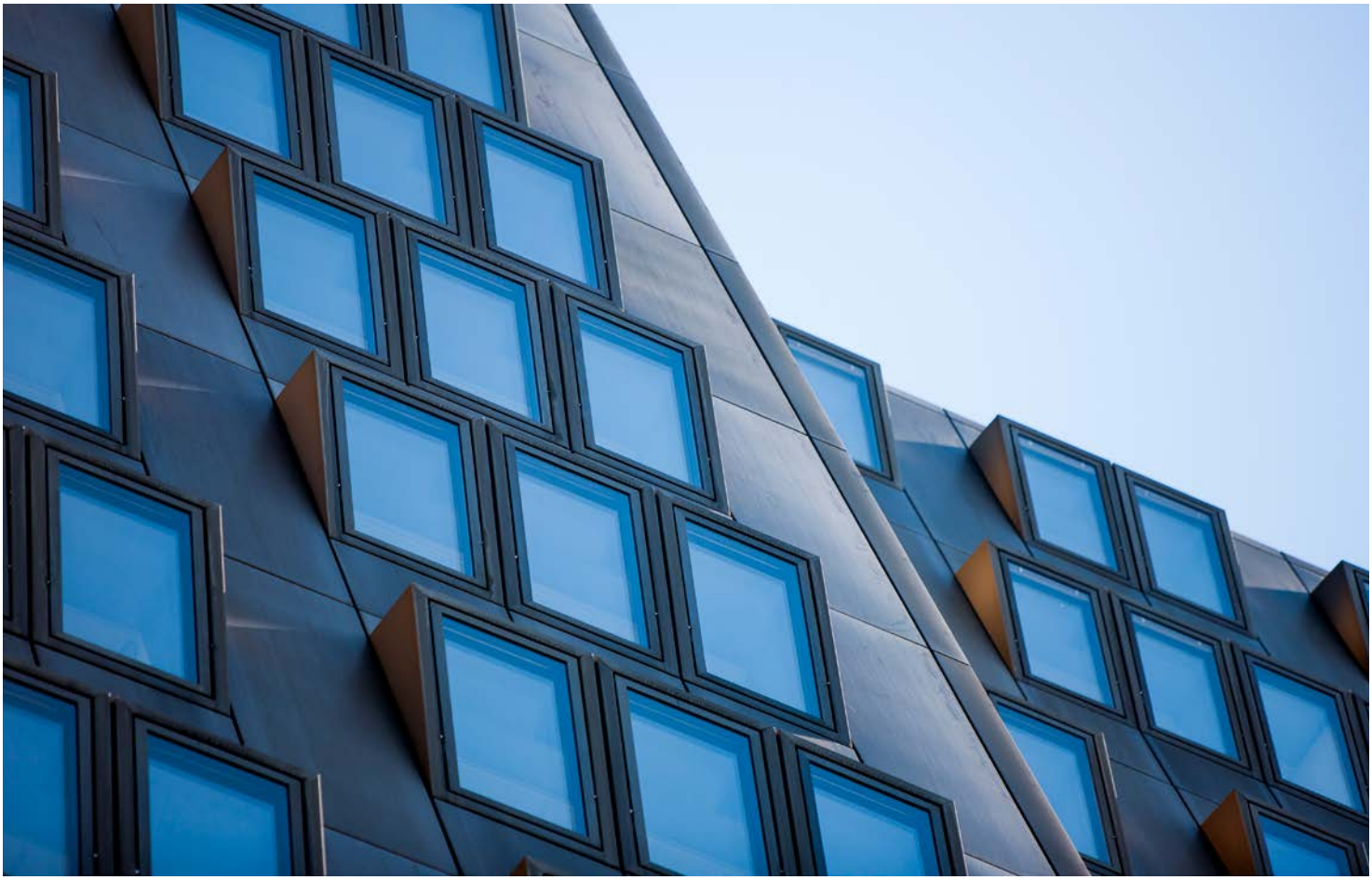
Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Koordination der Cyber–Defence

Reihe BUND 2023/30

Bericht des Rechnungshofes



III–1041 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 2023–0.738.679 (005.055)

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.

IMPRESSUM
Herausgeber:
Rechnungshof Österreich
1030 Wien, Dampfschiffstraße 2
www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im Oktober 2023

AUSKÜNFTE
Rechnungshof
Telefon (+43 1) 711 71 – 8946
E–Mail info@rechnungshof.gv.at
facebook/RechnungshofAT
Twitter: @RHSprecher

FOTOS
Cover: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BGBl.	Bundesgesetzblatt
BlgNR	Beilagen zu den Stenographischen Protokollen des Nationalrats
BMI	Bundesministerium für Inneres
BMLV	Bundesministerium für Landesverteidigung
B–VG	Bundes–Verfassungsgesetz
bzw.	beziehungsweise
etc.	et cetera
EU	Europäische Union
EUR	Euro
(f)f.	folgend(e)
GmbH	Gesellschaft mit beschränkter Haftung
i.d.(g.)F.	in der (geltenden) Fassung
IKDOK	Innerer Kreis der Operativen Koordinierungsstruktur
IKT	Informations– und Kommunikationstechnologie
inkl.	inklusive
IT	Informationstechnologie
Mio.	Million(en)
NIS	Netz– und Informationssystemsicherheit
NISG	Netz– und Informationssystemsicherheitsgesetz
OpKoord	Operative Koordinierungsstruktur
rd.	rund
RH	Rechnungshof
Rz	Randziffer
S.	Seite
TZ	Textzahl(en)

u.a.	unter anderem
VBÄ	Vollbeschäftigungsäquivalent(e)
vgl.	vergleiche
Z	Ziffer
z.B.	zum Beispiel

SOUVERÄNITÄTSGEFÄHRDUNG DURCH CYBER–ANGRIFF

Cyber–Defence ist die Abwehr von Cyber–Angriffen auf die Einrichtungen des Österreichischen Bundesheeres (Eigenschutz) oder auf die Souveränität des österreichischen Staates (Souveränitätsfall). Für diesen Fall hat die Verteidigungsministerin den Eintritt einer Souveränitätsgefährdung zu beurteilen, weil es ihr obliegt, den Einsatz zur militärischen Landesverteidigung zu verfügen. Das Verteidigungsministerium hatte noch keine konkreten Kriterien bzw. Szenarien ausgearbeitet, anhand derer beurteilt werden konnte, ob eine Souveränitätsgefährdung aufgrund eines Cyber–Angriffs vorlag, und anhand derer die Entscheidung über einen Cyber–Defence–Einsatz getroffen werden konnte.

Mit der Cyber–Sicherheit befassten sich die „Österreichische Strategie für Cybersicherheit“ (samt Maßnahmenkatalog) sowie das Konzept „Gesamtstaatliches Cyber Krisenmanagement“ (CKM 2019). Die als strategische Maßnahme des Verteidigungsministeriums hierzu erforderliche Cyber–Verteidigungsstrategie (Leitlinie Cyber–Verteidigung) befand sich erst in einem Entwurfsstadium.

EFFIZIENTE ZUSAMMENARBEIT

Die Organisationsreform des Verteidigungsministeriums hatte die für Cyber–Defence wesentlichen Organisationseinheiten unter gemeinsamer Leitung in der „Direktion 6 – IKT und Cyber“ der Generaldirektion für Landesverteidigung zusammengeführt. Damit wurden die Voraussetzungen für eine effiziente Zusammenarbeit zwischen diesen Organisationseinheiten geschaffen.

KEINE CYBER–ÜBUNGEN ZU SOUVERÄNITÄTSFALL

In den Jahren 2018 bis 2022 nahm das Verteidigungsministerium an insgesamt 32 Cyber–Übungen teil. Spezifische Übungen eines Cyber–Defence–Falls aufgrund einer Souveränitätsgefährdung hatten das Verteidigungsministerium bzw. das Bundesheer nicht durchgeführt: Es waren weder Konzepte zur Feststellung einer Souveränitätsgefährdung, notwendige Maßnahmen beim Übergang von einer Cyber–Krise in einen Cyber–Defence–Einsatz noch Konzepte zur Zurechnung eines Angriffs an einen staatlichen Akteur erprobt worden.

WIRKUNGSBEREICH

- Bundesministerium für Landesverteidigung

Koordination der Cyber–Defence

Prüfungsziel

Der RH überprüfte von August bis November 2022 im Verteidigungsministerium die Koordination der Cyber–Defence.

Cyber–Defence ist die Abwehr von Cyber–Angriffen auf die Souveränität des österreichischen Staates (Souveränitätsfall) oder auf die Einrichtungen des Österreichischen Bundesheeres (in der Folge: **Bundesheer**) (Eigenschutz). Dafür verantwortlich ist das Verteidigungsministerium im Rahmen der militärischen Landesverteidigung. Ziel der Gebarungsüberprüfung waren die Darstellung und Beurteilung

- der rechtlichen Grundlagen für den Souveränitätsfall bzw. den militärischen Eigenschutz im Cyber–Raum (Cyber–Defence),
- der Strategie, Planung, Organisation und Umsetzung der Cyber–Defence im Verteidigungsministerium und
- der Leistungen des Verteidigungsministeriums für die Cyber–Sicherheit im Rahmen von Assistenzleistungen, Amtshilfe oder gesetzlich definierten Leistungen.

Der überprüfte Zeitraum umfasste die Jahre 2021 bis November 2022. In Einzelfällen nahm der RH auch Bezug auf Sachverhalte außerhalb dieses Zeitraums.

Kurzfassung

Die Koordination der Cyber–Sicherheit obliegt gemäß dem Netz– und Informationssystemsicherheitsgesetz (**NISG**) den Sicherheitsressorts (Innenministerium, Bundeskanzleramt, Außenministerium und Verteidigungsministerium). Im Cyber–Vorfalls– und Krisenmanagement ist das Innenministerium für operative Maßnahmen zuständig, das Bundesheer kann im Rahmen einer eigens anzufordernden Assistenzleistung mitwirken. (TZ 1)

Beim Übergang von einer Cyber–Krise in einen Cyber–Defence–Einsatz geht die Zuständigkeit von der Innenministerin bzw. dem Innenminister auf die Verteidigungsministerin bzw. den Verteidigungsminister über. Im Zuge der allgemeinen Einsatzvorbereitung hat daher das Verteidigungsministerium die ständige Einsatzbereitschaft des Bundesheeres auch zur Abwehr von Cyber–Angriffen sicherzustellen und die erforderlichen personellen und materiellen Voraussetzungen für einen Einsatz im Cyber–Raum zu schaffen. (TZ 1)

Das Verteidigungsministerium und damit die für Informations– und Kommunikationstechnologie (**IKT**) zuständige „Direktion 6 – IKT und Cyber" (in der Folge: **Direktion 6**) der Generaldirektion für Landesverteidigung waren einer Vielzahl von Cyber–Sicherheitsereignissen und –Vorfällen ausgesetzt. Allein in der einmonatigen Zeitspanne von Ende Oktober bis Ende November 2022 wurden durch Sicherheitsvorkehrungen im Netzwerk rd. 390.000 Sicherheitsereignisse[1] automatisiert detektiert und abgewehrt. Von den Sicherheitsereignissen und Vorfällen, die in den ersten drei Quartalen 2022 im Rahmen des militärischen Eigenschutzes festgestellt wurden, überprüfte das Verteidigungsministerium rd. 400 Vorfälle genauer. In weiterer Folge hatte es davon rd. 30 detailliert zu analysieren. Der Eigenschutz der IKT–Systeme war somit eine Aufgabe, die das Verteidigungsministerium umfassend und permanent zu erfüllen hatte. (TZ 2)

Grundlagen

Die Aufgaben des Bundesheeres sind verfassungsrechtlich in Art. 79 Bundes–Verfassungsgesetz (**B–VG**) und im Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland festgelegt; auf einfachgesetzlicher Ebene präzisiert das Wehrgesetz 2001 die Aufgaben und das Militärbefugnisgesetz die Mittel und Befugnisse des Bundesheeres. Alle Leistungen im Cyber–Raum sind im Rahmen dieser verfassungsrechtlich festgelegten Aufgaben zu erbringen. Dies umfasst die Verteidigung der angegriffenen IKT–Systeme zur Abwehr von Cyber–Angriffen, die Ausnützung fremder IKT–Systeme zur Informationssammlung und den Angriff auf IKT–Systeme, um Cyber–Angriffe zu beenden. (TZ 3)

Die Abwehr von Cyber–Angriffen auf die Souveränität Österreichs war eine anlassbezogene Aufgabenstellung im Rahmen der militärischen Landesverteidigung. In diesem Fall erweitert sich der Aufgabenbereich des Bundesheeres auch auf den Schutz der IKT–Systeme der verfassungsmäßigen Einrichtungen der Republik Österreich und den Schutz kritischer Infrastrukturen, soweit diese für die militärische

[1] Die Sicherheitsereignisse betrafen überwiegend Datenverkehr von verdächtigen IP–Adressen, verdächtige Aktivitäten bzw. verdächtige Nutzung eines Netzwerks. Es wurden aber z.B. auch potenzielle Schadsoftware oder Denial–of–Service–Angriffe (DoS = Verhinderung des Zugriffs auf einen Web–Dienst) durch die Sicherheitseinrichtungen geblockt.

Einsatzführung und Sicherstellung der Souveränität relevant waren. Die Verfügung über einen (Cyber–Defence–)Einsatz des Bundesheeres zur militärischen Landesverteidigung obliegt der Verteidigungsministerin innerhalb der ihr von der Bundesregierung erteilten Ermächtigung. (TZ 3)

Die gesamtstaatliche Österreichische Sicherheitsstrategie diente der Gewährleistung der „Umfassenden Sicherheitsvorsorge" in Österreich. Im Politikbereich Verteidigung wurde sie durch die Teilstrategie Verteidigungspolitik und das Militärstrategische Konzept 2017 ergänzt. Mit der Cyber–Sicherheit befassten sich die Österreichische Strategie für Cybersicherheit (samt Maßnahmenkatalog) sowie das Konzept Gesamtstaatliches Cyber Krisenmanagement (CKM 2019). Die als strategische Maßnahme des Verteidigungsministeriums hierzu erforderliche Cyber–Verteidigungsstrategie (in der Folge: **Leitlinie Cyber–Verteidigung**) befand sich erst in einem Entwurfsstadium. (TZ 4)

Entscheidung über einen Cyber–Defence–Einsatz

Im Konzept Gesamtstaatliches Cyber Krisenmanagement (CKM 2019) wurde lediglich allgemein darauf verwiesen, dass zur Vermeidung von Doppelgleisigkeiten Strukturen, die für das Cyberkrisenmanagement des Innenministeriums eingerichtet sind, auch für die militärische Landesverteidigung im Cyber–Raum zu nutzen wären. Die konkreten Verantwortlichkeiten bis zur Entscheidung über einen Cyber–Defence–Einsatz waren lediglich in groben Zügen dargestellt. Ein gesamtstaatliches Konzept, das die einzelnen Verfahrensschritte konkretisiert, die erforderlichen Kommunikationskanäle auch zwischen mehreren Gebietskörperschaften definiert und zu einem koordinierten Zusammenwirken aller beteiligten staatlichen Stellen beiträgt, lag nicht vor. (TZ 5)

In einem Anlassfall hat die Verteidigungsministerin den Eintritt einer Souveränitätsgefährdung zu beurteilen, weil es ihr oblag, den Einsatz zur militärischen Landesverteidigung zu verfügen. Darüber hinaus war eine gesamtstaatliche Abstimmung mit der Bundesregierung und insbesondere den Sicherheitsressorts erforderlich. Die vorhandenen verteidigungspolitischen und militärstrategischen Grundsatzdokumente des Verteidigungsministeriums enthielten allerdings nur allgemeine Umschreibungen einer Souveränitätsgefährdung Österreichs durch einen Cyber–Angriff. Konkrete Beurteilungskriterien bzw. Szenarien, auf deren Grundlage die Entscheidung über einen Cyber–Defence–Einsatz getroffen werden konnte, hatte das Verteidigungsministerium noch nicht ausgearbeitet. (TZ 5)

