabhängige Kontrollkommission Verfassungsschutz[73], der Rechtsschutzbeauftragte und auf Ebene der Landespolizeidirektionen die Landesämter Staatsschutz und Extremismusbekämpfung. (TZ 6)

(b) Das Innenministerium hatte keine zentralen Vorgaben an ein IKS. Die Umsetzung eines geeigneten IKS oblag jeder Organisationseinheit für den ihr zugewiesenen Aufgabenbereich. (TZ 14)

Vor dem 1. Dezember 2021 nahm die Aufgaben des Verfassungsschutzes das BVT wahr. Es war bis 2018 in vier, danach in sechs Abteilungen ohne Trennung von Staatsschutz und Nachrichtendienst gegliedert. Die Direktorin bzw. der Direktor des BVT war gleichzeitig die bzw. der Informationssicherheitsbeauftragte des Innenministeriums. Nach dem 1. Oktober 2018 war das Referat „Interne Sicherheit" bei der stellvertretenden Direktorin bzw. beim stellvertretenden Direktor angesiedelt. Daneben waren noch zwei Abteilungen mit Aufgaben im Geheimschutz betraut. Aufgaben im IKS zum Geheimschutz waren in der DSN in der Direktion im Rechtsbüro und im Büro „Interne Sicherheit" angesiedelt. Die Leitung des Rechtsbüros war gleichzeitig die bzw. der Informationssicherheitsbeauftragte des Innenministeriums. Sie bzw. er nahm an Sitzungen der Informationssicherheitskommission teil und gestaltete Schulungsunterlagen sowie Leitlinien. Das Büro „Interne Sicherheit" führte Kontrollen und Durchsuchungen sowie die Vertrauenswürdigkeitsprüfungen von Bediensteten der DSN operativ durch. (TZ 14)

(2) (a) Im Verteidigungsministerium waren das Abwehramt und das Heeres-Nachrichtenamt auf Grundlage des § 20 Militärbefugnisgesetz für die nachrichtendienstliche Aufklärung und Abwehr eingerichtet. (TZ 6)

Das Abwehramt war zuständig für die Abwehr von Gefahren für die militärische Sicherheit sowohl im Inland als auch von zu Auslandseinsätzen entsandten Kontingenten. Es sammelte Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen Leben und Gesundheit von Personen, gegen Infrastruktur und militärisch klassifizierte Informationen erwarten ließen. Durch das vorzeitige Erkennen sollten entsprechende Straftaten verhindert werden. (TZ 6)

Das Heeres-Nachrichtenamt war zuständig für die strategische Auslandsaufklärung. Seine Bediensteten beschafften Informationen über Regionen, Staaten und Organisationen, die für die österreichische und europäische Sicherheitspolitik relevant

[73] Die Unabhängige Kontrollkommission Verfassungsschutz war ein gemäß Art. 20 Abs. 2 Z 2 Bundes-Verfassungsgesetz unabhängiges und weisungsfreies Organ der Verwaltung im Rahmen ihrer Aufgaben. Gemäß § 17a SNG war sie seit ihrer Einsetzung u.a. mit der begleitenden strukturellen Kontrolle der DSN und der Landesämter Staatsschutz und Extremismusbekämpfung betraut, um insbesondere systemische Mängel und Optimierungsbedarf der Organisationen aufzuzeigen.

waren. Diese Informationen wurden analysiert und in Form von Berichten und Präsentationen als Entscheidungsgrundlage für die Führung aufbereitet. (TZ 6)

(b) Das IKS für den Bereich Spionageprävention war in der Organisation des Verteidigungsministeriums den Angelegenheiten der militärischen Sicherheit und der bzw. des Sicherheits- und Informationssicherheitsbeauftragten der nachrichtendienstlichen Abwehr zugewiesen. Der Leiter des Abwehramtes nahm die Aufgaben des Sicherheits- und Informationssicherheitsbeauftragten wahr. Ebenso war er in der Funktion der nachrichtendienstlichen Abwehr ressortweit zuständig. Die Verantwortung für Regelungen des IKS für Spionageprävention war bei der nachrichtendienstlichen Abwehr zentralisiert. Die Aufgaben umfassten den Schutz militärischer Rechtsgüter. (TZ 14)

(3) (a) Im Außenministerium wirkten mehrere Organisationseinheiten an der Spionageprävention mit. Das Außenministerium befasste die relevanten Bundesministerien und Nachrichtendienste u.a. in allen Agrémentverfahren[74] – diese betrafen bilaterale Botschafterinnen und Botschafter und Militärattachés – sowie in einigen Fällen vor der Erteilung von Dienstantrittsvisa für andere Personen. Es war darüber hinaus auf Grundlage des Art. 9 des Wiener Übereinkommens berechtigt, ohne Angabe von Gründen Diplomatinnen und Diplomaten zur unerwünschten Person (persona non grata) zu erklären und sie aufzufordern, das Land zu verlassen. (TZ 6)

(b) Im Außenministerium bestand gemäß Geschäftseinteilung keine spezifische IKS-Zuständigkeit betreffend Spionageprävention. Die Umsetzung von IKS-Maßnahmen erfolgte in jeder Organisationseinheit. Es existierten interne Vorgaben und Dokumente, die Teil des IKS waren und mehrere Abteilungen umfassten. (TZ 14)

1.b. Welche internen Kontrollsysteme bestehen im jeweiligen Ministerium, um Spionage zu verhindern und etwaige Spionagenetzwerke zu identifizieren – andererseits auf Ebene der IT-Infrastruktur?

(1) Im Innenministerium bestanden schriftliche Vorgaben betreffend den Zutritt zu den Standorten oder zu spezifischen Räumlichkeiten des Innenministeriums gesamt, einzelner Abteilungen oder spezifisch für die DSN. Bei Besuchen Externer regelten sie z.B. die Vergabe von Zutrittsberechtigungen für Wartungstätigkeiten im Zusammenhang mit IT-Services und IT-Produkten, den Umfang der Sicherheitsüberprüfung der Mitarbeiterinnen und Mitarbeiter externer Dienstleister und den Umgang mit Externen beim Zutritt und während ihrer Anwesenheit in der DSN. Ressortfremden war die Einfahrt in die DSN-Liegenschaft verboten. (TZ 25)

[74] Agrément bezeichnet die völkerrechtliche Zustimmung des Empfangsstaates, Vertreterinnen und Vertreter des Entsendestaates für eine diplomatische oder sonstige Mission zu empfangen.