Assistenzeinsätze des Bundesheeres auf Anforderung von Behörden und Organen des Bundes, der Länder oder Gemeinden dienen dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit sowie der demokratischen Freiheiten der Einwohnerinnen und Einwohner und der Aufrechterhaltung der Ordnung

und Sicherheit im Inneren. Die gesamtstaatlichen Sicherheitsstrategien zur umfassenden wie auch zur Cyber–Sicherheit und die daraus abgeleiteten Strategien des Verteidigungsministeriums (Teilstrategie Verteidigungspolitik, Militärstrategisches Konzept 2017) betrachteten die Assistenzleistungen des Bundesheeres, ergänzend zu den erforderlichen Maßnahmen durch die zivilen Kräfte, als wesentlichen und unabdingbaren Beitrag zur gesamtstaatlichen Krisenbewältigung. Nach der bisher einzigen festgestellten – das Außenministerium betreffenden – Cyber–Krise empfahl der Nationale Sicherheitsrat, das Verteidigungsministerium (und das Innenministerium) personell und technisch ausreichend auszustatten, sodass die permanente Einsatzfähigkeit von Cyber–Kräften gewährleistet ist. (TZ 6)

Die permanenten Aufgaben des Verteidigungsministeriums nach dem NISG – insbesondere die laufende Zusammenarbeit mit den anderen Sicherheitsressorts und Mitwirkung bei der Lagebilderstellung – waren ein Beitrag zur gesamtstaatlichen Cyber–Sicherheit. Weitere Aufgaben des Verteidigungsministeriums ergaben sich im Rahmen der Amtshilfe sowie der Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen für die sichere Verwendung von klassifizierten Informationen. (TZ 7)

Cyber–Defence: Strategie und Planung

Gemäß der Organisationsreform 2021 war die Generaldirektion für Landesverteidigung dem Generalstab nachgeordnet und bestand aus neun Direktionen. In der neuen Direktion 6 waren die wesentlichen Kapazitäten der Cyber–Defence zusammengeführt. Ihr Aufgabengebiet umfasste die gesamten IKT–Agenden des Verteidigungsministeriums und des Bundesheeres sowie die operative Umsetzung der Cyber–Defence. Damit waren die Voraussetzungen für eine effiziente Zusammenarbeit zwischen den Organisationseinheiten geschaffen. Die Direktion 6 war im November 2022 allerdings noch nicht durch einen Erlass verfügt, sie arbeitete noch auf Grundlage der vorläufigen Projektorganisation. In der Geschäftseinteilung der Direktion 6 waren die Aufgaben von Organisationseinheiten noch nicht festgelegt, auch Gesamtziele für die Direktion 6 fehlten. (TZ 8)

Die beantragte Bewertung und Zuordnung (Systemisierung) der Arbeitsplätze der einzelnen Organisationseinheiten der Direktion 6 hatte das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport noch nicht vorgenommen. Diesbezügliche Verhandlungen waren nach Auskunft des Verteidigungsministeriums noch nicht abgeschlossen und im November 2022 unterbrochen. Die Direktion 6 erfüllte ihre Aufgaben zwar in der neuen Struktur, teilweise jedoch durch dienstzugeteilte Bedienstete. Wesentliche Abläufe und Prozesse der Direktion 6 befanden sich noch in einem Bearbeitungsprozess, der erst nach Systemisierung der Arbeitsplätze und anschließender Verfügung der Organisationspläne abgeschlossen werden kann. (TZ 9)

Das Verteidigungsministerium plante für die Direktion 6, die Anzahl der Arbeitsplätze in zwei Phasen zu erhöhen. Ziel der Aufstockung, die insbesondere das Militärische Cyberzentrum, die Führungsabteilung und das Institut für Militärisches Geowesen betraf, war ein schrittweiser Auf– und Ausbau von Fähigkeiten. (TZ 9)

Neben der Direktion 6 befassten sich weitere Organisationseinheiten mit Aufgaben der Cyber–Defence: In der Generaldirektion für Landesverteidigung war die Direktion Fähigkeiten und Grundsatzplanung für die Konzeption der Fähigkeiten der gesamten Streitkräfte zuständig, die Direktion 1 – Einsatz für den Einsatz und die Einsatzvorbereitung der gesamten Streitkräfte. Beide kooperierten eng mit den jeweils zuständigen Abteilungen in der Direktion 6. Die militärischen Nachrichtendienste wirkten unmittelbar an Kernaufgaben der Cyber–Defence mit: Das Abwehramt hatte die Aufgabe der nachrichtendienstlichen Abwehr, diente dem militärischen Eigenschutz und hatte auch im Cyber–Bereich die präventive und aktive Abwehr wahrzunehmen. Das für die nachrichtendienstliche Aufklärung zuständige Heeres–Nachrichtenamt erstellte ein nachrichtendienstliches Lagebild (u.a. militärisch, politisch, ökonomisch), das bei gegebenem Anlass Cyber–Agenden einbezog. (TZ 10)

Die Direktion 6 wirkte mit anderen Organisationseinheiten in unterschiedlichen Bereichen zusammen:

- Für das Cyber–Lagebild analysierte das Militärische Cyberzentrum Cyber–Angriffe bzw. Vorfälle. Einen wöchentlichen Informationsaustausch gab es zwischen dem IKT & Cybersicherheitszentrum (mit den Bereichen Militärisches Cyberzentrum, IKT–Betrieb und IKT–Cybereinsatz) und den Nachrichtenämtern. Die Prozesse der Abstimmung und Zusammenarbeit waren allerdings nicht schriftlich festgelegt. Angesichts der Bedeutung der Aufgabe Cyber–Defence für die militärische und somit auch für die gesamtstaatliche Sicherheit ist es wesentlich, dass die Prozesse für diese Zusammenarbeit schriftlich festgelegt sind, um deren Einhaltung unabhängig von den agierenden Personen sicherzustellen.
- Für zentrale Aufgaben der Landesverteidigung hatte das Verteidigungsministerium eine Ablauforganisation in Form von sogenannten Kernprozessen in einer eigenen Richtlinie „Zentrale Prozesse der Landesverteidigung 2022“ festgelegt. In den relevanten Prozessen „Streitkräfte entwickeln“ und „Streitkräfte einsetzen und führen“ war die Direktion 6 in nahezu sämtliche Prozessschritte eingebunden.
- Auf Ebene der Direktion 6 erfolgte die Zusammenarbeit der Organisationseinheiten über eine wöchentliche Direktionsbesprechung, die der Koordination und gegenseitigen Information diente und in der die Bearbeitung der einzelnen Aufgaben abgestimmt wurde. (TZ 11)

Das Verteidigungsministerium arbeitete an Konzepten, mit denen die Cyber–Defence festgeschrieben und gesteuert werden sollte. Die dafür zentrale Leitlinie Cyber–Verteidigung befand sich im November 2022 in Ausarbeitung. Die Inhalte des Entwurfs waren nur allgemein formuliert, die Organisationseinheiten für deren Umsetzung waren darin nicht bestimmt. (TZ 12)

Um die Grundlagen für die Entwicklung der Cyber–Kräfte im Bundesheer zu schaffen, war auch ein Querschnittskonzept „Einsatz im Cyber–Raum“ in Bearbeitung. Dieses enthielt nur wenig detaillierte Vorgaben und sah keine Organisationseinheiten zur konkreten Bearbeitung vor. (TZ 12)

Für das Militärische Cyberzentrum beschrieb eine Geschäftsordnung dessen Organisation und regelte die Ablauforganisation im Normdienst, die Aufgabenzuordnung, den Dienstbetrieb und die Behandlung von Geschäftsfällen. Für andere Organisationseinheiten der Direktion 6 lagen keine Geschäftsordnungen vor. (TZ 12)

Cyber–Defence: Umsetzung

Die Einsatzkräfte des Bundesheeres setzen sich aus Truppen und Organisationselementen der Friedensgliederung und jenen, die zu Übungszwecken oder zum Zwecke eines Einsatzes einberufen wurden, zusammen. Die Direktion 6 hatte in militärischen Bedrohungsfällen rasch zu reagieren; dafür bedurfte es vorab der Ausarbeitung einer Einsatzorganisation (Aufbau– sowie Ablauforganisation). Die Direktion 6 hatte einen Entwurf der besonderen Aufbauorganisation sowie einer Geschäftsordnung für den Einsatz ausgearbeitet, allerdings war dieser im November 2022 noch nicht verfügt. (TZ 13)

Das gesamtstaatliche Cyberkrisenmanagement stellte ein Koordinierungsverfahren zur Bewältigung von Cyber–Krisen dar und umfasste sämtliche Maßnahmen zur Bewältigung einer Cyber–Krise einschließlich der militärischen Landesverteidigung im Cyber–Raum, der außenpolitischen Maßnahmen sowie der Zurechnung von Cyber–Angriffen an einen Akteur. Die Cyber Sicherheit Steuerungsgruppe gab in ihrem Konzept zum Cyberkrisenmanagement vor, dass die administrativen Verfahren zur Bewältigung von Cyber–Krisen in Krisen– und Kontinuitätsplänen bzw. Einsatzplänen festzulegen sind. Bis zum Ende der Gebarungsüberprüfung im November 2022 bestanden keine derartigen gesamtstaatlichen Pläne. (TZ 14)

Das Verteidigungsministerium führte in Strategiepapieren aus, dass das ehemals völkerrechtlich klar normierte Kriegsbild teilweise durch einen subkonventionellen Angriff in allen Bereichen – Land, Luft, Cyber– und Informationsumfeld – in hybrider Form ersetzt wurde. Das Verteidigungsministerium arbeitete daher auch für den Bereich Cyber an Konzepten von konkreten Bedrohungsbildern und –szenarien. Diese sollten die Voraussetzungen für den Einsatz und das Zusammenwirken der

Streitkräfte im Cyber–Raum beschreiben und einer zielgerichteten Weiterentwicklung der Cyber–Kräfte im Bundesheer dienen. Im November 2022 lagen detaillierte Bedrohungsbilder erst im Entwurf vor. (TZ 15)

Mit den 2019 erstellten Planungszielen zum Militärstrategischen Konzept 2017 hatte das Bundesheer Grundlagendokumente zur Fähigkeitenentwicklung ausgearbeitet; diese wurden zur Zeit der Gebarungsüberprüfung aktualisiert. Dokumente mit detaillierten Ausführungen zur Fähigkeitenplanung und –entwicklung im Bereich Cyber lagen allerdings erst im Entwurf vor. Von den darin beschriebenen neun Fähigkeiten war das Verteidigungsministerium lediglich bei einer – der zentralen – Fähigkeit (Schutz und Verteidigung der eigenen IKT–Systeme und Netzwerke) in der Umsetzung weiter fortgeschritten. Weitere Cyber–Fähigkeiten befanden sich erst im Aufbau. (TZ 15)

Das Budget des Verteidigungsministeriums sah für die Jahre 2021 und 2022 ein eigenes Cyber–Sicherheitspaket im Umfang von 40 Mio. EUR vor. In einer schriftlichen Weisung des Chefs des Generalstabs aus dem Jahr 2021 war u.a. festgelegt, wie diese Mittel verwendet werden sollten. Das Verteidigungsministerium teilte mit, dass vom genannten Budget in den Jahren 2021 und 2022 (inklusive Folgebeschaffungen) bereits 40,85 Mio. EUR für Systeme betreffend die nachrichtendienstliche Aufklärung und Abwehr von Cyber–Angriffen, für den generellen Ankauf von spezieller Hard– und Software für den Cyber–Bereich, für Maßnahmen zum Eigenschutz der Cyber–Sicherheit und für den Bereich der elektronischen Kampfführung aufgewendet wurden. Weitere in der Weisung des Chefs des Generalstabs festgelegte Vorhaben – diese betrafen u.a. die militärische Cyber–Range, Einsatzteams und das Security Operation Center – konnten mangels Personalressourcen noch nicht umgesetzt werden. Im November 2022 lagen im Verteidigungsministerium zu diesen Vorhaben erst Planungsunterlagen vor. (TZ 16)

Das Verteidigungsministerium verfolgte verschiedene Ansätze, um im Bereich Cyber–Sicherheit neues Personal aufzubauen und bestehendes Personal auszubilden. In der Führungsunterstützungsschule sowie im sechssemestrigen Fachhochschul–Bachelorstudiengang der Theresianischen Militärakademie wurden das Kaderpersonal bzw. zukünftige IKT–Offizierinnen und –Offiziere zu Expertinnen und Experten für den Einsatz von IKT–Systemen, für elektronische Kampfführung sowie zu Spezialisten für den Betrieb und die Überwachung von militärischen Einsatznetzwerken ausgebildet. (TZ 17)

Zusammenarbeit auf Bundesebene

Neben dem permanenten Eigenschutz der militärischen IKT–Systeme und den anlassbezogenen Cyber–Assistenzleistungen hatte das Verteidigungsministerium wesentliche Aufgaben nach dem NISG als Beitrag zur gesamtstaatlichen Cyber–Sicherheit zu erfüllen. Diese Leistungen wurden weitgehend vom Militärischen Cyberzentrum, vom militärischen Abwehramt und vom militärischen Heeres–Nachrichtenamt erbracht. (TZ 18)

Das Verteidigungsministerium wirkte im Rahmen des „Inneren Kreises der Operativen Koordinierungsstruktur“ (**IKDOK**) gemäß NISG bei der Erstellung eines gesamtstaatlichen Cyber–Lagebildes mit. Darüber hinaus erstellte es eigene militärische Lagebilder, die auch Cyber–Aspekte enthielten. Die dafür notwendigen Cyber–relevanten Informationen stellten nicht nur die zuständigen Organisationen des Verteidigungsministeriums zur Verfügung, sie ergaben sich auch aus Informationen durch den IKDOK, durch das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) sowie von Partnerorganisationen und aus Berichten. Das Verteidigungsministerium hatte allerdings noch nicht festgelegt, ob die Ergebnisse des militärischen Cyber–Lagebildes zur künftigen Beurteilung einer Souveränitätsgefährdung infolge von Cyber–Ereignissen herangezogen werden sollen. Auch die Fragen der 24/7–Verfügbarkeit sowie der strukturierten Informationsweiterleitung an das militärische Computer–Notfallteam und an die künftigen Einsatzteams waren nicht entschieden. (TZ 19)

In den Jahren 2018 bis 2022 nahm das Verteidigungsministerium an insgesamt 32 Cyber–Übungen teil. Im Rahmen der gesamtstaatlichen Cyber–Übung ASDEM2018 hatten das Verteidigungsministerium bzw. das Bundesheer gemeinsam mit dem Innenministerium den Übergang vom Cyberkrisenmanagement des Innenministeriums zum militärisch geleiteten Cyber–Defence–Fall ansatzweise geübt. Spezifische Übungen eines Cyber–Defence–Falls aufgrund einer Souveränitätsgefährdung hatten das Verteidigungsministerium bzw. das Bundesheer jedoch nicht durchgeführt: Es waren weder Konzepte zum Feststellen einer Souveränitätsgefährdung, notwendige Maßnahmen betreffend den Übergang von einer Cyber–Krise in einen Cyber–Defence–Einsatz noch Konzepte zur Zurechnung eines Angriffs an einen staatlichen Akteur erprobt worden. (TZ 20)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen an das Bundesministerium für Landesverteidigung hervor:

ZENTRALE EMPFEHLUNGEN

- Die Fertigstellung der Leitlinie Cyber–Verteidigung wäre voranzutreiben und diese ehestmöglich zu erlassen. (TZ 4)

- Die Konkretisierung des Konzepts Gesamtstaatliches Cyber Krisenmanagement (CKM 2019) wäre im Zusammenwirken mit den anderen Sicherheitsressorts (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für europäische und internationale Angelegenheiten) im Hinblick auf einen Cyber–Defence–Fall weiterzuverfolgen, um die angestrebten Ziele – Klarstellung von Verantwortlichkeiten, Einrichtung von Kommunikationskanälen innerhalb einer und zwischen mehreren Gebietskörperschaften und effiziente Koordination – zu erreichen. (TZ 5)

- In der Leitlinie Cyber–Verteidigung oder anderen geeigneten Dokumenten wären – als Grundlage der Entscheidung über einen Cyber–Defence–Einsatz – Kriterien bzw. Optionen festzulegen, um Souveränitätsverletzungen oder –gefährdungen infolge von Cyber–Angriffen zu beurteilen. Diese hätten jedenfalls die Fragen

  - der Feststellung und Bewertung einer Beeinträchtigung der Unabhängigkeit und Funktionsfähigkeit der Einrichtungen von Gebietskörperschaften und

  - der Bedeutung einzelner kritischer Infrastrukturen hinsichtlich einer Verletzung der Souveränität Österreichs zu behandeln.

  - Darüber hinaus wäre auch zu klären, welches Ausmaß mögliche Auswirkungen eines Cyber–Angriffs erreichen müssten, um einen militärischen Einsatz zu rechtfertigen.