Eine interne Dienstanweisung der DSN regelte die Erstellung von Informationen für die Ressortleitung sowie für die Generaldirektion für die öffentliche Sicherheit und legte entsprechende Prozesse fest. Die Informationen durften für die Ressortleitung keine klassifizierten Dokumente und für die Generaldirektion für die öffentliche Sicherheit nur Dokumente bis zur Klassifizierungsstufe „EINGESCHRÄNKT" enthalten. In beiden Fällen gab die Direktorin bzw. der Direktor der DSN die Informationsweitergabe frei. (TZ 17)

Das Innenministerium verfügte über schriftliche Vorgaben zur Vergabe bzw. Handhabung von Zugriffsrechten, die entweder für das Innenministerium gesamt, für einzelne Abteilungen oder spezifisch für die DSN galten. Die DSN regelte außerdem für die eigenen Anwendungen und Laufwerke die Grundlagen und Prozesse zur Vergabe und zum Entzug von Zugriffsberechtigungen für unterschiedliche dienstliche Szenarien (z.B. Eintritt, Austritt, Dienstzuteilung). (TZ 17)

Benutzerrechte waren nach dem Need-to-know-Prinzip zu vergeben. Bei der Beantragung und Vergabe der Zugriffsrechte für Bedienstete der DSN waren das Vier-Augen-Prinzip einzuhalten und gegebenenfalls weitere IKS-Maßnahmen vorgesehen (zusätzliche Faktoren, Einbindung weiterer Stellen, kein Kopieren und Übernehmen von Zugriffsrechten). Verantwortlichkeiten für die Kontrolle der Zugriffsrechte und um deren Aktualität sicherzustellen, waren festgelegt. (TZ 17)

Neben der technischen Beschränkung der Zugriffsmöglichkeiten sahen das Innenministerium und die DSN auch Sensibilisierungsgespräche zum sicheren Umgang mit den IT-Systemen sowie Melderoutinen bei Gefährdung für die Integrität der IT-Infrastruktur vor. Dokumente ab der Klassifizierungsstufe „VERTRAULICH" durften nur auf Geräten ohne externe Vernetzung verarbeitet werden. Führungskräfte waren für die Einhaltung der IT-Sicherheitsrichtlinien verantwortlich. Zur Absicherung des IT-Sicherheitsniveaus im Innenministerium legte dieses darüber hinaus im Rahmen einer „Sicherheitsorganisationsstruktur" für ausgewählte Bedienstete spezifische Verantwortlichkeiten fest, z.B. als IT-Sicherheitsbeauftragte oder IT-Sicherheitsvertrauenspersonen. Es bestanden außerdem Regelungen zur Verwendung von wechselbaren Datenträgern (z.B. USB-Sticks) allgemein und zur Beschränkung von Transfer, Transport und Verarbeitung klassifizierter Daten auf Datenträgern im Speziellen. (TZ 17)

(2) Im Verteidigungsministerium bestanden für den Objektschutz schriftliche Vorgaben, die den Zutritt zu den Liegenschaften, zu spezifischen Gebäuden oder einzelnen Anlagen regelten. Besondere Vorschriften gab es für die nachrichtendienstlich genutzten Objekte. Die Regelungen verfolgten das Ziel, den Schutz militärischer Rechtsgüter bereits im täglichen Betrieb, ohne zusätzliche Absicherungsmaßnahmen, sicherzustellen. Besondere Anforderungen betrafen abhörsichere und abhör-

geschützte Bereiche, in denen Besprechungen über klassifizierte Unterlagen stattfinden durften. (TZ 25)

Der Zutritt zum Abwehramt war grundsätzlich nur aus dienstlichen Gründen zulässig und bedurfte einer Genehmigung durch einen (zahlenmäßig engen) Kreis von Genehmigungsberechtigten. Die Zutritte waren zu protokollieren, elektronische Geräte (z.B. Mobiltelefone, Smartwatches, Laptops) von ressortfremden Personen versperrt zu deponieren und ausgegebene Erkennungszeichen sichtbar zu tragen. (TZ 25)

Im Verteidigungsministerium bestanden schriftliche Vorgaben zur Vergabe bzw. Handhabung von Zugriffsrechten, die entweder für das Verteidigungsministerium gesamt, für einzelne Abteilungen oder spezifisch für das Abwehramt galten. (TZ 17)

Die Büroordnung des Abwehramtes regelte den Umgang mit elektronischen Akten und Papierakten. Die Verwaltung von Akten und die Speicherung von nachrichtendienstlichen (operativen) Daten waren voneinander getrennt und erfolgten in unterschiedlichen Systemen. Die Vergabe von Rechten dafür hatte durch den Leiter des Abwehramtes (mit eingeschränkter Delegationsmöglichkeit) nach dem Need-to-know-Prinzip zu erfolgen. Im System wurden die Zugriffe auf einzelne Datensätze technisch protokolliert. (TZ 17)

Im Netzwerk des Abwehramtes war eine Verarbeitung von klassifizierten Informationen bis zur Stufe „GEHEIM“ möglich. Das Abwehramt verfügte über einen vom Verteidigungsministerium getrennten ELAK. (TZ 17)

Im Abwehramt standen technische Lösungen für die Sprachkommunikation über klassifizierte Informationen zur Verfügung. Beispielsweise konnten Informationen der Stufe „EINGESCHRÄNKT“ über eine zugelassene Lösung mit administrierten Mobiltelefonen besprochen werden. (TZ 17)

Eine eigene Regelung bestand für die Vorlage von Geschäftsstücken an die Ressortleitung, das Kabinett und das Generalsekretariat. Die Vorlage erfolgte grundsätzlich im Wege der Generalstabsabteilung oder unter gleichzeitiger Information des Chefs des Generalstabes. (TZ 17)

(3) Im Außenministerium wurden technische bzw. bauliche Schutzmaßnahmen und Kontrollsysteme ergänzt durch Regelungen zum Zutritt nur für sicherheitsüberprüftes Personal (weiter eingeschränkt beispielsweise für besonders sensible Bereiche wie den Serverraum), zur Verwendung elektronischer Zutrittssysteme in der Zentralstelle sowie zum verpflichtenden Führen von Schlüsselvormerken. (TZ 25)

Mitarbeiterinnen und Mitarbeiter externer Dienstleister, die Zutritt für Standorte oder Dienste des Außenministeriums benötigten, wurden entweder gemäß §§ 55 f. Sicherheitspolizeigesetz sicherheitsüberprüft oder von sicherheitsüberprüften Personen begleitet. (TZ 25)

Um eine sichere Kommunikation im Zusammenhang mit Informationen zu eingeschränkten Inhalten (inklusive Klassifizierungsstufe „EINGESCHRÄNKT“) gewährleisten zu können, gab es im Außenministerium Vorgaben und Dienstanweisungen. Das Außenministerium verfügte über technische Möglichkeiten, um auch telefonisch über Informationen zu eingeschränkten Inhalten kommunizieren zu können. (TZ 17)

2. Wie konkret haben sich die Ausschreibungsverfahren im Zusammenhang mit den IT-Infrastrukturen und deren Sicherung innerhalb der Ministerien gestaltet und wurde tatsächlich die zweckdienstliche IT-Infrastruktur im Sinne der Budgeteffizienz und Zweckdienlichkeit ausgewählt?

(1) Für öffentliche Auftragsvergaben war das Bundesvergabegesetz oder das Bundesvergabegesetz Verteidigung und Sicherheit 2012 anzuwenden. Letzteres sah aufgrund der im Verteidigungs- und Sicherheitsbereich erhöhten Geheimhaltungs- und Versorgungsinteressen besondere Regelungen zur Informations- und Versorgungssicherheit vor. Beide Vergabegesetze enthielten Ausnahmen, etwa zu Aufträgen, auf die die Ausnahmebestimmung in Art. 346 AEUV Anwendung fand. (TZ 27)

Folgende Tabelle zeigt die Aufteilung der Auftragsabwicklung der von den drei überprüften Ministerien im Zeitraum 2017 bis 2024 beschafften IT-Sicherheitsinfrastruktur und wie viel sie anteilsmäßig über die BBG bzw. selbst beschafften:

Beschaffungen IT-Sicherheitsinfrastruktur in den drei überprüften Ministerien; 2017 bis 2024

	Einbeziehung der BBG	durch das Ministerium selbst	BVergGVS und Ausnahmen zu Vergabegesetzen
	Abwicklung des Auftragsvolumens		
	in %		
Innenministerium (für DSN)	58	42	0
Verteidigungsministerium (für Abwehramt)	89	2	9
Außenministerium	70	14	16

BBG = Bundesbeschaffung GmbH
BVergGVS = Bundesvergabegesetz Verteidigung und Sicherheit 2012

Quellen: BMI; BMLV; BMEIA; Auswertung: RH

(2) Bei der Vergabe der Leistungen zum Hochsicherheitsnetzwerk der DSN berief sich das Innenministerium auf die Ausnahmen des Art. 346 AEUV bzw. des § 9 Abs. 1 Z 5 Bundesvergabegesetz Verteidigung und Sicherheit 2012; die Vergabe erfolgte sohin außerhalb des Vergaberechts. Die Auswahl fiel auf ein Unternehmen, das aufgrund seiner bisherigen Tätigkeiten über eingehende Kenntnisse der österreichischen Verwaltung und insbesondere auch des Innenministeriums verfügte. Die Gesamtkosten für die Beschaffung betrugen 1,25 Mio. EUR. (TZ 27)

Im Juni 2022 berichtete eine deutsche Mediengesellschaft über die Beauftragungen durch das Innenministerium im Zusammenhang mit einem IKT-Projekt für die DSN, über Verbindungen des beauftragten Unternehmens zu einem ehemaligen Geschäftsführer eines deutschen Zahlungsdienstleisters sowie über mögliche, damit zusammenhängende Verbindungen zur Russischen Föderation. (TZ 27)

Infolge dieser Berichterstattung nahm die DSN von der Umsetzung des Hochsicherheitsnetzwerks durch externe Unternehmen Abstand. Das Konzept des externen Unternehmens kam nicht zur Anwendung. Potenzielle Auswirkungen der medialen Vorhalte auf andere Projekte des Unternehmens für die Republik Österreich untersuchte weder das Innenministerium noch die DSN. (TZ 27)

(3) Im Innenministerium war für Beschaffungen ein Standardprozess etabliert. Je nach Leistungsgegenstand waren definierte Abteilungen zentral zuständig. Wenn die DSN als Bedarfsträger es z.B. aus Gründen der Informationssicherheit für notwendig erachtete, konnte sie Vergaben auch selbst, d.h. ohne Einbindung von Stellen außerhalb der DSN, durchführen. Das Bundesvergabegesetz 2018 und das Bundesvergabegesetz Verteidigung und Sicherheit 2012 sahen Ausnahmen für Beschaffungen im Sicherheitsbereich bzw. für Zwecke nachrichtendienstlicher Tätigkeiten vor.[75] Die DSN orientierte sich bei den Beschaffungen nach eigenen Angaben an international (in Nachrichtendiensten) bewährten Vorgehensweisen. Sie griff bei der Vorselektion der Hersteller bzw. Lieferanten und Produkte auf nachrichtendienstliche Erkenntnisse, Umfeldanalysen sowie Marktforschung in offenen Quellen zum Renommee der Produkte und der Hersteller bzw. Lieferanten zurück. Eine darüber hinausgehende (verpflichtende) Überprüfung der Unternehmen war rechtlich nicht vorgesehen bzw. möglich. Relevante Personen konnten sicherheitsüberprüft werden, wenn sie Zugang zu klassifizierten Informationen erhalten sollten. Das Thema „Lieferkette technischen Equipments“ war im internen Risikomanagement der DSN berücksichtigt. (TZ 28)

(4) Im Verteidigungsministerium fielen Beschaffungen für die militärischen Nachrichtendienste in den Aufgabenbereich der Vergabeabteilung. Die Zuordnung von Beschaffungen (IT-Beschaffungen) zu Zwecken der Spionageprävention war nicht