  Damit soll im Anlassfall eine koordinierte, strategisch geleitete und rasche Bewältigung von Gefährdungssituationen sichergestellt werden. (TZ 5)

- Das Vorhaben von zumindest zwei Einsatzteams, das Vorhaben des Security Operation Centers und das Vorhaben der Cyber–Plattform als Trainingszentrum (militärische Cyber–Range) wären umzusetzen. (TZ 16)

- Übungen zu einem Cyber–Defence–Fall mit Souveränitätsgefährdung wären verstärkt durchzuführen: Dabei wären u.a. die Fragen der Feststellung eines Souveränitätsfalls, des Übergangs von einer Cyber–Krise in einen Cyber–Defence–Einsatz und der Zurechnung eines Angreifers an einen staatlichen Akteur zu behandeln. Weitere zu übende Szenarien wären der Schutz der verfassungsmäßigen Einrichtungen und der kritischen Infrastruktur sowohl in Bezug auf einen Cyber–Defence–Einsatz als auch hinsichtlich einer Assistenzleistung. (TZ 20)

Zahlen und Fakten zur Prüfung

Organisation der Cyber–Defence im Verteidigungsministerium	
Rechtsgrundlagen	Art. 79 Bundes–Verfassungsgesetz (B–VG), BGBl. 1/1930 i.d.g.F. Wehrgesetz 2001 (WG 2001), BGBl. I 146/2001 i.d.g.F. Militärbefugnisgesetz (MBG), BGBl. I 86/2000 i.d.g.F. Netz– und Informationssystemsicherheitsgesetz (NISG), BGBl. I 111/2018 i.d.g.F.
Cyber–Raum	Der Cyber–Raum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber–Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.
Cyber–Defence	• ist **militärische Landesverteidigung** im Cyber–Raum (und damit Teil der umfassenden Landesverteidigung), • umfasst **sämtliche vom Bundesheer gesetzten Maßnahmen**, um einen Cyber–Angriff auf die Souveränität Österreichs oder auf Einrichtungen des Bundesheeres mit militärischen Mitteln abzuwehren, • **bezieht sich auf den Cyber–Raum** und soll speziell von den Cyber–Kräften des Bundesheeres mittels Computer Network Operations (Kampf in Computernetzwerken) zum Schutz der eigenen Informations– und Kommunikationstechnologie (IKT), zur Informationsgewinnung über andere IKT–Systeme oder zur Beeinträchtigung des Informationsflusses in IKT–Systemen durchgeführt werden.

Zuständigkeiten im Verteidigungsministerium betreffend Cyber–Defence	
Organisationseinheit	**Aufgabe**
• Generaldirektion Verteidigungspolitik (Sektion I)	verteidigungspolitische Strategieentwicklung
• Generaldirektion für Landesverteidigung:	
Direktion 1 – Einsatz	Einsatz und Einsatzvorbereitung der Streitkräfte
Direktion 6 – IKT und Cyber	wesentliche Teile der Leistungserbringung für die Cyber–Defence durch das IKT & Cybersicherheitszentrum und die Abteilungen IKT–Cyberplanung und IKT–Cybereinsatz
Direktion Fähigkeiten und Grundsatzplanung	Konzeption der Fähigkeiten der Streitkräfte
• Chef des Generalstabs:	
Abwehramt	Beitrag zur Gewährleistung der Sicherheit der militärischen IKT–Infrastruktur, zum Cyber–Lagebild, Vorbereitung offensiver nachrichtendienstlicher Maßnahmen
Heeres–Nachrichtenamt	Erstellung eines gesamtheitlichen Lagebildes (militärisch, politisch, ökonomisch, hybrid) einschließlich Dimension Cyber

Kennzahlen für den Cyber–Bereich im Verteidigungsministerium	
• Cyber–Ereignisse	
– detektierte Sicherheitsereignisse im November 2022	rd. 390.000
– bearbeitete Vorfälle (von 1. Jänner 2022 bis 30. September 2022)	rd. 400
davon eingehend analysierte Vorfälle	*rd. 30*
• **Übungen** im Cyber–Bereich im Zeitraum 2018 bis 2022 mit Beteiligung Verteidigungsministerium/Bundesheer	32

Quellen: Regierungsvorlage NISG; Konzept Cyber Krisenmanagement 2019; Militärstrategisches Konzept 2017; BMLV

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von August bis November 2022 im Bundesministerium für Landesverteidigung (in der Folge: **Verteidigungsministerium**) die Koordination der Cyber–Defence[2].

(2) Die Koordination der Cyber–Sicherheit obliegt gemäß dem Netz– und Informationssystemsicherheitsgesetz (BGBl. I 111/2018 i.d.g.F.) (**NISG**) dem Bundesministerium für Inneres (in der Folge: **Innenministerium**), dem Bundeskanzleramt, dem Bundesministerium für europäische und internationale Angelegenheiten (in der Folge: **Außenministerium**) und dem Verteidigungsministerium (siehe RH–Bericht „Koordination der Cyber–Sicherheit" (Reihe Bund 2022/13, TZ 11, TZ 28)). Das dafür wichtigste interministerielle Gremium war der Innere Kreis der Operativen Koordinierungsstruktur (**IKDOK**), der sich aus diesen Bundesministerien unter Leitung des Innenministeriums zusammensetzte. Darin brachten sie Informationen zur Cyber–Sicherheitslage ein und das Innenministerium generierte daraus das zugehörige Lagebild. Im Cyber–Vorfalls– und –Krisenmanagement ist das Innenministerium für operative Maßnahmen zuständig. Das Österreichische Bundesheer (in der Folge: **Bundesheer**) kann diesbezüglich im Rahmen einer eigens anzufordernden Assistenzleistung mitwirken. Ein sicherheitspolizeilicher Assistenzeinsatz[3] des Bundesheeres (hier für die Cyber–Sicherheit) kann auch von österreichischen Behörden und Organen in Anspruch genommen werden, sofern die im Bundesheer vorhandenen personellen Kapazitäten ausreichen, ohne den prioritären Eigenschutz des Bundesheeres zu beeinträchtigen.

(3) Cyber–Defence ist die Abwehr von Cyber–Angriffen auf die Souveränität des österreichischen Staates (Souveränitätsfall) oder auf die Einrichtungen des Bundesheeres (Eigenschutz). Dafür verantwortlich ist das Verteidigungsministerium im Rahmen der militärischen Landesverteidigung. Beim Übergang von einer Cyber–Krise in einen Cyber–Defence–Einsatz geht die Zuständigkeit auf der operativen Ebene von der Innenministerin bzw. dem Innenminister auf die Verteidigungsministerin bzw. den Verteidigungsminister über. Im Zuge der allgemeinen Einsatzvorbereitung hat das Verteidigungsministerium die ständige Einsatzbereitschaft des Bundesheeres auch zur Abwehr von Cyber–Angriffen sicherzustellen und die erforderlichen personellen und materiellen Voraussetzungen für einen Einsatz im Cyber–Raum zu schaffen.

[2] Der vorliegende Bericht verwendet bei Begriffen mit dem Präfix „Cyber–" grundsätzlich die Schreibweise mit Bindestrich (z.B. „Cyber–Sicherheit"). Ausnahmen bilden Eigennamen – etwa von Gremien oder Strategien – oder wörtliche Zitate.

[3] Ein Assistenzeinsatz für die Cyber–Sicherheit erfolgte im Jänner 2020 im Auftrag des Innenministeriums betreffend die Cyber–Krise im Außenministerium.

(4) Ziele der Gebarungsüberprüfung waren die Darstellung und Beurteilung folgender zentraler Themen:

1. rechtliche Grundlagen für den Souveränitätsfall bzw. den militärischen Eigenschutz im Cyber–Raum (Cyber–Defence),

2. Strategie, Planung und Umsetzung der Cyber–Defence,

3. Organisation und personelle Voraussetzungen der Cyber–Defence im Verteidigungsministerium,

4. Bedrohungsbild, Kompetenzen und Projekte des Verteidigungsministeriums zum Aufbau von Cyber–Kompetenzen,

5. Leistungen des Verteidigungsministeriums für die Cyber–Sicherheit (außerhalb der Cyber–Defence) im Rahmen von Assistenzleistungen, Amtshilfe oder gesetzlich definierten Leistungen.

(5) Der überprüfte Zeitraum umfasste die Jahre 2021 bis November 2022. In Einzelfällen nahm der RH auch Bezug auf Sachverhalte außerhalb dieses Zeitraums.

(6) Nicht Gegenstand der Gebarungsüberprüfung war die 2021 eingeleitete Organisationsreform der Zentralstelle des Verteidigungsministeriums und des Bundesheeres.

(7) Der RH übermittelte das Prüfungsergebnis im April 2023. Wie mit dem Verteidigungsministerium vereinbart, stellte er jene fünf Schlussempfehlungen (2, 4, 5, 18 und 26), die das Verteidigungsministerium nur im Zusammenwirken mit den anderen Sicherheitsressorts (Bundeskanzleramt, Innenministerium und Außenministerium) umsetzen kann, auch diesen Bundesministerien zur Kenntnisnahme zur Verfügung. Darüber hinaus übermittelte der RH jene zwei Schlussempfehlungen (6 und 9), die das Verteidigungsministerium nur im Zusammenwirken mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (in der Folge: **Beamtenministerium**) umsetzen kann, auch diesem Bundesministerium.

Das Verteidigungsministerium nahm im Juli 2023 Stellung, das Beamtenministerium im Mai 2023. Das Bundeskanzleramt, Innenministerium und Außenministerium gaben keine Stellungnahmen ab.

Der RH erstattete seine Gegenäußerung an das Verteidigungsministerium im Oktober 2023. Gegenüber dem Beamtenministerium war keine Gegenäußerung erforderlich.

Cyber–Vorfälle

2.1 (1) Die Österreichische Strategie für Cybersicherheit 2021 hielt zu den Bedrohungen aus dem Cyber–Raum fest, dass staatliche, aber auch nichtstaatliche Akteure den Cyber–Raum als Aktionsfeld für Angriffe verwendeten. Diese reichen von Cyber–Kriminalität und Cyber–Spionage über Cyber–Terrorismus bis hin zur Cyber–Kriegsführung. Potenzielle Angriffsziele können sowohl staatliche als auch private Einrichtungen, insbesondere kritische Infrastrukturen und wesentliche Dienste (gemäß NISG), aber auch militärische Waffen–, Aufklärungs– und Führungssysteme sein.

Folgende Angriffsmethoden können hierbei zum Einsatz kommen:

Tabelle 1: Angriffsmethoden im Cyber–Raum

weitverbreitete Cyber–Angriffsmethoden	Beschreibung
Identitätsdiebstahl	Bei Identitätsdiebstahl bzw. Identitätsmissbrauch durch Cyber–Angriffe versuchen Angreifer, Zugriff auf Teile der Identität eines Nutzers (z.B. Benutzernamen und Passwörter) zu erlangen, um diese für eigene Zwecke verwenden zu können. Beispiele: Phishing, Man–in–the–Middle
Schadsoftware	Schadsoftware (Malware) ist Software, die auf dem Zielrechner schädliche Operationen ausführt. Beispiele: Viren, Trojaner, Würmer, Rootkits, Ransomware oder Spyware
Missbrauch von Internet–Strukturen	Nützliche Internet–Strukturen können als Angriffswerkzeuge missbraucht werden. Andere Internet–Dienste sind speziell für die Durchführung von Cyber–Angriffen entwickelt worden. Beispiele: missbräuchlich verwendete Cloud–Dienstleistungen als Phishing–Seiten, Botnetze, Manipulation oder Missbrauch von Internet–Basisdiensten wie Domain–Name–Services
Hacking	In der IT–Sicherheit werden Angreifer, die sich unbefugt Zugang zu Systemen oder Netzen verschaffen, oft als „Hacker“ bezeichnet. Beispiele: Ausnutzen von Fehlkonfigurationen, von Schwachstellen oder Implementierungsfehlern
Denial–of–Service–Angriffe	Denial–of–Service–Angriffe (DoS, übersetzt „Angriffe auf die Betriebsfähigkeit“) richten sich gegen die Verfügbarkeit, mit der Absicht, Dienste, einzelne Systeme oder ganze Netze zu stören oder vollständig betriebsunfähig zu machen. Beispiele: Spam, Überflutung von Webservern durch eine Vielzahl von Anfragen

Quelle: (deutsches) Bundesamt für Sicherheit in der Informationstechnik (BSI)

Informations– und Kommunikationssysteme müssen daher geschützt werden, um die Authentizität, Vertraulichkeit, Verfügbarkeit und Integrität von Daten zu gewährleisten.

(2) Im Innenministerium wurde die operative nationale NIS–Behörde (**NIS** = Netz– und Informationssystemsicherheit) eingerichtet, die u.a. Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung in der Umsetzung der Vorgaben des NISG unterstützt. Auf Grundlage des NISG betrieb das Innenministerium auch die Meldesammelstelle (RH–Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13)) für Vorfälle, die die Cyber–Sicher-

heit betreffen (Risiken, Vorfälle, Sicherheitsvorfälle). Die dafür zuständige operative NIS–Behörde im Innenministerium[4] erhielt sowohl verpflichtende Meldungen bei Sicherheitsvorfällen[5] als auch freiwillige[6] Meldungen zu Risiken oder Vorfällen.

In den ersten drei Quartalen im Jahr 2022 nahm die NIS–Behörde in Summe rd. 80 verpflichtende bzw. freiwillige Meldungen[7, 8] entgegen. Die Gründe, die zu einer Meldung führten, waren im Wesentlichen Hacking–Angriffe, Schadsoftware (Malware und Virus–Software), aber auch Identitätsdiebstahl. Die Angriffe fanden überwiegend in den Sektoren Gesundheit, Telekommunikation und Banken statt.

(3) Streitkräfte waren in ihrer Einsatzführung zunehmend abhängig von digitalen Systemen und Netzwerken im Cyber–Raum. Unterbrechung, Manipulation und Zerstörung von Daten und IKT–Infrastruktur sowie Datenabfluss konnten die Einsatzfähigkeit der militärischen Landesverteidigung beeinträchtigen.

Das Verteidigungsministerium und damit die für Informations– und Kommunikationstechnologie (**IKT**) und Cyber zuständige „Direktion 6 – IKT und Cyber“ (in der Folge: **Direktion 6**) waren einer Vielzahl von externen Sicherheitsereignissen und Vorfällen ausgesetzt. Allein in der einmonatigen Zeitspanne von Ende Oktober bis Ende November 2022 wurden durch Sicherheitsvorkehrungen wie Firewalls und Bedrohungserkennungssysteme im Netzwerk (Security Information & Event Management–Systeme) rd. 390.000 Sicherheitsereignisse[9] im Verteidigungsministerium automatisiert detektiert und abgewehrt.

[4] Die Innenministerin bzw. der Innenminister war gemäß NISG (§ 5 Abs. 1 Z 3 bzw. § 11 Abs. 1) dazu verpflichtet, Meldungen von Cyber–(Sicherheits–)Vorfällen entgegenzunehmen, zu analysieren und daraus regelmäßig ein Lagebild zu erstellen, um dieses an inländische Behörden oder Stellen weiterzuleiten.

[5] Verpflichtende Meldungen laut NISG von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste, Einrichtungen des Bundes. Ein „Sicherheitsvorfall“ ist gemäß § 3 Z 6 NISG definiert als eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat.

[6] Sonstige Vorfälle (gemäß § 3 Z 7 NISG definiert als Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz– und Informationssystemen haben und kein Sicherheitsvorfall sind) und Risiken (gemäß § 3 Z 8 NISG definiert als alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz– und Informationssystemen haben) konnten von den genannten Einrichtungen und auch von jeder Person freiwillig gemeldet werden.

[7] Daten des Bundeskriminalamts (Cyber–Crime), der Direktion Staatsschutz und Nachrichtendienst und des BMI–internen CSIRT (computer security incident response team = Organisation, die Informationen über Sicherheitsvorfälle sammelt, Analysen durchführt und auf Anfragen reagiert) sind in der Auswertung nicht enthalten.

[8] Seitens der für die IKT des Verteidigungsministeriums zuständigen Direktion 6 waren in den ersten drei Quartalen 2022 keine NIS–Meldungen zu verzeichnen.

[9] Die Sicherheitsereignisse betrafen überwiegend Datenverkehr von verdächtigen IP–Adressen, verdächtige Aktivitäten bzw. verdächtige Nutzung eines Netzwerks. Es wurden aber z.B. auch potenzielle Schadsoftware oder Denial–of–Service–Angriffe (DoS = Verhinderung des Zugriffs auf einen Web–Dienst) durch die Sicherheitseinrichtungen geblockt.

Von den in den ersten drei Quartalen 2022 im Rahmen des militärischen Eigenschutzes festgestellten Sicherheitsereignissen und Vorfällen überprüfte das Verteidigungsministerium rd. 400 Vorfälle genauer. In weiterer Folge analysierte es rd. 30 davon im Detail. Hierbei handelte es sich im Wesentlichen um Angriffe wie Hacking (z.B. Ausnutzung von Schwachstellen), um Versuche des Identitätsdiebstahls (betrügerische, personalisierte E–Mails bzw. Spearphishing[10]) oder um Hinweise auf Hacking–Angriffe, wo Angriffsspuren im eigenen Netzwerk zu kontrollieren waren. Die genannten Vorfälle wurden laut Angaben des Verteidigungsministeriums in einer frühen Phase erkannt, so dass der „Angriffsversuch" zu keiner Beeinträchtigung der Schutzziele geführt hatte. (Eine gemäß NISG verpflichtende Meldung eines Sicherheitsvorfalls lag somit nicht vor.)

2.2 Der RH hielt fest, dass der Schutz und die Verteidigung der eigenen IKT–Systeme und Netzwerke (Eigenschutz) eine umfassend und permanent zu leistende Aufgabe für das Verteidigungsministerium und damit für die Direktion 6 und die nachrichtendienstlichen Ämter ist (siehe TZ 13).

Grundlagen

Rechtliche Grundlagen

3 (1) Die Aufgaben des Bundesheeres sind verfassungsrechtlich in

- Art. 79 Bundes–Verfassungsgesetz (**B–VG;** BGBl. 1/1930 i.d.g.F.) und im
- Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland (KSE–BVG; BGBl. I 38/1997 i.d.g.F.)

festgelegt. Auf einfachgesetzlicher Ebene präzisieren das

- Wehrgesetz 2001 (WG 2001; BGBl. I 146/2001 i.d.g.F.) die Aufgaben und das
- Militärbefugnisgesetz (MBG; BGBl. I 86/2000 i.d.g.F.) die Mittel und Befugnisse des Bundesheeres.

Alle Leistungen des Bundesheeres im Cyber–Raum waren im Rahmen dieser verfassungsrechtlich festgelegten Aufgaben zu erbringen.

[10] Beim Spearphishing versenden Cyber–Kriminelle gezielt betrügerische E–Mails, die sich gegen bestimmte Organisationen oder bestimmte Personen richten. Spearphishing–Versuche werden von Tätern initiiert, die konkret auf Geschäftsgeheimnisse, finanzielle Gewinne oder auch militärische Informationen aus sind.

Die folgende Tabelle stellt die Aufgaben im Überblick dar:

Tabelle 2: Aufgaben des Österreichischen Bundesheeres

Leistungen des Bundesheeres im Cyber–Raum und Aufgaben nach dem Bundes–Verfassungsgesetz (B–VG)			
Cyber–Aufgaben	Cyber–Defence	Assistenz in Cyber–Krise	internationale Übungen und Operationen
Rechtsgrundlagen	Art. 79 B–VG		KSE–BVG
	§ 2 Wehrgesetz 2001		§ 2 Wehrgesetz 2001
	Militärbefugnisgesetz		
Einteilung	primäre Kernaufgabe	subsidiäre Assistenz	Auslandseinsatz
Aufgabe	militärische Landesverteidigung inklusive Eigenschutz militärischer Rechtsgüter • allgemeine Einsatzvorbereitung • unmittelbare Vorbereitung eines Einsatzes • Einsatz	sicherheitspolizeiliche Assistenz	Entsendung in das Ausland • Friedenssicherung • internationale Katastrophenfälle • Übungen
		Assistenz in Katastrophenfällen	
Verantwortlichkeit	Verteidigungsministerium/Bundesheer	heranziehende Behörden und Organe („zivile Gewalt“)	Bundesregierung, Verteidigungsministerium

KSE–BVG = Bundesverfassungsgesetz über Kooperation und Solidarität bei der Entsendung von Einheiten und Einzelpersonen in das Ausland

Quellen: bezughabende Rechtsquellen

(2) Die Abwehr von Cyber–Angriffen auf militärische Rechtsgüter (§ 1 Abs. 7 und 8 MBG), insbesondere IKT–Systeme, ist zur Gewährleistung der IT–Sicherheit eine vorrangige und permanente Aufgabe im Rahmen der militärischen Landesverteidigung (TZ 2). Dieser unmittelbare Eigenschutz trägt dazu bei, die militärische Einsatzfähigkeit aufrechterhalten zu können.[11]

(3) Die Abwehr von Cyber–Angriffen auf die Souveränität Österreichs (Art. 9a B–VG) durch einen anderen Staat oder durch eine staatlich gelenkte Organisation war eine anlassbezogene Aufgabe im Rahmen der militärischen Landesverteidigung. Ein Cyber–Angriff auf Österreich, der einen Souveränitätsfall ausgelöst hätte, war bis zum Ende der Gebarungsüberprüfung nicht eingetreten.

In einem solchen Anlassfall erweitert sich der Aufgabenbereich des Bundesheeres auch auf den Schutz der IKT–Systeme der verfassungsmäßigen Einrichtungen der Republik Österreich und den Schutz kritischer Infrastrukturen, soweit diese für die militärische Einsatzführung und Sicherstellung der Souveränität relevant sind. Die Verfügung über einen (Cyber–Defence–)Einsatz des Bundesheeres zur militärischen Landesverteidigung obliegt der Verteidigungsministerin bzw. dem Verteidigungsminister innerhalb der ihr bzw. ihm von der Bundesregierung erteilten Ermächti-

[11] Für die „wichtigen Dienste“ des Verteidigungsministeriums waren technische und organisatorische Sicherheitsvorkehrungen auch nach dem NISG geboten.

gung[12] (Art. 80 Abs. 2 B–VG). Der Schutz ist durch den Kampf in Computernetzwerken (Computer Network Operations) sicherzustellen. Dies umfasst die Verteidigung der angegriffenen IKT–Systeme zur Abwehr von Cyber–Angriffen, die Ausnützung fremder IKT–Systeme zur Informationssammlung und den Angriff auf IKT–Systeme, um Cyber–Angriffe zu beenden (Militärstrategisches Konzept 2017, S. 8 f.; vgl. § 17 Z 2 Militärbefugnisgesetz).

(4) Die Aufgaben des Bundesheeres umfassen nicht nur den Einsatz, sondern auch die allgemeine Einsatzvorbereitung (§ 2 Wehrgesetz 2001). Daher haben das Verteidigungsministerium und das Bundesheer die ständige Einsatzbereitschaft für den Cyber–Defence–Fall sicherzustellen, indem sie die personellen und materiellen Voraussetzungen für eine wirksame Einsatzdurchführung schaffen. Dazu gehörten auch Planungs–, Übungs– und Ausbildungsmaßnahmen sowie Maßnahmen zur Gewährleistung der IT–Sicherheit der militärischen IKT–Systeme im Zusammenhang mit möglichen Cyber–Angriffen.

(5) Subsidiär kann auch die zivile Gewalt – grundsätzlich alle Behörden und Organe des Bundes, der Länder und Gemeinden – das Bundesheer im Rahmen eines Assistenzeinsatzes zur Abwehr von Cyber–Angriffen, die nicht die militärische Landesverteidigung betreffen, in Anspruch nehmen (zu den näheren Voraussetzungen siehe TZ 6)[13].

(6) Nach Art. 9 B–VG galten die allgemein anerkannten Regeln des Völkerrechts als Bestandteile des Bundesrechts. Maßnahmen zur Verteidigung der Souveränität eines Staates müssen nach einhelliger Meinung auch im Cyber–Raum im Einklang mit dem Völkerrecht stehen, insbesondere mit

- der Satzung (Art. 51) der Vereinten Nationen (Gewaltverbot, Selbstverteidigungsrecht von Staaten gegen einen bewaffneten Angriff),
- dem humanitären Völkerrecht[14] (keine direkten Angriffe auf Zivilisten und zivile Objekte in einem bewaffneten Konflikt) und
- der völkergewohnheitsrechtlichen[15] Due–Diligence–Pflicht (dieser zufolge muss der Staat dafür sorgen, dass Handlungen innerhalb seines Hoheitsbereichs die Souveränität anderer Staaten nicht verletzen).

[12] Ministerratsbeschluss 64/5 vom 6. November 1984: „Die Bundesregierung erteilt dem Bundesminister für Landesverteidigung die Ermächtigung, den Einsatz des Bundesheeres aufgrund von Richtlinien zu verfügen, die die Bundesregierung im jeweiligen Bedarfsfall zu beschließen hat. Bei Gefahr in Verzug hat der Bundesminister für Landesverteidigung den Bundeskanzler über die bereits vor Beschlussfassung einer Richtlinie getroffenen erforderlichen Maßnahmen laufend zu informieren."

[13] Im Juli 2023 beschloss der Nationalrat das Bundes–Krisensicherheitsgesetz, das mit Jänner 2024 in Kraft treten wird. Dieses Gesetz trifft Vorsorge für allgemeine Krisen und bezieht sich nicht ausdrücklich auf Cyber–Krisen (für Cyber–Krisen bleibt das NISG anwendbar).

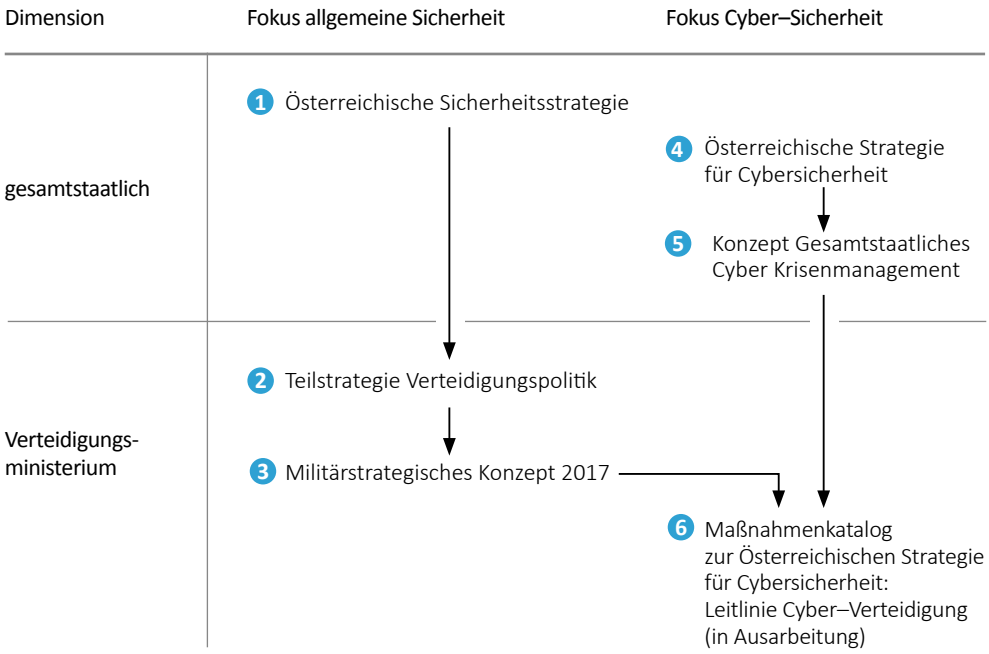
[14] insbesondere Genfer Abkommen zum Schutze von Zivilpersonen (1949) und Zusatzprotokoll I und II (1977)

[15] Völkergewohnheitsrecht ist eine Form ungeschriebenen Völkerrechts, das durch allgemeine Übung, getragen von der Überzeugung der rechtlichen Verbindlichkeit der Norm, entsteht.

Strategische Grundlagen

4.1 (1) Die folgende Abbildung gibt einen Überblick über die gesamtstaatlichen sowie militärischen Strategien zu den Themen Sicherheit und Verteidigung sowie Cyber–Sicherheit und Cyber–Defence:

Abbildung 1: Überblick über Strategien mit Relevanz für die Cyber–Defence



Quelle: BMLV; Darstellung: RH

(2) Die Österreichische Sicherheitsstrategie 2013 (in der Folge: **Sicherheitsstrategie 2013**)[16] war eine gesamtstaatliche Strategie zur „Umfassenden Sicherheitsvorsorge“ (äußere und innere, zivile und militärische Sicherheit). Sie nannte die Bewältigung von Cyber–Angriffen als militärisches Aufgabenfeld, enthielt dazu aber keine weiteren Ausführungen.

(3) Die Teilstrategie Verteidigungspolitik aus 2014 beschrieb in Umsetzung der Sicherheitsstrategie 2013 die Zielsetzungen für den Teilbereich militärische Verteidigung und die Aufgaben des Bundesheeres. Dabei bezog sie den Cyber–Bereich jeweils ausdrücklich in das Leistungsprofil des Bundesheeres ein: Abwehr von Cyber–Angriffen auf die Souveränität Österreichs, militärischer Eigenschutz im Cyber–Raum, Assistenzeinsätze zur Gewährleistung der Cyber–Sicherheit. Insbe-

[16] beruhend auf einer Entschließung des Nationalrats vom 3. Juli 2013, mit der die Bundesregierung ersucht wurde, die Sicherheitspolitik nach vorgegebenen Grundsätzen zu gestalten

sondere hob sie die Notwendigkeit für einen gesicherten Übergang von der sicherheitspolizeilichen Assistenzleistung in die militärische Cyber–Verteidigung hervor.[17]

(4) Das Militärstrategische Konzept 2017 (MSK 2017) bildete gemeinsam mit den 2022 aktualisierten Planungszielen (Soll–Zielen) die Grundlage für die Streitkräfteentwicklung. Es konkretisierte die Aufgaben des Bundesheeres gesamt sowie für den Cyber–Raum die Aufgaben der Cyber–Kräfte (insbesondere der Cyber–Truppe). Die im Militärstrategischen Konzept 2017 aufgestellten Grundsätze für die zu entwickelnden Fähigkeiten (z.B. Einsatzorientierung) waren in den Planungszielen bei der Festlegung der konkreten Fähigkeitsanforderungen (z.B. permanente Einsatzbereitschaft der Cyber–Kräfte) zu berücksichtigen. Darauf aufbauend waren Konzepte zu den anzuwendenden Verfahren (z.B. Kampf in Computernetzwerken) und zur Umsetzung der angestrebten Fähigkeiten zu erstellen (TZ 15).

(5) Für den Bereich Cyber–Sicherheit gab es ab 2013 eine eigene gesamtstaatliche, auf den Grundsätzen der Sicherheitsstrategie 2013 beruhende Österreichische Strategie für Cybersicherheit (in der Folge: **Strategie für Cybersicherheit**). Die zur Zeit der Gebarungsüberprüfung aktuelle Version stammte von Dezember 2021 (Strategie für Cybersicherheit 2021; Ministerratsbeschluss vom 23. Dezember 2021). Die Cyber–Verteidigung war als Teil der gesamtstaatlichen Cyber–Sicherheitsvorsorge festgelegt, die Einsatzführung dafür der Verteidigungsministerin bzw. dem Verteidigungsminister zugewiesen.

(6) Im Juli 2019 beschloss die Cyber Sicherheit Steuerungsgruppe ein Konzept zum Gesamtstaatlichen Cyber Krisenmanagement (CKM 2019), das sich noch auf den Auftrag der Strategie für Cybersicherheit in der Fassung 2013 zur Einrichtung eines Cyberkrisenmanagements bezog. Dieses hielt allgemeine Voraussetzungen und Zuständigkeiten für die Cyber–Verteidigung fest und unterschied diese vom im NISG vorgesehenen Cyberkrisenmanagement. Der Übergang von einer Cyber–Krise (Innenministerium) in die Cyber–Verteidigung (Verteidigungsministerium) sollte zu keinem Bruch in der Umsetzung von Maßnahmen führen. Die für eine Cyber–Krise eingerichteten Strukturen (z.B. Koordinationsausschuss) sollten auch im Cyber–Defence–Einsatz genutzt werden, um Doppelgleisigkeiten und Informationsverluste zu vermeiden.