[75] insbesondere § 9 Abs. 1 Z 1, 4 und 5 Bundesvergabegesetz 2018 und § 9 Abs. 1 Z 5 und 6 Bundesvergabegesetz Verteidigung und Sicherheit 2012

möglich, weil die Bedarfsbegründungen der antragstellenden Organisationseinheiten keine Rückschlüsse darauf zuließen. Nachrichtendienstliche Anforderungen waren bereits bei der Einleitung von Beschaffungsvorgängen zu berücksichtigen. (TZ 28)

Im Bereich der nachrichtendienstlichen Abwehr führte das Abwehramt Beschaffungen in geringem Umfang durch, die der Informationsgewinnung, dem Eigenschutz sowie der Abwehr von Gefahren zuzurechnen waren. So beschaffte das Abwehramt beispielsweise Abhörschutzboxen für mobile Telefone. (TZ 28)

(5) Das Außenministerium beschaffte IT-Leistungen vorrangig über die BBG. Ministeriumsintern gab es darüber hinaus Vorgaben für Beschaffungen im Wege der Direktvergabe sowie zur Kerndatenmeldung vergebener Aufträge gemäß §§ 61 ff. Bundesvergabegesetz 2018. Diese Vorgaben wiesen auf Ausnahmen von der Bekanntgabeverpflichtung hin und die Abteilung VI.6 sensibilisierte anlassbezogen in Vergabeprozessen hinsichtlich der Ausnahme zur Bekanntgabe „bestimmter Angaben". Bei Auftragswerten oberhalb der Direktvergabegrenze war jedenfalls die Sektion VI zu befassen. (TZ 28)

Der für einen konkreten IT-Beschaffungsvorgang zuständigen Organisationseinheit oblag die Erstbeurteilung, ob Aspekte der Spionageabwehr bzw. -prävention vorlagen. In Abstimmung mit den zuständigen Fachabteilungen war sodann eine vergaberechtlich zulässige Vorgangsweise zu erarbeiten. (TZ 28)

Vor Einleitung einer IT-Beschaffung waren bestehende bzw. anlassbezogen erstellte Sicherheitskonzepte Grundlage für die Leistungsdefinition. Risikomanagement, das Erkennen von IT-Sicherheitsrisiken sowie die Beachtung von allfällig verbleibenden Restrisiken erfolgten bei Bedarf in Abstimmung mit den entsprechenden Organisationen. Bei Bedarf wurden Beschaffungen bzw. deren Konzepte auch einem Penetrationstest durch unabhängige externe Unternehmen unterzogen. (TZ 28)

3. Sind die internen Kontrollsysteme ausreichend, um den gewünschten Zweck zu erfüllen?

Ein IKS soll sicherstellen, dass sich niemand in der Organisation fehlerhaft verhält und dass Prozesse eingehalten werden; es soll letztlich auch dazu beitragen, Spionage hintanzuhalten. Der Schutz des Vermögens und von Informationen, die Ordnungsmäßigkeit und die Rechtmäßigkeit der Handlungen sollen sichergestellt werden. Prinzipien wie Funktionstrennung, Mindestinformation und Vier-Augen-Prinzip sind daraus ableitbar.

Nachstehende Tabelle gibt einen zusammenfassenden Überblick über die allgemeinen Prinzipien eines IKS mit Fokus auf die Ausprägung Spionageprävention und über ihre Umsetzung in den überprüften Bundesministerien:

Allgemeine Kontrollprinzipien des IKS bezogen auf Spionageprävention

Kontrollprinzip	Beschreibung – allgemein	Spionageprävention (beispielhaft)	BMI	BMLV	BMEIA
Funktionstrennung	keine Alleinverantwortung für den gesamten Prozess; konsequente Trennung von entscheidender, ausführender und kontrollierender Funktion	• Antrag und Vergabe Zugriffsrechte • Protokollierung der Zugriffe und Kontrolle; Auditierung der Kontrolle	x	x	x
Vier-Augen-Prinzip	Kontrollen im Prozessablauf durch Implementierung des Vier-Augen-Prinzips	• Antrag und Vergabe Zugriffsrechte	x	x	x
Kontrollautomatik	systematischer Einbau von Kontrollen im Arbeitsablauf, z.B. IT-gestützt (automatisierte Systemkontrollen)	• Kontrolle der Zugriffsrechte • Melderoutinen bei Sicherheitsvorfällen	x	x	x
Mindestinformation	Bereitstellung nur jener Informationen an Management sowie Mitarbeiterinnen und Mitarbeiter, die zur Erfüllung der Aufgaben notwendig sind	• Geheimschutz • abgestufte personenbezogene Überprüfungen	x	x	x
minimale Rechte	adäquate Beschränkung von Zugangs- und Zugriffsberechtigungen (z.B. zu IT-Systemen); Einräumung nur jener Berechtigungen zu sensiblen Daten, die zur Erfüllung der Aufgaben unbedingt erforderlich sind	• Zutrittskontrollen und Zutrittsbeschränkungen • Zugriff auf Systeme nur nach IKT-Sicherheitsbelehrung • Zugriffsrechte nach Need-to-know-Prinzip • abgestufte personenbezogene Überprüfungen	x	x	x
Transparenz und Nachvollziehbarkeit	klare, detaillierte und transparente Regelung der Arbeitsabläufe in schriftlicher Form; nachvollziehbare Dokumentation von Unterlagen und Abläufen	• Dienstvorschriften und -anweisungen	x	x	x

Quelle: RH

In den überprüften Bundesministerien waren – bezogen auf die Kontrollprinzipien – Dienstvorschriften und Dienstanweisungen, Richtlinien und Erlässe vorhanden. Ebenso waren die Erteilung und Dokumentation von Zugang zu und Zugriff auf Informationen vorhanden sowie diesbezügliche Kontrollen nachvollziehbar. Für Zutritte zu Gebäuden oder Liegenschaften bestanden Genehmigungsverfahren. (TZ 29)

Die überprüften Bundesministerien verfügten jeweils über ein IKS mit Elementen zur Spionageprävention. Regelungen und Maßnahmen waren in Dienstvorschriften dokumentiert, Bedienstete wurden darin unterwiesen und regelmäßig fortgebildet.

In den vom RH stichprobenhaft überprüften Fällen konnten Vorbereitungshandlungen und die Einhaltung der IKS-Elemente festgestellt werden.