(7) Ergänzend zum strategischen Rahmen der Strategie für Cybersicherheit 2021 hatten die Bundesministerien regelmäßig in Abstimmung mit der Cyber Sicherheit Steuerungsgruppe konkrete Maßnahmen zur Cyber–Sicherheitsvorsorge zu beauftragen (Maßnahmenkatalog zur Strategie für Cybersicherheit 2021). Das Verteidigungsministerium verfolgte u.a. die Maßnahme „Erstellen einer Cyberverteidigungsstra-

[17] Diese Forderung ging aus der Entschließung des Nationalrats betreffend die Sicherheitsstrategie 2013 vom 3. Juli 2013 hervor und fand sich deckungsgleich in der Teilstrategie Innere Sicherheit 2015 des Innenministeriums (S. 9).

tegie und eines Fähigkeitenprofils zur Cyberverteidigung“. Zur Zeit der Gebarungsüberprüfung war die Cyber–Verteidigungsstrategie (**Leitlinie Cyber–Verteidigung**) noch in Ausarbeitung.[18] Sie sollte die strategische Ausrichtung der Cyber–Verteidigung definieren. Die für den militärischen Eigenschutz relevante IKT–Sicherheitsstrategie des Verteidigungsministeriums wurde im Oktober 2022 neu erlassen.

4.2 Der RH sah die Fertigstellung der Strategie des Verteidigungsministeriums zur Cyber–Verteidigung als vorrangige Aufgabe, da bereits die Sicherheitsstrategie 2013 die Bewältigung von Cyber–Angriffen als militärisches Aufgabenfeld definierte und die Strategie für Cybersicherheit 2021 konkrete Maßnahmen der Bundesministerien zur Cyber–Sicherheitsvorsorge einforderte.

Der RH empfahl dem Verteidigungsministerium, die Fertigstellung der Leitlinie Cyber–Verteidigung voranzutreiben und diese ehestmöglich zu erlassen (zu den empfohlenen Inhalten siehe TZ 5).

4.3 In seiner Stellungnahme verwies das Verteidigungsministerium auf seine Bestrebungen, die strategischen Planungsdokumente wie die Leitlinie Cyber–Verteidigung und dazu erforderliche Konzepte fertigzustellen.

4.4 Zum Vorbringen des Verteidigungsministeriums, bestrebt zu sein, die Leitlinie Cyber–Verteidigung fertigzustellen, hielt der RH fest, dass sie nicht nur für die strategische Planung erforderlich, sondern auch Grundlage für andere Konzepte war (z.B. Querschnittskonzept „Einsatz im Cyber–Raum“ oder „Einsatzorganisation der Direktion 6“). Ihrer raschen Fertigstellung kam daher besondere Bedeutung zu.

Entscheidung über einen Cyber–Defence–Einsatz

5.1 (1) Ziel des Gesamtstaatlichen Cyber Krisenmanagements (CKM 2019) als besondere Lage des Staatlichen Krisen– und Katastrophenschutzmanagements (SKKM) war es, alle relevanten staatlichen Stellen (insbesondere Bundesministerien, Ämter der Landesregierungen, Gemeinden) und die Einsatzkräfte zu einem gesamtstaatlichen Handeln im Rahmen der jeweiligen gesetzlichen Aufgaben zusammenzufassen.

Das Konzept Gesamtstaatliches Cyber Krisenmanagement (CKM 2019) ging davon aus, dass zur Vermeidung von Doppelgleisigkeiten die für das Cyberkrisenmanagement des Innenministeriums eingerichteten Strukturen auch für die militärische Landesverteidigung im Cyber–Raum zu nutzen wären. Im Koordinationsausschuss nach NISG könnte also die gesamtstaatliche Abstimmung über einen Cyber–

[18] Die Ausarbeitung der Leitlinie erfolgte im Rahmen eines im Mai 2021 verfügten Projekts; der vorliegende zweite Entwurf vom 22. September 2022 befand sich im ressortinternen Stellungnahmeverfahren.

Defence–Einsatz erfolgen. Anders als für die im NISG definierte Cyber–Krise beruhte dies aber nicht auf einer ausdrücklichen gesetzlichen Anordnung.

Ein gesamtstaatliches Konzept, das die Verantwortlichkeiten im Detail klarstellt, die einzelnen Verfahrensschritte bis zur Entscheidung über einen Cyber–Defence–Einsatz konkretisiert, die erforderlichen Kommunikationskanäle – auch zwischen mehreren Gebietskörperschaften – definiert und zu einem koordinierten Zusammenwirken aller beteiligten staatlichen Stellen beiträgt, lag nicht vor.

(2) Im Anlassfall hatte die Verteidigungsministerin den Eintritt einer Souveränitätsgefährdung zu beurteilen, weil es ihr oblag, einen allfälligen Einsatz zur militärischen Landesverteidigung (innerhalb der von der Bundesregierung erteilten Ermächtigung, TZ 3) zu verfügen. Darüber hinaus war eine gesamtstaatliche Abstimmung mit der Bundesregierung und insbesondere den Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium) erforderlich. Die vorhandenen verteidigungspolitischen und militärstrategischen Grundsatzdokumente enthielten allgemeine Umschreibungen, unter welchen Voraussetzungen die Souveränität Österreichs durch einen Cyber–Angriff verletzt wäre: Dies wäre insbesondere dann der Fall, wenn die Abwehr des Angriffs auf militärische IKT–Systeme, kritische Infrastrukturen oder verfassungsmäßige[19] Einrichtungen nur mit militärischen Mitteln erreicht werden kann (siehe dazu Militärstrategisches Konzept 2017, S. 5, 8; Trends und Konfliktbild 2030, S. 44). Weitergehende Kriterien für die Beurteilung der Souveränitätsverletzung bzw. –gefährdung waren in den strategischen Dokumenten nicht ausgeführt. Das Verteidigungsministerium verwies hierzu auf die Ausarbeitung der Leitlinie Cyber–Verteidigung (TZ 12).

(3) Ein Kriterium für die Entscheidung, ob Maßnahmen gegen einen Cyber–Angriff auf Ebene der militärischen Landesverteidigung zu treffen sind, war die Zurechnung (Attribuierung) eines Cyber–Angriffs an einen staatlichen bzw. staatsnahen Akteur.[20] Die einzelnen Schritte einer solchen Zurechnung, die mehrere Bundesministerien betraf, waren im Konzept Gesamtstaatliches Cyber Krisenmanagement (CKM 2019) in groben Zügen festgelegt. Das Verteidigungsministerium hatte im Jänner 2022 dazu einen weitergehenden Vorschlag in einem Untergremium der Cyber Sicherheit Steuerungsgruppe eingebracht, der bis zur Zeit der Gebarungsüberprüfung noch nicht abschließend behandelt war.

[19] Verfassungsmäßige Einrichtungen waren alle durch Verfassungsgesetz eingerichteten Organe; z.B. oberste Organe der Vollziehung und der Gerichtsbarkeit sowie gesetzgebende Organe aller Gebietskörperschaften. Im weiteren Sinn waren darunter auch die grundsätzlichen Organisationsprinzipien des Bundesverfassungsrechts und der Landesverfassungsrechte zu verstehen (*Truppe* in *Kneihs/Lienbacher*, B–VG Art. 79 Rz 32).

[20] Maßnahmen gegen einen anderen Staat setzen nach Völkerrecht die Verantwortlichkeit dieses Staates für den Cyber–Angriff und damit die Zurechnung an ihn voraus.

5.2 (1) Der RH hielt kritisch fest, dass im Konzept Gesamtstaatliches Cyber Krisenmanagement (CKM 2019)

- die operativen Schritte und konkreten Verantwortlichkeiten bis zur Entscheidung der Verteidigungsministerin oder des Verteidigungsministers bzw. der Bundesregierung über einen Cyber–Defence–Einsatz lediglich in groben Zügen festgelegt waren und
- für die gesamtstaatliche Abstimmung lediglich allgemein auf die organisatorischen Strukturen des Cyberkrisenmanagements (unter der Leitung des Innenministeriums) verwiesen wurde.

Der RH empfahl dem Verteidigungsministerium, die Konkretisierung des Konzepts Gesamtstaatliches Cyber Krisenmanagement (CKM 2019) im Zusammenwirken mit den anderen Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium) im Hinblick auf einen Cyber–Defence–Fall weiterzuverfolgen, um die angestrebten Ziele – Klarstellung von Verantwortlichkeiten, Einrichtung von Kommunikationskanälen innerhalb einer und zwischen mehreren Gebietskörperschaften und effiziente Koordination – zu erreichen.

(2) Der RH kritisierte, dass das Verteidigungsministerium noch keine konkreten Beurteilungskriterien bzw. Szenarien ausgearbeitet hatte, anhand derer über einen Cyber–Defence–Einsatz entschieden werden kann.

Er empfahl dem Verteidigungsministerium, in der Leitlinie Cyber–Verteidigung oder anderen geeigneten Dokumenten – als Grundlage der Entscheidung über einen Cyber–Defence–Einsatz – Kriterien bzw. Optionen festzulegen, um Souveränitätsverletzungen oder –gefährdungen infolge von Cyber–Angriffen zu beurteilen. Diese Dokumente hätten jedenfalls die Fragen

- der Feststellung und Bewertung einer Beeinträchtigung der Unabhängigkeit und Funktionsfähigkeit der Einrichtungen von Gebietskörperschaften und
- der Bedeutung einzelner kritischer Infrastrukturen[21] hinsichtlich einer Verletzung der Souveränität Österreichs zu behandeln.
- Darüber hinaus wäre auch zu klären, welches Ausmaß mögliche Auswirkungen eines Cyber–Angriffs erreichen müssten, um einen militärischen Einsatz zu rechtfertigen.

Damit soll im Anlassfall eine koordinierte, strategisch geleitete und rasche Bewältigung von Gefährdungssituationen sichergestellt werden.

[21] § 22 Sicherheitspolizeigesetz definiert als kritische Infrastrukturen alle Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher IKT, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben.

(3) Der RH stellte kritisch fest, dass das Untergremium der Cyber Sicherheit Steuerungsgruppe den vom Verteidigungsministerium ausgearbeiteten Vorschlag für eine Zurechnung (Attribuierung) eines Cyber–Angriffs an einen staatlichen bzw. staatsnahen Akteur bis zum Ende der Gebarungsüberprüfung noch nicht abschließend behandelt hatte.

Der RH empfahl dem Verteidigungsministerium, gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium) die Umsetzung des Vorschlags für ein Verfahrenskonzept hinsichtlich der Zurechnung (Attribuierung) eines Cyber–Angriffs an einen staatlichen bzw. staatsnahen Akteur voranzutreiben; das Verfahrenskonzept wäre in Form eines aktualisierten Konzepts operativ zu setzen.

5.3 Laut Stellungnahme des Verteidigungsministeriums werde es die Empfehlung innerhalb seines Wirkungsbereichs in einem separaten Schritt bearbeiten. Die darüber hinaus fachlich involvierten Ressorts bzw. Dienststellen würden eingeladen.

Hinsichtlich der fehlenden Szenarien für eine Souveränitätsgefährdung bzw. –verletzung im Cyber–Raum verweise das Verteidigungsministerium auf die rechtlichen Beurteilungen. Es würden im Cyber–Raum dieselben rechtlichen Rahmenbedingungen für die militärische Landesverteidigung gelten wie auch zu Land oder zu Wasser.

Die Feststellungen des RH zu den konzeptionellen Lücken (u.a. Attribuierungskonzept) seien plausibel und nachvollziehbar.

Das Verteidigungsministerium sei bestrebt (siehe auch TZ 4), die strategischen Planungsdokumente, wie die Leitlinie Cyber–Verteidigung, und dazu erforderliche Konzepte fertigzustellen.

Assistenzleistungen bei Cyber–Angriffen

6.1 (1) Neben der Kernaufgabe der militärischen Landesverteidigung normierte Art. 79 Abs. 2 B–VG subsidiär („ferner“) die sicherheitspolizeiliche Assistenz als Aufgabe des Bundesheeres. Die Assistenzleistung erfolgte nur auf Anforderung[22] anderer Behörden und Organe, denen das Einschreiten von Angehörigen des Bundesheeres funktionell zuzurechnen war. Das Bundesheer war dabei aufgrund der für die anfordernden Behörden geltenden Rechtsgrundlagen und Befugnisse tätig (zu den allgemeinen Voraussetzungen eines Assistenzeinsatzes siehe RH–Bericht „Assistenz– und Unterstützungsleistungen des Bundesheeres zum Grenzmanagement“; (Reihe Bund 2020/38, TZ 5, TZ 6)). Im Cyber–Bereich erbrachte das Verteidigungs-

[22] Selbstständiges militärisches Einschreiten war zu diesen Zwecken nur im Ausnahmefall zulässig (höhere Gewalt, Angriff auf das Bundesheer).

ministerium bzw. das Bundesheer bisher in einem Fall eine Assistenzleistung mit seinen Cyber–Kräften in einer festgestellten Cyber–Krise. Diese betraf einen verdeckten Cyber–Angriff auf die IT–Systeme des Außenministeriums im Dezember 2019 (siehe RH–Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 24 f.)).

(2) Das Wehrgesetz 2001 berechtigte aufgrund der verfassungsgesetzlichen Ermächtigung alle Behörden und Organe des Bundes, der Länder und Gemeinden in ihrem jeweiligen Wirkungsbereich zur Anforderung einer Assistenzleistung. Voraussetzung war, dass sie die ihnen zukommende Aufgabe nur unter Mitwirkung des Bundesheeres erfüllen konnten; diese Aufgabe umfasste den Schutz

- der verfassungsmäßigen Einrichtungen (inklusive der Verfassungsordnung an sich) und
- ihrer Handlungsfähigkeit sowie
- der demokratischen Freiheiten der Einwohnerinnen und Einwohner und
- der Aufrechterhaltung der Ordnung und Sicherheit im Inneren.

Laut Gesetzesmaterialien (Regierungsvorlage Wehrgesetz–Novelle 2001, 300 BlgNR 21. Gesetzgebungsperiode S. 29) soll die Assistenzleistung durch das Bundesheer als ultima ratio nur dann zulässig sein, wenn die originär zuständige Stelle die konkrete Aufgabe weder mit eigenen Mitteln noch unter Heranziehung kurzfristig aufgebotener Mittel bewältigen konnte. Daher durften Assistenzleistungen auch nicht unbefristet erbracht werden. Die Kosten für den eigenen Personal– und (Amts–) Sachaufwand trug das Verteidigungsministerium.[23]

(3) Eine den (verfassungs–)gesetzlichen Vorgaben entsprechende Anforderung einer Assistenzleistung stellte eine Weisung dar (Sonderverfügungsrecht der zivilen Behörden), der grundsätzlich zu folgen war (§ 33 Abs. 2 Allgemeine Dienstvorschriften für das Bundesheer, BGBl. 43/1979 i.d.g.F.). Der Einsatz zur militärischen Landesverteidigung (inklusive des militärischen Eigenschutzes) hatte jedoch Vorrang vor der Erbringung von Assistenzleistungen.

(4) Das Verteidigungsministerium vertrat die Rechtsansicht, dass „unter dem ausschließlichen Gesichtspunkt möglicher Assistenzeinsätze keine militärischen Kapazitäten bzw. Strukturen abgeleitet werden können und Assistenzeinsätze mit den für die strukturbegründenden verfassungsmäßigen Aufgaben (militärische Landesverteidigung) bereitgestellten militärischen Fähigkeiten zu erfüllen sind“ (Planungsziele zum Militärstrategischen Konzept 2017 (Version 2022); internes Rechtsgutachten). Diese Rechtsansicht beruhte auf der Assistenzleistung als ultima ratio (Wehrgesetz) und als subsidiäre Aufgabe gegenüber der Kernaufgabe der militärischen Landesverteidigung.

[23] „Übertragene“ Aufgaben als „Besorgung ihrer Aufgaben“ nach § 2 Finanz–Verfassungsgesetz, BGBl. 45/1948 i.d.g.F. Nicht vom Verteidigungsministerium getragen wird der Zweckaufwand.