Der RH wies darauf hin, dass seine Feststellungen nur auf den Zeitpunkt der Überprüfung zutrafen. Eine darüber hinausgehende Beurteilung der Wirksamkeit der Kontrollmaßnahmen konnte der RH nicht vornehmen. Die Überwachung der Einhaltung der Regelungen des IKS ist eine Management- bzw. Führungsaufgabe, die von den jeweiligen Vorgesetzten wahrzunehmen ist. Nur im Rahmen regelmäßiger Kontrollen kann das erwartete Schutzniveau aufrechterhalten werden. (TZ 29)

4. Über welche finanziellen Ressourcen verfügt das jeweilige Ministerium, um Spionage zu verhindern? Sind diese ausreichend, um effektiv gegen Spionage-Verdachtsmomente vorzugehen?

(1) Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung finanzieller Ressourcen zur Spionageprävention einzubeziehen. (TZ 8, TZ 10, TZ 12)

(2) Die Auszahlungen des Innenministeriums für den Aufgabenbereich Staatsschutz und Nachrichtendienst verdreifachten sich zwischen 2017 und 2024. Sie stiegen von 2017 bis 2021 moderat und ab 2022 stark. Der vergleichsweise hohe Anteil des Sachaufwands im Jahr 2022 war insbesondere auf IKT-Investitionen im Zusammenhang mit dem Aufbau der DSN zurückzuführen. (TZ 8)

(3) Die militärischen Nachrichtendienste waren budgetär in den Generalstab integriert. Eine nähere Detaillierung und interne Kennzeichnung bestanden nicht. Wegen der fehlenden budgetären Zuordnung sowie der Änderung der Budgetstruktur im überprüften Zeitraum war es nicht möglich, valide Zahlen zu den finanziellen Ressourcen zu erheben, die den Nachrichtendiensten des Bundesheeres und konkret dem Abwehramt insgesamt bzw. der Spionageabwehr zur Verfügung standen; auch war die Entwicklung der Auszahlungen in diesem Bereich nicht zuverlässig darstellbar. (TZ 10)

(4) Daten zum Einsatz finanzieller Ressourcen im Außenministerium für dessen Aufgabenerfüllung lagen vor. Die Spionageprävention war keine explizite Aufgabe des Außenministeriums. Finanzielle Ressourcen im Zusammenhang mit Spionageprävention waren daher nicht gesondert ausgewiesen. (TZ 12)

5. Über welche personellen Ressourcen verfügt das jeweilige Ministerium, um Spionage zu verhindern? Sind diese ausreichend, um effektiv gegen Spionage-Verdachtsmomente vorzugehen?

(1) Der RH wies darauf hin, dass die Veränderungen im geopolitischen Umfeld (TZ 5) zu hochdynamischen Veränderungen der Bedrohungs- und Sicherheitslage und der Anforderungen an die Spionageprävention geführt hatten. Der RH hält es daher für zweckmäßig, diese Dynamik in die Bereitstellung personeller Ressourcen zur Spionageprävention einzubeziehen. (TZ 7, TZ 9, TZ 11)

(2) Das Innenministerium erhöhte die personellen Ressourcen für die Spionageabwehr im überprüften Zeitraum (1. Jänner 2017 bis 1. Jänner 2025), vor allem ab Einrichtung der DSN mit Dezember 2021. Der Personalstand in VBÄ lag am 1. Jänner 2025 bei 207 % des Wertes vom 1. Jänner 2017. Gleichzeitig stiegen im Hinblick auf internationale Entwicklungen und die veränderte Bedrohungslage die Anforderungen an die DSN insgesamt und insbesondere auch im Bereich der Spionageabwehr. Dies kam u.a. auch durch den starken Anstieg der Auszahlungen für Mehrdienstleistungen zwischen 2017 und 2024 – insbesondere ab 2022 – auf 373 % des Ausgangswerts 2017 zum Ausdruck. (TZ 7)

(3) Die im Abwehramt unmittelbar für den Bereich der Spionageabwehr zur Verfügung stehenden Personalressourcen verdoppelten sich von 2017 bis 2024; dies war im Wesentlichen mit der Umsetzung des neuen Organisationsplans im Jahr 2022 und internen Umschichtungen begründet. Die durch die internationale Bedrohungslage – insbesondere infolge des Krieges in der Ukraine sowie verstärkter Spionagetätigkeit – gestiegenen Anforderungen an die militärische Spionageabwehr verursachten allerdings Bedarf an zusätzlichen personellen Ressourcen, was sich u.a. auch in einer deutlichen Steigerung der Auszahlungen für Mehrdienstleistungen in diesem Bereich zeigte. Die Auszahlungen für Mehrdienstleistungen blieben von 2017 bis 2021 nahezu unverändert, ab 2022 stiegen sie markant auf das Dreieinhalbfache im Jahr 2024. (TZ 9)

(4) Im Außenministerium war keine spezifische Organisationseinheit für Spionageabwehr zuständig, entsprechende Aufgaben waren auf mehrere Abteilungen verteilt. Zwischen 1. Jänner 2017 und 1. Jänner 2025 stieg der Personalstand in den primär mit dem Aufgabenbereich befassten Abteilungen auf knapp mehr als das Doppelte. (TZ 11)

6. Welche Maßnahmen wurden im jeweiligen Ministerium gesetzt, um etwaigen Verdachtsmomenten von ausländischer Spionage nachzugehen? Waren diese ausreichend, um im Sinne einer Generalprävention ausländische Spionage zu verhindern?

(1) Für die laufende und operative Zusammenarbeit der Bundesministerien waren je nach Art bzw. Klassifizierung der Informationen unterschiedliche Organisationseinheiten (bzw. Organisationsebenen) zuständig. Die DSN, das Abwehramt und das Außenministerium hatten Prozesse definiert, die dem RH in Interviews erläutert wurden: (TZ 31)

- Die DSN hatte Prozesse zur Informationsanalyse, -aufbereitung und -weitergabe innerhalb der DSN bzw. des Innenministeriums, zur Informationsweitergabe zum Abwehramt und Heeres-Nachrichtenamt, zu anderen Ressorts und zu Partnerdiensten im Ausland definiert. (TZ 17)
- Das Abwehramt bereitete nach eigenen Angaben bei Kenntnissen aus fremden oder eigenen Ermittlungen, die eine Einbindung anderer Dienststellen bzw. Bundesministerien notwendig machten, nach Vor- und Freigabe durch die Leitungsebene entsprechende Informationen auf. Diese übermittelte es entweder schriftlich oder mündlich an die externen Bedarfsträger.
- Das Außenministerium nahm auf die Geschäftseinteilung und die darin festgelegten Agenden Bezug.

Die Bundesministerien tauschten Informationen je nach Art bzw. Klassifizierung im Wege der Amtshilfe[76], über gesicherte Datenleitungen oder persönlich aus. (TZ 31)

In Österreich – insbesondere in Wien – haben zahlreiche diplomatische Vertretungen sowie internationale Organisationen ihren Sitz. Das Wiener Übereinkommen regelt die Rahmenbedingungen für die diplomatischen Beziehungen zwischen den Staaten. Vorbehaltlich der Art. 5, 8, 9 und 11 des Wiener Übereinkommens konnte der Entsendestaat die Mitglieder des Personals seiner Mission nach freiem Ermessen ernennen.[77] (TZ 31)

(2) Das Außenministerium befasste die relevanten Bundesministerien und Nachrichtendienste u.a. in allen Agrémentverfahren (für bilaterale Botschafterinnen und Botschafter und für Militärattachés) sowie in einigen Fällen vor der Erteilung von Dienstantrittsvisa für andere Personen. Die DSN erhielt vom Außenministerium auf Anfrage Daten über einzelne in Österreich akkreditierte Diplomatinnen und Diplomaten, deren Angehörige, sonstige Missionsangehörige sowie Mitarbeiterinnen und

[76] Art. 22 Bundes-Verfassungsgesetz

[77] Allerdings konnte gemäß Art. 11 des Wiener Übereinkommens bei Fehlen einer ausdrücklichen Vereinbarung über den Personalbestand der Mission der Empfangsstaat verlangen, dass dieser Personalbestand in jenen Grenzen gehalten wird, die er in Anbetracht der bei ihm vorliegenden Umstände und Verhältnisse sowie der Bedürfnisse der betreffenden Mission für angemessen und normal hält.

Mitarbeiter internationaler Organisationen oder Personengruppen. Nach Art. 9 des Wiener Übereinkommens konnte ein Empfangsstaat dem Entsendestaat jederzeit ohne Angabe von Gründen notifizieren, dass der Missionschef oder ein Mitglied des diplomatischen Personals der Mission persona non grata war oder dass ein anderes Mitglied des Personals der Mission ihm nicht genehm war. In diesen Fällen hatte der Entsendestaat die betreffende Person entweder abzuberufen oder ihre Tätigkeit bei der Mission zu beenden. Eine Person konnte als non grata oder nicht genehm erklärt werden, bevor sie im Hoheitsgebiet des Empfangsstaats eintraf. (TZ 31)

Sachverhalte und Informationen, die zu einer Ausweisung führen konnten, übermittelten der Direktor der DSN sowie der Leiter des Abwehramtes nach übereinstimmenden Angaben der Bundesministerien ausschließlich persönlich und mündlich den zuständigen Personen im Außenministerium. Schriftliche Unterlagen dazu übermittelten sie grundsätzlich nicht. Das Außenministerium gab an, dass – sobald Hinweise auf nicht mit dem Wiener Übereinkommen vereinbare nachrichtendienstliche Tätigkeiten vorgelegt wurden – diese mit den betroffenen Bundesministerien und Nachrichtendiensten erläutert und geprüft wurden. Waren ausreichend Hinweise für ein Fehlverhalten einer Diplomatin bzw. eines Diplomaten vorhanden, wurde nach Beteiligung aller betroffenen Bundesministerien über etwaige Ausweisungen entschieden. Im Falle multilateral akkreditierter Diplomatinnen bzw. Diplomaten erfolgte die im jeweiligen Amtssitzabkommen vorgesehene Konsultation mit der betroffenen internationalen Organisation. (TZ 31)

Österreich erklärte seit Beginn des Krieges in der Ukraine im Februar 2022 elf Personen zu personae non gratae und wies sie aus. Dies betraf ausschließlich diplomatisches Personal der Russischen Föderation. (TZ 31)

(3) Im Innen-, Verteidigungs- und Außenministerium waren personenbezogene Überprüfungen von Bewerberinnen und Bewerbern eine Aufnahmevoraussetzung.

- Die Sicherheitsüberprüfung (§§ 55 ff. Sicherheitspolizeigesetz) diente der Abklärung der Vertrauenswürdigkeit einer Person anhand personenbezogener Daten, die Aufschluss über allfällige Anhaltspunkte dafür geben, ob die Person gefährliche Angriffe begehen werde. Die Sicherheitsüberprüfung war nach den Regelungen des Geheimschutzes Voraussetzung für den Zugang zu klassifizierten Informationen ab der Stufe „VERTRAULICH“ (§ 3 Abs. 1 Z 1 lit. c InfoSiG und § 6 Abs. 1 Z 3 Geheimschutzordnung). (TZ 20)
- Die Vertrauenswürdigkeitsprüfung war in § 2a SNG geregelt. Der Gesetzgeber hatte sie im Rahmen der Neugestaltung des Verfassungsschutzes eingeführt, weil sich die bestehende Sicherheitsüberprüfung laut Gesetzesmaterialien als unzureichend erwiesen hatte, um den Schutz klassifizierter Informationen zu gewährleisten. Vor Beginn der Tätigkeit in der DSN mussten sich künftige Bedienstete gemäß § 2a Abs. 1 SNG einer Vertrauenswürdigkeitsprüfung für den Verfassungsschutz unterzie-

hen. Danach hatten Bedienstete der DSN alle drei Jahre abwechselnd eine Sicherheitsüberprüfung für den Zugang zu streng geheimer Information und eine Vertrauenswürdigkeitsprüfung zu wiederholen. (TZ 20)