(5) Gleichzeitig wurde mehrfach festgehalten, dass die Mitwirkung des Verteidigungsministeriums an der gesamtstaatlichen Cyber–Sicherheit von wesentlicher Bedeutung war:

- Dies betonten sowohl die gesamtstaatlichen Sicherheitsstrategien (Sicherheitsstrategie 2013, Strategie für Cybersicherheit 2021) als auch die daraus abgeleiteten Strategien des Verteidigungsministeriums (Teilstrategie Verteidigungspolitik 2014, Militärstrategisches Konzept 2017).
- Der Nationalrat forderte in einer Entschließung vom Juli 2013 (zur Sicherheitsstrategie 2013) dazu auf, die für Assistenzeinsätze (ausdrücklich auch im Cyber–Raum) notwendigen Fähigkeiten des Bundesheeres in einem gesamtstaatlichen Planungsprozess[24] festzulegen und regelmäßig fortzuschreiben.
- Im Zusammenhang mit der Cyber–Krise beim Außenministerium empfahl der Nationale Sicherheitsrat im Februar 2020, das Verteidigungsministerium und das Innenministerium personell und technisch ausreichend auszustatten, so dass die permanente Einsatzfähigkeit von Cyber–Kräften gewährleistet ist.
- Auch im Rahmen des NISG erbrachte das Bundesheer laufend Leistungen für die gesamtstaatliche Cyber–Sicherheit (siehe TZ 7, TZ 18).
- Zwei weitere mögliche Szenarien im Zusammenhang mit Cyber–Assistenzleistungen des Bundesheeres waren,
  - dass in einer vom Innenministerium zu koordinierenden Cyber–Krise die Assistenzleistung des Bundesheeres aufgrund steigender, schwerwiegender Auswirkungen in einen Cyber–Defence–Fall übergeht und damit auch die koordinative Zuständigkeit für Maßnahmen zur Bewältigung des Cyber–Angriffs vom Innenministerium auf das Verteidigungsministerium übergeht oder
  - dass parallel zu einem Cyber–Defence–Fall eine Cyber–Assistenzleistung des Bundesheeres für andere Behörden nötig ist.

6.2 (1) Der RH wies darauf hin, dass die Entschließung des Nationalrats, die für Assistenzeinsätze (ausdrücklich auch im Cyber–Raum) notwendigen Fähigkeiten des Bundesheeres in einem gesamtstaatlichen Planungsprozess festzulegen und regelmäßig fortzuschreiben, jedenfalls über eine anlassbezogene Planung eines konkreten Assistenzeinsatzes hinausging. Weiters hielt er fest, dass die gesamtstaatlichen Sicherheitsstrategien die Assistenzleistungen des Bundesheeres (u.a. auch zur Abwehr von Cyber–Angriffen) – ergänzend zu den erforderlichen Maßnahmen durch die zivilen Kräfte – als wesentlichen und unabdingbaren Beitrag zur gesamtstaatlichen Krisenbewältigung betrachteten. Die verschiedenen Szenarien der Mitwirkung des Verteidigungsministeriums an der gesamtstaatlichen Cyber–Sicherheit machten deutlich, dass eine frühzeitige inhaltliche Einbindung des Verteidigungsministeriums in die Abwehr von Cyber–Angriffen (z.B. über eine Assistenzleistung) notwendig war.

[24] Bisher erließ das Innenministerium in Abstimmung mit dem Verteidigungsministerium eine Richtlinie für den Assistenzeinsatz an seine nachgeordneten Dienststellen.

Der RH empfahl dem Verteidigungsministerium, gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium) in einen permanenten Austausch hinsichtlich der Parameter für Assistenzleistungen im Cyber–Bereich einzutreten.

(2) Der RH wies in diesem Zusammenhang darauf hin, dass Cyber–Defence – unabhängig von Assistenzeinsätzen – von der militärischen Verteidigungsaufgabe umfasst ist.

Er empfahl dem Verteidigungsministerium, gemeinsam mit dem Beamtenministerium – in Umsetzung eines gesamtstaatlichen Cyber–Sicherheitskonzepts sowie der Empfehlung des Nationalen Sicherheitsrates vom Februar 2020 – für eine ausreichende personelle und technische Ausstattung zu sorgen, um die permanente Einsatzfähigkeit von Cyber–Kräften zu gewährleisten.

6.3 (1) Laut Stellungnahme des Verteidigungsministeriums könne ohne qualifizierten Personalzuwachs die Fähigkeitenentwicklung im Bereich der Cyber–Verteidigung kaum realisiert werden. Die konkreten Vorhaben und Maßnahmen seien im Rahmen der Gebarungsüberprüfung angesprochen worden.

Der Umfang des (für die Direktion 6) angestrebten Organisationsplans orientiere sich strikt am Pfad der weiterführenden bestehenden Kennzahl „Verbesserung der Fähigkeiten der militärischen Landesverteidigung im Cyber–Raum [...] Personeller Aufwuchs des spezialisierten Cyberpersonals“ im Wirkungsziel 1. Die Berechnung folge den bisher weiterentwickelten Planungen für die mögliche Erreichung der zweiten Ausbaustufe.

(2) Das Beamtenministerium gab in seiner Stellungnahme an, dass es maßgeblich zur Umsetzung des Beschlusses des Nationalen Sicherheitsrates vom 28. Februar 2020 betreffend Stärkung der Cyber–Abwehr beitrage; dies durch die in allen Bundesministerien mögliche Einrichtung von spezialisierten IT–Security–Arbeitsplätzen, die bereits nach dem neuen IT–Besoldungssystem (RIVIT) deutlich besser bezahlt werden könnten.

6.4 Der RH erwiderte dem Verteidigungsministerium, dass nach Genehmigung des Organisationsplans des Militärischen Cyberzentrums durch das Beamtenministerium (siehe TZ 9) die Grundlage geschaffen wurde, die geplante Personalentwicklung umzusetzen.

Rechtliche Grundlagen für weitere Leistungen des Verteidigungsministeriums im Cyber–Bereich

7.1 (1) Im NISG festgelegte Aufgaben

Nach dem NISG hatte das Verteidigungsministerium permanente Aufgaben als Beitrag zur gesamtstaatlichen Cyber–Sicherheit zu erfüllen (siehe RH–Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13, TZ 6, TZ 13 ff., TZ 19 f.)). Diese bezogen sich auf die laufende Zusammenarbeit der vier Sicherheitsressorts Bundeskanzleramt, Innenministerium, Außenministerium und Verteidigungsministerium. Das Verteidigungsministerium wirkte hierbei insbesondere bei der Erstellung des Lagebildes, in den Gremien IKDOK und Operative Koordinierungsstruktur (**OpKoord**), im Informationsaustausch mit dem Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) sowie im Cyberkrisenmanagement und dessen Koordinationsausschuss mit. Eine weitergehende Beschreibung der vom Verteidigungsministerium im Rahmen des NISG zu erbringenden Leistungen findet sich in TZ 18.

(2) Amtshilfe

Die Verteidigungsministerin bzw. der Verteidigungsminister und das Bundesheer waren als Organe des Bundes zur Amtshilfe (Art. 22 B–VG) verpflichtet. Im Unterschied zur Assistenzleistung, bei der die Handlungen des Bundesheeres der anfordernden (zivilen) Behörde zugerechnet wurden, war das Bundesheer bei der Amtshilfe im eigenen Wirkungsbereich tätig. Die Amtshilfe konnte auch den Cyber–Bereich betreffen, z.B. eine Auskunftserteilung bzw. Informationsweitergabe im Rahmen des IKDOK über die Ergebnisse von Schadcode–Analysen, die das Bundesheer zum Schutz der eigenen Systeme durchführte. Auf diese Weise wurde Spezialwissen im Verteidigungsministerium für den IKDOK bzw. Gesamtstaat genutzt.

(3) Zertifizierungen

Die Dienststelle Abwehramt des Verteidigungsministeriums hatte als nationale Zertifizierungsstelle Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, Einrichtungen und Anlagen auszustellen. Dabei war zu überprüfen, ob ein Unternehmen den erforderlichen Schutz für die sichere Verwendung von klassifizierten (vertraulichen, geheimen) Informationen gewährleisten konnte. Dies war für die Unternehmen erforderlich, um an industriellen Tätigkeiten oder an Forschung teilzunehmen und um Aufträge im Zusammenhang mit Vorhaben zu erlangen, die der Erfüllung von Aufgaben des Bundesheeres dienten.

(4) Unterstützungsleistungen

Sonstige Leistungen des Verteidigungsministeriums bzw. des Bundesheeres an staatliche Organe oder an Dritte (z.B. Einrichtungen der kritischen Infrastruktur) waren auch im IKT–Bereich (nur) im Rahmen der Aufgabe der militärischen Landesverteidigung möglich (sogenannte Unterstützungsleistungen; siehe RH–Bericht „Assistenz– und Unterstützungsleistungen des Bundesheeres zum Grenzmanagement“ (Reihe Bund 2020/38, TZ 10)). Daher legte das Verteidigungsministerium im Grundsatzerlass 2021 (zu Unterstützungsleistungen des Bundesheeres) fest, dass solche Leistungen der allgemeinen Einsatzvorbereitung (z.B. Übung, Ausbildung) oder wehrpolitischen Interessen (Vertrauen der Öffentlichkeit) zu dienen hatten.

Sie waren nach Vereinbarung und gegen Entgelt (§§ 63, 64 Bundeshaushaltsgesetz 2013, BGBl. I 139/2009 i.d.g.F.) zu erbringen. Seit 2021 bezog sich der Erlass auch ausdrücklich auf die organisatorische, logistische und technische Unterstützung, um bei gesamtstaatlich relevanten krisenhaften Entwicklungen die Handlungsfähigkeit der anfragenden Institutionen rasch wiederherzustellen.

7.2 Der RH betonte die besondere Bedeutung des im Verteidigungsministerium und Bundesheer vorhandenen Expertenwissens im Cyber–Bereich für die gesamtstaatliche Ebene. Aus dieser Zusammenarbeit auf gesamtstaatlicher Ebene ergibt sich für das Verteidigungsministerium ein Nutzen durch vermehrten Informationsaustausch sowie erweiterte Ausbildungs– und Übungsmöglichkeiten.

Der RH empfahl dem Verteidigungsministerium, die im Ressort und im Bundesheer vorhandene Expertise im Cyber–Bereich aktiv auch im Sinne der Prävention in die notwendigen gesamtstaatlichen Prozesse einzubringen (NISG, Amtshilfe, Unterstützungsleistungen).

Cyber–Defence: Strategie und Planung

Ziele und Aufbau der Direktion 6

8.1 (1) 2021 leitete das Verteidigungsministerium in seiner Zentralstelle und im Bundesheer eine Organisationsreform ein (diese war nicht Gegenstand dieser Gebarungsüberprüfung (TZ 1)). Ziel war eine Weiterentwicklung der oberen Führung zu einer insgesamt strafferen, nachhaltigen und schnelleren Führungsstruktur der Zentralstelle und des Bundesheeres und somit eine Optimierung der militärischen Planungs– und Führungsstrukturen. Die Zentralstelle sollte auf strategische Aufgaben und auf Aufgaben der allgemeinen staatlichen Verwaltung fokussiert werden. Gleichzeitig sollte die Truppe im personellen Bereich gestärkt werden. Dazu wurde die neue Generaldirektion für Landesverteidigung eingerichtet. Diese sollte alle Einsätze führen, die allgemeine Einsatzvorbereitung vornehmen und war für die Fähigkeitenentwicklung des Bundesheeres verantwortlich.

(2) Mit 1. Mai 2022 erließ die Verteidigungsministerin[25] eine Geschäftseinteilung, die die neue Organisation abbildete. Demnach bestand das Verteidigungsministerium auf der Ebene der Sektionen aus der Generaldirektion Verteidigungspolitik (Sektion I), der Generaldirektion Präsidium (Sektion II) und dem Generalstab. Die Generaldirektion für Landesverteidigung war dem Generalstab nachgeordnet und bestand aus neun Direktionen. Der Chef des Generalstabs bildete mit den Leitern dieser neun Direktionen[26] den Generalstab und führte im Wege der Direktionen das Bundesheer.

Dem Chef des Generalstabs unmittelbar nachgeordnet waren u.a. die Einrichtungen für die nachrichtendienstliche Abwehr (Abwehramt) und für die nachrichtendienstliche Aufklärung (Heeres–Nachrichtenamt).

(3) Das Aufgabengebiet der Direktion 6 umfasste die gesamten IKT–Agenden des Verteidigungsministeriums und Bundesheeres sowie die operative Umsetzung der Cyber–Defence. Zur Überleitung in die Direktion 6 waren Organisationseinheiten aus der Zentralstelle[27] und aus den im Zuge der Organisationsreform aufgelösten Kommanden Streitkräfte[28] und Streitkräftebasis[29] vorgesehen. Damit bündelte die Organisationsreform wesentliche Kapazitäten der IKT und der Cyber–Defence in der Direktion 6.

[25] Mag. Klaudia Tanner

[26] Fähigkeiten– und Grundsatzplanung (Dion Fäh&GSPl), Einsatz (Dion1 Eins), Luftstreitkräfte (Dion2 LuSK), Ausbildung (Dion3 Ausb), Logistik (Dion4 Log), Rüstung (Dion5 Rüst), IKT und Cyber (Dion6 IKT&Cy), Infrastruktur (Dion7 Infra), Militärisches Gesundheitswesen (Dion8 MilGesW)

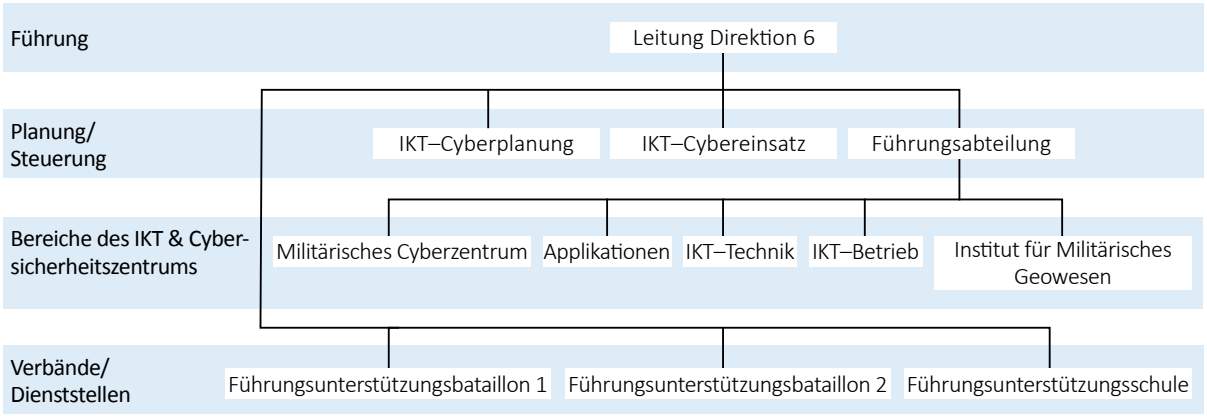
[27] Abteilung IKT–Cyberplanung (IKTCyPl), Abteilung Führungsunterstützung (FüU)

[28] Joint 6–Abteilung (J6), Führungsunterstützungsbataillone 1 und 2 (FüUB1 und FüUB2)

[29] Generalstabsabteilung 6 (G6), Führungsunterstützungsschule (FüUS), IKT & Cybersicherheitszentrum (IKTCySihZ) mit der Führungsabteilung (FüAbt) und den Bereichen IKT–Technik (IKTTe), IKT–Betrieb (IKTBetr), Applikationen (Appl), Militärisches Cyberzentrum (MilCyZ) und Institut für Militärisches Geowesen (IMG)

Der organisatorische Aufbau der Direktion 6 ist in folgender Abbildung dargestellt:

Abbildung 2: Struktur der Direktion 6 – IKT und Cyber



Quelle: BMLV; Darstellung: RH

Nachfolgende Tabelle enthält eine Übersicht über die Aufgaben der Organisationseinheiten in der Direktion 6:

Tabelle 3: Aufgaben der Organisationseinheiten in der Direktion 6 – IKT und Cyber

Organisationseinheit	Aufgabe(n)
IKT–Cyberplanung	Fähigkeitenentwicklung und Aufgabenstrukturplanung für IKT und Cyber– und Informationsraum
IKT–Cybereinsatz	Angelegenheiten der Führungsunterstützung bei Einsätzen des Bundesheeres, der Einsatzführung der Cyber–Kräfte im elektronischen Kampf und des Kampfes im Cyber–Raum
Führungsabteilung	Führungsaufgaben der Direktion 6, Koordinierung und Steuerung von Elementen im IKT–Cybersicherheitszentrum, Verwaltungsaufgaben in der Direktion 6 (fallweise in der Generaldirektion für Landesverteidigung)
Militärisches Cyberzentrum	Bereitstellung aller Sicherheitssysteme und Maßnahmen für den Eigenschutz der IKT–Services und die Abwehr von Bedrohungen und Angriffen aus dem Cyber–Raum, Erhaltung der sicheren Informationsverarbeitung und Implementierung von technischem Schutz im Bereich der elektronischen Kampfführung
Applikationen	Bereitstellung von Softwarelösungen und Softwareprodukten für Services im einsatzorientierten Aufgabenspektrum und im täglichen Dienstbetrieb, Betrieb des dynamisch gesicherten militärischen Netzes
IKT–Technik	Erhaltung, Betriebsunterstützung, technische Konzeption und Bereitstellung der gesamten IKT–Infrastruktur des Verteidigungsministeriums inklusive Systemsoftware, technischer Querschnittsaufgaben, Radarsysteme und Funkgeräte
IKT–Betrieb	operativer IKT–Servicebetrieb mit IKT–Anwenderunterstützung, Bearbeitung von Providerleistungen in der Telekommunikation, Frequenz– und Schlüsselwesen, IKT–Betriebsüberwachung für Übungen und Einsätze, Betriebsführung zu Sonderbauinfrastrukturen
Institut für Militärisches Geowesen	Bereitstellung analoger und digitaler Geoinformationen und georeferenzierter Daten für alle Anwendungen im Bundesheer
Führungsunterstützungsbataillon 1	Führungsunterstützung der Streitkräfte, Betrieb von interoperablen, taktischen Informations– und Kommunikationsnetzwerken und deren dezentrale Netzsteuerung, Administration als Force Provider, Organisationselement für elektronische Kampfführung (Führungsunterstützungsbataillon 2)
Führungsunterstützungsbataillon 2	
Führungsunterstützungsschule	Kader–Aus–, –Fort– und –Weiterbildung für Miliz– und Berufssoldaten inklusive ziviler Bediensteter der Cyber–Kräfte, Grundlagenarbeit Führungsunterstützung im Zusammenwirken mit allen Bereichen der Führungsunterstützung

Quelle: BMLV

(4) In der Direktion 6 waren sowohl planende bzw. steuernde als auch operative Elemente für Cyber–Defence eingerichtet. Damit waren wesentliche Teile zur Leistungserbringung der Cyber–Defence (Planung – Beschaffung – Bereitstellung – Einsatz)[30] in der Direktion 6 zusammengeführt und erfolgten durch folgende Organisationseinheiten:

- die Planung federführend durch die Abteilung IKT–Cyberplanung,
- die Bereitstellung durch die Bereiche IKT–Technik, IKT–Betrieb, Applikationen, Militärisches Cyberzentrum und Institut für Militärisches Geowesen, die zusammen das IKT & Cybersicherheitszentrum bildeten,
- der Einsatz durch die Abteilung IKT–Cybereinsatz.

(5) Die Leitung der Direktion 6 oblag einem Direktor, dem durch die Geschäftseinteilung des Verteidigungsministeriums vom Mai 2022 unmittelbar ad personam Aufgaben übertragen waren.[31] Die in der Direktion 6 angesiedelten Organisationseinheiten und deren Aufgaben legte diese Geschäftseinteilung jedoch nicht fest, da sie nur die organisatorische Gliederung der Zentralstelle regelte und die Generaldirektion für Landesverteidigung mit ihren Direktionen der Zentralstelle des Verteidigungsministeriums nachgeordnet war. Die Organisation der Direktion 6 war zur Zeit der Gebarungsüberprüfung noch nicht[32] durch Erlass schriftlich verfügt, sie arbeitete auf Grundlage der vorläufigen Projektorganisation.

Eine (einstweilige) Dienstanweisung legte die Aufgaben der Abteilungen IKT–Cyberplanung und IKT–Cybereinsatz fest; die Aufgaben der anderen Organisationseinheiten der Direktion 6 waren davon nicht umfasst. Ebenso wenig waren Gesamtziele für die Organisationseinheit Direktion 6 festgelegt.

(6) Nach Aussage des Verteidigungsministeriums verminderte die neue Organisation den Koordinierungsaufwand zwischen den Organisationseinheiten. Die Zusammenführung der Organisationselemente für Planung, Bereitstellung und Einsatz innerhalb der Direktion 6 erleichterte deren Zusammenwirken und hatte positive Effekte auf die Umsetzung der Kernprozesse der militärischen Landesverteidigung. Nach Finalisierung der Organisationsreform (TZ 9) seien gute Voraussetzungen für eine verbesserte Ablauforganisation gegeben.

[30] Lediglich die Beschaffung erfolgte über eine in der Direktion 5 – Rüstung zentral für IKT–Beschaffungen des Bundesheeres eingerichtete Organisationseinheit.

[31] Folgende Angelegenheiten waren übertragen: Chief Digital Officer, Chief Information Officer und Cyber–Koordinator des Verteidigungsministeriums, militärische Grundsätze im Rahmen des Telekommunikationsgesetzes, Frequenz– und Spektrummanagement, nationale GALILEO–Behörde als technisch–operationeller Anteil der österreichischen CPA (Competent PRS Authority; PRS = Public Regulated Service = öffentlich–regulierter Dienst).

[32] Das der Direktion 6 zugewiesene Personal war vom Beamtenministerium noch nicht systemisiert. Nach Freigabe durch das Beamtenministerium kann die Organisation der Direktion 6 per Erlass durch die dafür zuständige Abteilung Organisation im Verteidigungsministerium schriftlich verfügt werden.

8.2 (1) Der RH stellte fest, dass die Organisationsreform des Verteidigungsministeriums und des Bundesheeres die für IKT und für Cyber–Defence wesentlichen Organisationseinheiten unter gemeinsamer Führung in der Direktion 6 zusammenführte. Damit wurden die Voraussetzungen für eine effiziente Zusammenarbeit zwischen den Organisationseinheiten insofern geschaffen, als Hierarchieebenen wegfielen und Kommunikationswege verkürzt wurden.

(2) Der RH stellte kritisch fest, dass die Direktion 6 noch nicht durch Erlass verfügt war, dass die Aufgaben nur für einen Teil ihrer Organisationseinheiten festgelegt waren und dass auch Gesamtziele fehlten.

Der RH empfahl daher dem Verteidigungsministerium, die neue Direktion 6 per Erlass zu verfügen (siehe TZ 9) und die Aufgaben ihrer Organisationseinheiten sowie die Gesamtziele schriftlich festzulegen.

8.3 Das Verteidigungsministerium hielt in seiner Stellungnahme fest, dass die Gliederung und Struktur der Direktion 6 weiterhin stringent weiterverfolgt werden. Wesentliche Voraussetzung sei die Verfügbarkeit von entsprechenden Strukturen und in weiterer Folge von qualifiziertem Personal.

Das Verteidigungsministerium wies weiters auf die laufende Bearbeitung der Thesenpapiere hin, um den zukünftigen Anforderungen für die Weiterentwicklung der Cyber–Kräfte gerecht werden zu können.

Organisation und Ressourcen der Direktion 6

9.1 (1) Mit Wirksamkeit vom 1. Mai 2022 legte die von der Verteidigungsministerin erlassene neue Geschäftseinteilung die Organisationsstruktur der Zentralstelle fest. Auf dieser Grundlage wurde auch die Organisationsstruktur der Direktion 6 eingerichtet, die dem der Zentralstelle nachgeordneten Bereich angehörte. Im November 2022 waren den Organisationseinheiten der Direktion 6 jedoch noch nicht jene Arbeitsplätze zugeordnet, die den neuen Organisationsplänen entsprachen. Nach diesen Plänen für die Direktion 6 wäre ein Teil der Arbeitsplätze neu einzurichten und ein Teil aufgrund der damit verbundenen Anforderungen, Aufgaben und ihrer organisatorischen Stellung neu zu bewerten. Dafür hatte das Verteidigungsministerium beim zuständigen Beamtenministerium am 23. Februar 2022 einen Antrag auf Bewertung und Zuordnung gemäß dem Beamten–Dienstrechtsgesetz 1979[33] gestellt.

[33] Das Beamten–Dienstrechtsgesetz 1979 (BGBl. 333/1979 i.d.g.F.) regelt die Bewertung und Zuordnung von Arbeitsplätzen, u.a. für Beamte des Allgemeinen Verwaltungsdienstes (§ 137) und für Militärpersonen (§ 147).

Die beantragte Bewertung und Zuordnung[34] (Systemisierung) der Arbeitsplätze wurde vom Beamtenministerium noch nicht vorgenommen. Das Verteidigungsministerium gab dazu an, dass die mit dem Beamtenministerium darüber geführten – mittlerweile erheblich verzögerten – Verhandlungen noch nicht abgeschlossen seien und ein Zeitpunkt für den Abschluss auch nicht absehbar sei.

Die Aufgabenerfüllung in der Direktion 6 erfolgte – bis zur neuen Systemisierung durch das Beamtenministerium und nachfolgenden Erlassung der neuen Organisationspläne – zwar schon in der neuen Struktur, teilweise jedoch durch der Direktion 6 dienstzugeteilte Mitarbeiterinnen und Mitarbeiter aus noch bestehenden Organisationseinheiten, die schon bisher mit Aufgaben der IKT und der Cyber–Defence befasst waren.

(2) Darüber hinaus gab das Verteidigungsministerium an, dass die wesentlichen Abläufe und Prozesse der Direktion 6 zur Zeit der Gebarungsüberprüfung einem Bearbeitungsprozess unterliegen würden; dieser könne erst nach Erlassung der Organisationspläne – für die die Systemisierung der Arbeitsplätze durch das Beamtenministerium Voraussetzung ist – tatsächlich abgeschlossen werden. Dies betraf insbesondere die mit der neuen Struktur entstandenen Dokumente wie die zentralen Prozesse des Verteidigungsministeriums und interne Anordnungen der Direktion 6 zur Unterstützung der Führungsfähigkeit des Ressorts.

(3) Das Verteidigungsministerium legte dem RH eine Übersicht über das für die Direktion 6 tätige Personal sowie über die für die Direktion 6 geplanten Arbeitsplätze vor:

- In den Organisationseinheiten bestanden Arbeitsplätze (Stand Oktober 2022), die allerdings aus Systemisierungen im Zuge früherer Organisationsreformen stammten.
- Das Verteidigungsministerium plante für die Direktion 6 eine Erhöhung der Anzahl von Arbeitsplätzen in zwei Phasen mit dem Ziel eines schrittweisen Auf– und Ausbaus von Fähigkeiten. Phase 1 umfasste die Überwachung des Cyber–Raums mit einer noch eingeschränkten Verteidigungsfähigkeit, Phase 2 die volle Einsatzfähigkeit für die Verteidigung des Cyber–Raums mit hoher Durchhaltefähigkeit. Die zusätzlichen Arbeitsplätze betrafen insbesondere das Militärische Cyberzentrum sowie die Führungsabteilung und das Institut für Militärisches Geowesen.
- Größer als die Differenz zwischen den bestehenden und geplanten Arbeitsplätzen war die Differenz zwischen den geplanten Arbeitsplätzen und der Anzahl der im November 2022 eingesetzten Vollbeschäftigungsäquivalente (**VBÄ**). Insbesondere für das Militärische Cyberzentrum war ein starker Personalzuwachs innerhalb der zwei Phasen geplant.

[34] Bei der Arbeitsplatzbewertung sind die mit dem Arbeitsplatz verbundenen Anforderungen an das Wissen, die für die Umsetzung des Wissens erforderliche Denkleistung und die Verantwortung zu berücksichtigen. Die bewerteten Arbeitsplätze sind (unter Bedachtnahme auf Richtverwendungen) einer Verwendungsgruppe und innerhalb dieser der Grundlaufbahn oder einer Funktionsgruppe zuzuordnen.

Dazu teilte das Verteidigungsministerium mit, dass die Organisationsreform zu einer Verzögerung der Personalentwicklung im Militärischen Cyberzentrum geführt hatte. Es sei nicht möglich gewesen, vor der vollständigen Umsetzung der Reform Arbeitsplätze systemisieren zu lassen, um damit die Anzahl jenes Personals zu erhöhen, das auf Cyber–Angelegenheiten spezialisiert war. Diese Stagnation im Jahr 2021 habe ein stark konkurrierender ziviler Arbeitsmarkt noch zusätzlich verschärft.

9.2 (1) Der RH hielt fest, dass die Verteidigungsministerin eine Geschäftseinteilung für das Verteidigungsministerium mit Wirksamkeit ab 1. Mai 2022 erlassen hatte. Er kritisierte, dass die Geschäftseinteilung erlassen wurde, bevor die neue Organisation in der geplanten Form tatsächlich arbeitsfähig war: Bei Erlassung der Geschäftseinteilung war die Systemisierung der vom Verteidigungsministerium vorgesehenen neuen Arbeitsplätze beim Beamtenministerium zwar beantragt, von diesem jedoch noch nicht genehmigt.

Der RH stellte fest, dass die Verhandlungen über die Systemisierung der Arbeitsplätze zwischen den beiden Bundesministerien noch nicht abgeschlossen waren und der Abschluss nicht absehbar ist. Daher bestand das Risiko einer unzulänglichen Wahrnehmung der Aufgaben betreffend Cyber–Defence.

Der RH empfahl daher dem Verteidigungsministerium, die Verhandlungen mit dem Beamtenministerium über die Systemisierung der Arbeitsplätze in der Direktion 6 mit dem Ziel einer Einigung und einer zügigen Umsetzung der Organisationspläne im Verteidigungsministerium rasch wieder aufzunehmen und abzuschließen.

(2) Der RH betonte, dass die Überarbeitung der Abläufe und Prozesse erst mit der Verfügung der Organisationspläne abgeschlossen werden kann, wofür die Systemisierung der Arbeitsplätze durch das Beamtenministerium Voraussetzung ist.

Er empfahl dem Verteidigungsministerium, die Überarbeitung der Abläufe und Prozesse nach Verfügung der Organisationspläne so rasch wie möglich abzuschließen und in Kraft zu setzen.

(3) Der RH hielt fest, dass im Militärischen Cyberzentrum 2022 die Anzahl der VBÄ geringer war als die Anzahl der vorhandenen Arbeitsplätze.

Er empfahl dem Verteidigungsministerium, die im Militärischen Cyberzentrum vorhandenen Arbeitsplätze rasch zu besetzen.

(4) Die noch nicht abgeschlossene Organisationsreform – für die auch die nicht erreichte Einigung mit dem Beamtenministerium wesentlich verantwortlich war – führte dazu, dass die erforderlichen Personalkapazitäten im Militärischen Cyberzentrum noch nicht weiter aufgebaut werden konnten.

Der RH empfahl dem Verteidigungsministerium, die für den weiteren Aufbau von Cyber–Kompetenzen im Militärischen Cyberzentrum geplanten Personalstände umzusetzen.

9.3 (1) Das Verteidigungsministerium teilte in seiner Stellungnahme mit, Gliederung und Struktur der Direktion 6 weiterhin stringent zu verfolgen. Wesentliche Voraussetzung sei die Verfügbarkeit von Strukturen und Personal (siehe auch TZ 8).

Maßnahmen hinsichtlich der fehlenden Personalressourcen des Militärischen Cyberzentrums und zur Schließung der dargestellten Fähigkeitslücken würden eingeleitet (Rapid Response Teams, Information Security Management System, Cyber–Truppenübungsplatz, Einsatz–Security Operation Center etc.). Die Strukturerweiterung sei unabhängig von noch offenen Strukturentscheidungen im Bundesheer zu sehen, da diese in allen bisherigen Planungsvarianten auch zwingend erforderlich sei, um bestehende Defizite zu beheben.

Der Umfang des angestrebten Organisationsplans orientiere sich strikt am Pfad der weiterführenden bestehenden Kennzahl „Verbesserung der Fähigkeiten der militärischen Landesverteidigung im Cyber–Raum [...] Personeller Aufwuchs des spezialisierten Cyberpersonals“ im Wirkungsziel 1. Die Berechnung folge den bisher weiterentwickelten Planungen für die mögliche Erreichung der zweiten Ausbaustufe.

Ohne qualifizierten Personalzuwachs könne die Fähigkeitenentwicklung im Bereich der Cyber–Verteidigung kaum realisiert werden. Die konkreten Vorhaben und Maßnahmen seien im Rahmen der Gebarungsüberprüfung angesprochen worden.

(2) Das Beamtenministerium gab in seiner Stellungnahme an, dass das Verteidigungsministerium die Herstellung des Einvernehmens zur Neuaufstellung des Organisationsplans Militärisches Cyberzentrum (OrgPlanNr. IT6) beantragt habe, der den bisherigen Organisationsplan (OrgPlan MilCyZ, OrgPlan FU6) ersetze.

Die übermittelten Unterlagen seien einem Bewertungsverfahren unterzogen und nach mehreren Besprechungen zwischen den beiden Ressorts einvernehmlich abgeschlossen worden. Einen darauf basierenden Antrag des Verteidigungsministeriums habe das Beamtenministerium am 16. März 2023 genehmigt.