- Die Verlässlichkeitsprüfung war in §§ 23 und 24 Militärbefugnisgesetz geregelt, nähere Bestimmungen über die Verlässlichkeitserklärung gemäß § 24 Abs. 1 leg. cit. in einer Verordnung des Bundesministers für Landesverteidigung[78]. Die Verlässlichkeitsprüfung diente der Abklärung der Verlässlichkeit einer Person anhand von Daten, die Aufschluss über allfällige Anhaltspunkte geben, ob von dieser Person eine Gefahr für die militärische Sicherheit ausgeht. Positive Beurteilungen der Verlässlichkeit endeten in einer Prüfbescheinigung für die jeweilige Zulassungsgruppe (von Zutrittsberechtigungen bis zum Zugang zu streng geheimen Informationen). (TZ 21)

  Im Innenministerium oblag die Gestaltung des Bewerbungsprozesses der für Personalangelegenheiten zuständigen Organisationseinheit. Personen, die eine Tätigkeit in der DSN anstrebten, mussten zunächst ein dreiteiliges Auswahlverfahren durchlaufen mit einer computerunterstützten psychologischen Testung, einem psychologischen Interview und einem Fachgespräch. Hier stand insbesondere das in der Ausschreibung beschriebene Anforderungsprofil im Vordergrund, nicht ein allenfalls vorliegendes Risiko für den Verfassungsschutz. Dieses musste im Rahmen der Vertrauenswürdigkeitsprüfung festgestellt werden. (TZ 20, TZ 22)

  Eine Voraussetzung für die Aufnahme in ein Dienstverhältnis zum Verteidigungsministerium war die Verlässlichkeitsprüfung. Zusätzlich hatten Personen, die eine Tätigkeit im Abwehramt anstrebten, ein mehrstufiges Auswahlverfahren zu durchlaufen. Dazu zählten neben der allgemeinen Erfüllung des Anforderungsprofils eine persönliche Auswahl der Personen, ein psychologisches Screening, eine erweiterte Verlässlichkeitsprüfung, ein Hearing und ein Assessment für Auslandseinsätze. (TZ 22)

  Das Außenministerium veranlasste vor der Aufnahme einer Bewerberin bzw. eines Bewerbers sowie bei Versetzungen als Sicherheitsmaßnahme u.a. eine Sicherheitsüberprüfung. Vor der Aufnahme wurden alle Bediensteten, auch jene des Kabinetts, einer Sicherheitsüberprüfung durch die DSN unterzogen. Eine den örtlichen Verhältnissen angepasste Vorgehensweise sah das Außenministerium für die österreichischen Vertretungsbehörden vor. (TZ 22)

[78] Verordnung des Bundesministers für Landesverteidigung über die Verlässlichkeitserklärung, BGBl. II 195/2001

Schlussempfehlungen

34 Zusammenfassend empfahl der RH:

Bundesministerium für Inneres

(1) Der personelle Ausbau der Direktion Staatsschutz und Nachrichtendienst, insbesondere im Bereich der Spionageabwehr, wäre weiterhin voranzutreiben. Bei der Beantragung zusätzlicher Planstellen bzw. bewerteter Arbeitsplätze wäre dabei auf Basis regelmäßiger Bedarfsanalysen eine Priorisierung nach Dringlichkeit vorzunehmen. (TZ 7)

(2) Unter Einbindung der wesentlichen Bedarfs- und Interessensträger wären die rechtlichen, organisatorischen und prozessualen Grundlagen der Vertrauenswürdigkeits- und Sicherheitsüberprüfung zu analysieren. Dies mit dem Ziel, eine flexible, zeitgemäße, effektive und effiziente Durchführung der Prüfung zu gewährleisten. Die Ergebnisse wären in geeigneter Weise umzusetzen. (TZ 20)

(3) Analog zum Militärbefugnisgesetz wäre auch im Staatsschutz- und Nachrichtendienst-Gesetz und im Sicherheitspolizeigesetz für die Vertrauenswürdigkeits- und Sicherheitsüberprüfung eine Regelung im Nationalrat zu initiieren, die Gründe für eine ex lege negativ zu beurteilende Überprüfung festlegt. (TZ 20)

(4) Analog zu den bestehenden Regelungen im Staatsschutz- und Nachrichtendienst-Gesetz zu den Personen, die einer Vertrauenswürdigkeitsprüfung unterzogen werden, wäre eine gesetzliche Regelung im Nationalrat zu initiieren, die Verwaltungspersonal mit vergleichbarem Einblick in die sensible Tätigkeit des Verfassungsschutzes in die Vertrauenswürdigkeitsprüfung einbezieht. (TZ 20)

(5) Andere Bundesministerien wären gegebenenfalls über jene sicherheitsrelevanten Umstände zu informieren, aufgrund derer das Bundesministerium für Inneres von der Nutzung der vertraglichen Leistungen im eigenen Bereich Abstand nimmt. (TZ 27)

Direktion Staatsschutz und Nachrichtendienst

(6) Es wäre bis zur Umsetzung der Anträge zur Personalaufstockung sicherzustellen, dass das vorhandene Personal der Direktion Staatsschutz und Nachrichtendienst entsprechend den laufenden Entwicklungen und der Bedrohungslage in den unterschiedlichen Phänomenbereichen flexibel eingesetzt werden kann. (TZ 7)

(7) Ein formelles regelmäßiges Austauschformat zwischen allen im Geheimschutz tätigen Organisationseinheiten in der Direktion Staatsschutz und Nachrichtendienst wäre aufzubauen. (TZ 14)

(8) Für rechtliche Fragen des Vergabeverfahrens wäre – unter Wahrung der Sicherheitsinteressen – die Expertise von zentralen, für Beschaffungen zuständigen Abteilungen des Bundesministeriums für Inneres heranzuziehen. (TZ 28)

Bundesministerium für Landesverteidigung

(9) Die personellen Ressourcen für die Spionageabwehr wären regelmäßig der internationalen Bedrohungslage anzupassen; der Organisationsplan des Abwehramtes wäre in diesem Sinne zu überarbeiten. (TZ 9)

(10) Die Auszahlungen für die militärischen Nachrichtendienste wären im Budgetvollzug im Sinne einer effizienten Steuerungsmöglichkeit intern zu kennzeichnen. (TZ 10)

(11) Basierend auf den Empfehlungen der Internen Revision wäre eine Risikoanalyse im Bereich der Nebenbeschäftigungen durchzuführen. Dies mit dem Ziel, Problembereiche für den Dienstgeber zu erkennen und gegebenenfalls die Verordnung über unzulässige Nebenbeschäftigungen zu überarbeiten. (TZ 24)

(12) Die Erstellung des Offboarding-Prozesses für die militärischen Nachrichtendienste wäre ehestmöglich abzuschließen; darin wäre die Dokumentation der einzelnen Schritte des Prozesses (etwa in Form einer Checkliste) vorzusehen. (TZ 26)

Bundesministerium für europäische und internationale Angelegenheiten

(13) Die für Sicherheitsangelegenheiten zuständige Abteilung wäre über staatssicherheitsrelevante Vorfälle zu informieren. (TZ 14)

(14) Zur Stärkung des Internen Kontrollsystems wäre die Implementierung des Informationssicherheitsmanagementsystems (ISMS) priorisiert abzuschließen und entsprechende Prozesse und Rollen unter Einbeziehung von Gesichtspunkten der Spionageprävention zu definieren. (TZ 14)

(15) Ressortweite standardisierte und verbindliche Schulungs- und Awarenessmaßnahmen mit anschließender Wissensüberprüfung, in deren Fokus auch das Thema Spionageprävention steht, wären umzusetzen. (TZ 14)

Bundesministerium für Inneres; Bundesministerium für Landesverteidigung; Bundesministerium für europäische und internationale Angelegenheiten

(16) Die Auswirkungen der geopolitischen Entwicklungen auf einen Veränderungs- oder Anpassungsbedarf der Österreichischen Sicherheitsstrategie wären weiterhin zu beobachten; allfällige notwendige Weiterentwicklungen der Österreichischen Sicherheitsstrategie wären beim Bundeskanzleramt anzustoßen und einer Beschlussfassung im Nationalrat zuzuführen. (TZ 5)

(17) Die personellen und finanziellen Ressourcen zur Spionageprävention wären entsprechend den dynamischen Entwicklungen der Bedrohungslage bereitzustellen. (TZ 7, TZ 8, TZ 9, TZ 10, TZ 11, TZ 12)

(18) Die Vorbereitung der Regierungsvorlage für ein novelliertes Informationssicherheitsgesetz wäre in der Informationssicherheitskommission sowie im Abstimmungsprozess mit sämtlichen Bundesministerien zu unterstützen, um die Harmonisierung der Rechtsgrundlagen für klassifizierte Informationen abzuschließen. (TZ 15)

(19) Die Arbeiten in der Informationssicherheitskommission an einer Klassifizierungsrichtlinie wären voranzutreiben, die die Bediensteten bei der Klassifizierung von Informationen unterstützen und die Einheitlichkeit fördern soll. (TZ 16)

(20) Der Wahrnehmung der Management- und Führungsaufgaben wäre – zum Erhalt des Schutzniveaus des Internen Kontrollsystems – hohe Aufmerksamkeit zu schenken. (TZ 29)

Bundesministerium für Inneres; Bundesministerium für Landesverteidigung

(21) Für Beschaffungen, die wesentliche Sicherheitsinteressen des Bundes betreffen und die damit für eine Ausnahme von den Bundesvergabegesetzen zugänglich sind, wäre auf eine gesetzliche Regelung hinzuwirken, die eine Überprüfung von Unternehmen vor Beauftragung (im Rahmen der Eignungsprüfung) unter Heranziehung nachrichtendienstlicher Erkenntnisse ermöglicht. (TZ 27)

Rechnungshof Österreich

Wien, im Juni 2026
Die Präsidentin:

Dr. Margit Kraker

Anhang

Ressortbezeichnung und -verantwortliche

Tabelle A: Innenministerium seit 2017

Ressortbezeichnung	Bundesminister
Bundesministerium für Inneres	bis 18. Dezember 2017: Mag. Wolfgang Sobotka
	18. Dezember 2017 bis 22. Mai 2019: Herbert Kickl
	22. Mai 2019 bis 3. Juni 2019: Hon.-Prof. Dr. Eckart Ratz
	3. Juni 2019 bis 7. Jänner 2020: Dr. Wolfgang Peschorn
	7. Jänner 2020 bis 6. Dezember 2021: Karl Nehammer, MSc
	seit 6. Dezember 2021: Mag. Gerhard Karner

Quelle: Parlament; Zusammenstellung: RH

Tabelle B: Verteidigungsministerium seit 2017

Zeitraum	Bundesministerien-gesetz-Novelle	Ressortbezeichnung	Bundesminister/in
bis 7. Jänner 2018	BGBl. I 3/2009	Bundesministerium für Landesverteidigung und Sport	bis 18. Dezember 2017: Mag. Hans Peter Doskozil
			18. Dezember 2017 bis 8. Jänner 2018: Mario Kunasek
seit 8. Jänner 2018	BGBl. I 164/2017	Bundesministerium für Landesverteidigung	8. Jänner 2018 bis 22. Mai 2019: Mario Kunasek
			22. Mai 2019 bis 3. Juni 2019: Mag. Johann Luif
			3. Juni 2019 bis 7. Jänner 2020: Mag. Thomas Starlinger
			seit 7. Jänner 2020: Mag.ª Klaudia Tanner

Quelle: Parlament; Zusammenstellung: RH

Tabelle C: Außenministerium seit 2017

Zeitraum	Bundesministerien-gesetz-Novelle	Ressortbezeichnung	Bundesminister/in
bis 28. Jänner 2020	BGBl. I 11/2014	Bundesministerium für Europa, Integration und Äußeres	bis 18. Dezember 2017: Sebastian Kurz
			18. Dezember 2017 bis 3. Juni 2019: Dr.in Karin Kneissl
			3. Juni 2019 bis 29. Jänner 2020: Mag. Alexander Schallenberg, LL.M.
seit 29. Jänner 2020	BGBl. I 8/2020	Bundesministerium für europäische und internationale Angelegenheiten	29. Jänner 2020 bis 11. Oktober 2021: Mag. Alexander Schallenberg, LL.M.
			11. Oktober 2021 bis 6. Dezember 2021: Dr. Michael Linhart
			6. Dezember 2021 bis 3. März 2025: Mag. Alexander Schallenberg, LL.M.
			seit 3. März 2025: Mag.a Beate Meinl-Reisinger, MES

Quelle: Parlament; Zusammenstellung: RH

R
H