Die tatsächliche Umsetzung des Organisationsplans sowie die technische Ausstattung lägen nicht im Zuständigkeitsbereich des Beamtenministeriums.

9.4 Der RH hielt gegenüber dem Verteidigungsministerium fest, dass nach Genehmigung des Organisationsplans des Militärischen Cyberzentrums durch das Beamtenministerium nunmehr die Grundlage geschaffen wurde, die geplante Personalentwicklung umzusetzen.

Organisationseinheiten mit Cyber–Defence–Aufgaben: Überblick

10 (1) Neben der Direktion 6 hatten weitere Organisationseinheiten Aufgaben der Cyber–Defence wahrzunehmen:

Tabelle 4: Organisationseinheiten mit Aufgaben der Cyber–Defence

Organisationseinheit	Aufgabe
Generaldirektion Verteidigungspolitik (Sektion I)	**verteidigungspolitische Strategieentwicklung**
Generaldirektion für Landesverteidigung	
Direktion 1 – Einsatz	Einsatz bzw. Einsatzvorbereitung der Streitkräfte
Direktion 6 – IKT und Cyber	wesentliche Teile der Leistungserbringung für Cyber–Defence durch das IKT und Cybersicherheitszentrum und die Abteilungen IKT–Cyberplanung und IKT–Cybereinsatz
Direktion Fähigkeiten– und Grundsatzplanung	Konzeption der Fähigkeiten der Streitkräfte
Chef des Generalstabs	
Abwehramt	Beitrag zur Gewährleistung der Sicherheit der militärischen IKT–Infrastruktur, zum Cyber–Lagebild, Vorbereitung offensiver nachrichtendienstlicher Maßnahmen
Heeres–Nachrichtenamt	Erstellung eines gesamtheitlichen Lagebildes (militärisch, politisch, ökonomisch, hybrid) einschließlich Dimension Cyber

Quelle: BMLV

Die Direktion 6 – mit dem IKT und Cybersicherheitszentrum (insbesondere dem Militärischen Cyberzentrum) und den Abteilungen IKT–Cyberplanung und IKT–Cybereinsatz – war, wie in TZ 8 und TZ 9 dargestellt, unmittelbar für die Cyber–Defence des Bundesheeres verantwortlich.

Organisationseinheiten, die sich im weiteren Sinne mit Aufgaben der Cyber–Defence befassten, waren:

- die Generaldirektion Verteidigungspolitik (sie entsprach der Sektion I im Verteidigungsministerium): Die von ihr entwickelten verteidigungspolitischen Zielsetzungen waren auch für Cyber–Defence maßgeblich;
- die Generaldirektion für Landesverteidigung mit
  - der Direktion Fähigkeiten– und Grundsatzplanung: Ihre Aufgabe war die Konzeption der Fähigkeiten der gesamten Streitkräfte; in Bezug auf Cyber arbeitete sie eng mit der dafür in der Direktion 6 zuständigen Abteilung IKT–Cyberplanung zusammen;
  - der Direktion 1 – Einsatz: Sie war für den Einsatz und die Einsatzvorbereitung der gesamten Streitkräfte zuständig und kooperierte eng mit der für den Cyber–Bereich zuständigen Abteilung IKT–Cybereinsatz in der Direktion 6;
- die militärischen Nachrichtendienste (das Abwehramt und das Heeres–Nachrichtenamt): Diese waren organisatorisch dem Chef des Generalstabs unmittelbar nachgeordnet.

(2) Die Nachrichtendienste wirkten unmittelbar an Kernaufgaben der Cyber–Defence mit:

(a) Das Abwehramt hatte die Aufgabe der nachrichtendienstlichen Abwehr und diente dem militärischen Eigenschutz[35]. Es hatte auch im Cyber–Bereich die präventive und aktive Spionage– und Sabotageabwehr sowie die Abwehr anderer subversiver Tätigkeiten, die Gegenspionage und die elektronische Abwehr wahrzunehmen. Daraus leitete das Abwehramt folgende konkrete Aufgaben ab:

- Maßnahmen zur permanenten Gewährleistung eines hohen Maßes an Sicherheit der militärischen IKT–Infrastruktur; dazu gehörten die Leitung und teilweise die Durchführung der Prozesse zur Akkreditierung, Auditierung und des Vorfallmanagements einschließlich Forensik bei allen nachrichtendienstlichen Sicherheitsvorfällen;
- Erbringung eines permanenten Beitrags zum Cyber–Lagebild als Teil des militärischen und des nationalen Gesamtlagebildes durch die Sammlung und Analyse von aus allen Quellen gewonnenen Daten;
- Vorbereitung von im Rahmen der Landesverteidigung möglicherweise erforderlichen offensiven nachrichtendienstlichen Maßnahmen (Computer Network Attacks – CNA).

[35] § 20 Abs. 2 Militärbefugnisgesetz: Die nachrichtendienstliche Abwehr dient dem militärischen Eigenschutz durch die Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen militärische Rechtsgüter zur Beeinträchtigung der militärischen Sicherheit erwarten lassen.

Ein Alleinstellungsmerkmal sah das Abwehramt darin, dass es einen Beitrag zur Ersterkennung von Bedrohungen und Angriffen auf die IT–Infrastruktur des Bundesheeres leisten konnte.

(b) Dem Heeres–Nachrichtenamt oblagen die Aufgaben der nachrichtendienstlichen Aufklärung[36]. In Umsetzung dieser Aufgaben nach dem Militärbefugnisgesetz erstellte es ein gesamtheitliches Lagebild (u.a. militärisch, politisch, ökonomisch). Es hatte keine direkten Cyber–Defence–Aufgaben, die Dimension Cyber war allerdings integraler Bestandteil des gesamtheitlichen Lagebildes und spielte unter folgenden Gesichtspunkten eine Rolle:

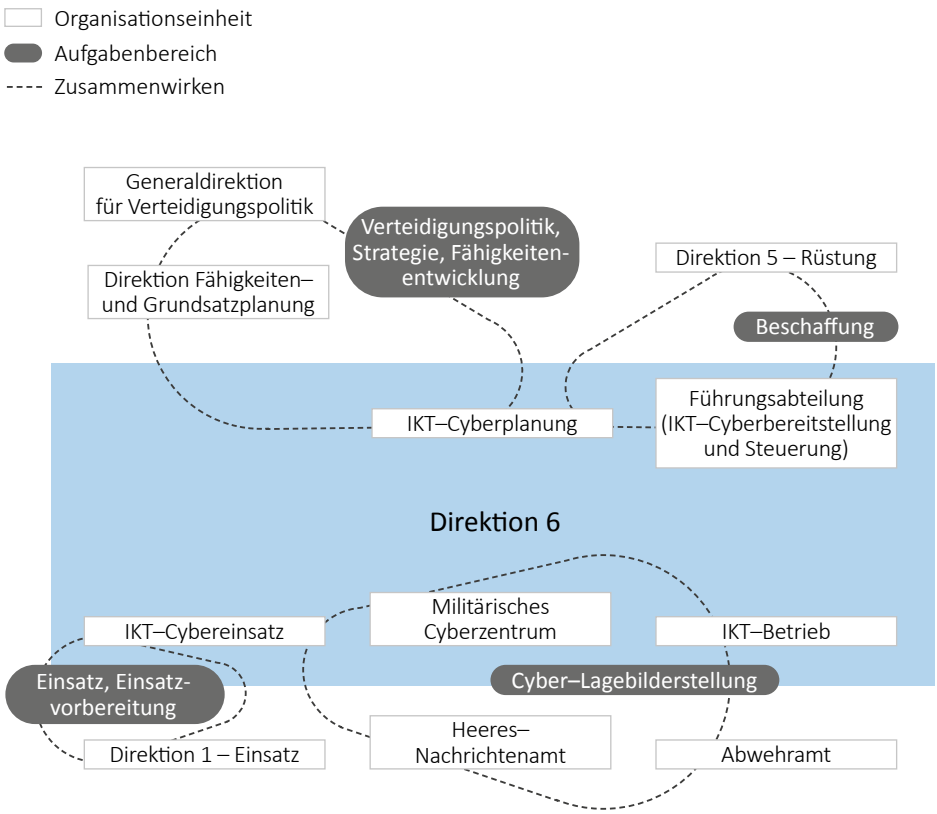
- Der Cyber–Raum war ein Instrument der nachrichtendienstlichen Informationsbeschaffung.
- Der Cyber–Raum war Beobachtungsobjekt hinsichtlich nachrichtendienstlich relevanter Entwicklungen und Vorgänge als Aspekt des gesamtheitlichen nachrichtendienstlichen Lagebildes.
- Es waren Maßnahmen zum Schutz eigener Netze vor Bedrohungen aus dem Cyber–Raum zu treffen (Cyber–Defence).

[36] § 20 Abs. 1 Militärbefugnisgesetz: Die nachrichtendienstliche Aufklärung dient der Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland oder über internationale Organisationen oder sonstige zwischenstaatliche Einrichtungen betreffend militärische und damit im Zusammenhang stehende sonstige Tatsachen, Vorgänge und Vorhaben.

Zusammenarbeit Direktion 6 und weitere Organisationseinheiten mit Cyber–Defence–Aufgaben

11.1 (1) Wesentliche Aspekte des Zusammenwirkens der Direktion 6 mit den anderen Organisationseinheiten (Tabelle 4) stellt die nachfolgende Abbildung dar:

Abbildung 3: Zusammenwirken der Organisationseinheiten mit Aufgaben der Cyber–Defence



Quelle: BMLV; Darstellung: RH

(2) Cyber–Lagebilderstellung

Betreffend das Cyber–Lagebild arbeiteten die Organisationseinheiten wie folgt zusammen:

- Das Militärische Cyberzentrum führte zur Bearbeitung der laufenden Aktivitäten wöchentliche Meetings auf Technikerebene mit dem Abwehramt durch. Cyber–Angriffe bzw. –Vorfälle wurden unter Einsatz eines klassifizierten Ticketsystems auf spezielle Angriffsmuster analysiert. Über diese Besprechungen wurden keine Protokolle verfasst.

- Täglich wurde ein Cyber–Lagebild zum Status der Cyber–Kräfte und den Vorkommnissen im Cyber–Raum innerhalb der Direktion 6 erstellt – mit Schwergewicht bei den Auswirkungen auf laufende Einsätze und Vorhaben des Bundesheeres. Dabei wirkten die Bereiche des IKT und Cybersicherheitszentrums (Militärisches Cyberzentrum, IKT–Betrieb und IKT–Cybereinsatz) zusammen; das so erstellte Cyber–Lagebild wurde der Direktion 1 – Einsatz übermittelt. Diese war federführend zuständig für die tägliche Lagebeobachtung des Bundesheeres.
- Weiters lieferte die Direktion 6 einen wöchentlichen Beitrag für die von der Direktion 1 – Einsatz betreute Einsatzkoordinierungsbesprechung des Bundesheeres. Der Beitrag der Abteilung IKT–Cybereinsatz fasste alle einsatzrelevanten Lagemeldungen der Verbände und Dienststellen der Direktion 6 zu einer Wochenlage einschließlich der Vorkommnisse im Cyber–Raum zusammen.
- Ein wöchentlicher Informationsaustausch, insbesondere zur Abstimmung für die Wochenmeldung betreffend das Cyber–Lagebild, fand zwischen den Bereichen des IKT und Cybersicherheitszentrums (Militärisches Cyberzentrum, IKT–Betrieb und IKT–Cybereinsatz) und den Nachrichtenämtern statt. Ergänzend dazu gab es monatliche Abstimmungen größeren inhaltlichen Umfangs mit den Nachrichtenämtern.

Die beschriebenen Prozesse der Abstimmung und Zusammenarbeit waren nicht schriftlich festgelegt.

(3) Verteidigungspolitik und Einsatz

Die Aufgabenwahrnehmung im Rahmen des Leistungserbringungszyklus Planung – Beschaffung – Bereitstellung – Einsatz erforderte es, dass die betroffenen Organisationseinheiten eng und abgestimmt zusammenarbeiteten. Für diese zentralen Aufgaben der Landesverteidigung hatte das Verteidigungsministerium eine Ablauforganisation in Form von sogenannten Kernprozessen in einer eigenen Richtlinie „Zentrale Prozesse der Landesverteidigung 2022“ festgelegt. In den relevanten Prozessen „Streitkräfte entwickeln“ und „Streitkräfte einsetzen und führen“ war die Direktion 6 in nahezu sämtliche Prozessschritte zumindest in mitwirkender Rolle eingebunden. Im Prozess „Streitkräfte entwickeln“ war die Abteilung IKT–Cyberplanung im Rahmen des Fähigkeitenmanagements zuständig für Ausrüstung, Organisation und Personal bei den Cyber– und Informationskräften; in den Prozess „Streitkräfte einsetzen und führen“ war in erster Linie die Abteilung IKT–Cybereinsatz eingebunden.

(4) Beschaffung

Auf Ebene der Direktion 6 arbeiteten die Organisationseinheiten für Planung, Beschaffung, Bereitstellung und Einsatz über eine wöchentliche Direktionsbesprechung auf Leitungsebene zusammen, die der Koordination, Abstimmung und Information über die Bearbeitung der einzelnen Aufgaben diente. Die außerhalb der

Direktion 6 liegende Beschaffung wurde über die Abteilungen IKT–Cyberplanung und die Führungsabteilung (Fachbereich IKT–Cyberbereitstellung und Steuerung) oder über technische Bereiche direkt eingebunden. Abgeleitet von den Vereinbarungen in der Direktionsbesprechung fanden Besprechungen zur Informationsweitergabe in den Organisationselementen Planung, Einsatz und Bereitstellung statt. Sonstige flexible Querverbindungen ergaben sich aus dem laufenden Geschäft und den größtenteils gemeinsam vorgenommenen Planungsschritten.

11.2 (1) Vor dem Hintergrund der Notwendigkeit einer regelmäßigen Zusammenarbeit zwischen den für Cyber–Defence zuständigen Organisationseinheiten anerkannte der RH, dass das Verteidigungsministerium die für Cyber–Defence wesentlichen Organisationseinheiten in der Direktion 6 zusammenführte (TZ 8). Damit waren die Voraussetzungen für eine effiziente Zusammenarbeit insofern geschaffen, als Hierarchieebenen wegfielen und sich Kommunikationswege verkürzten.

(2) Der RH hob hervor, dass es hinsichtlich der Cyber–Lage einen täglichen direktionsinternen und einen wöchentlichen Informationsaustausch der Direktion 6 mit den militärischen Nachrichtendiensten gab, diese Zusammenarbeit also regelmäßig stattfand. Er hielt jedoch kritisch fest, dass die diesbezüglichen Prozesse und Abläufe nicht verschriftlicht waren. Angesichts der Bedeutung der Aufgabe Cyber–Defence für die militärische und somit auch für die gesamtstaatliche Sicherheit ist es wesentlich, dass die Prozesse für diese Zusammenarbeit schriftlich festgelegt sind, um deren Einhaltung unabhängig von den agierenden Personen sicherzustellen.

Der RH empfahl dem Verteidigungsministerium, die zur Feststellung der Cyber–Lage notwendigen Prozesse und die Zusammenarbeit sowohl innerhalb der Direktion 6 als auch mit den militärischen Nachrichtendiensten (Abwehramt, Heeres–Nachrichtenamt) schriftlich festzulegen und deren Einhaltung zu verfügen.

(3) Der RH hielt positiv fest, dass das Verteidigungsministerium für den Leistungserbringungszyklus Planung – Beschaffung – Bereitstellung – Einsatz ressortweit anzuwendende Kernprozesse festgelegt und diese in einer Richtlinie festgehalten und verfügt hatte. In diese Kernprozesse waren auch die Direktion 6 bzw. einzelne ihrer Abteilungen entsprechend ihren Aufgaben eingebunden. Auch die Bearbeitung der Aufgaben Planung, Beschaffung, Bereitstellung und Einsatz auf der Ebene der Direktion 6 erfolgte strukturiert.

Leitlinien und Konzepte für Cyber–Defence

12.1 (1) Abgeleitet von den gesamtstaatlichen, verteidigungspolitischen und militärstrategischen Sicherheitsstrategien (TZ 4) arbeitete das Verteidigungsministerium an Konzepten zur Festlegung und zur Steuerung der Cyber–Defence. Die dazu zentrale Leitlinie Cyber–Verteidigung war im November 2022 in Ausarbeitung und lag dem RH als Entwurf vor.

Der Entwurf enthielt Ausführungen zu nationalen und internationalen strategischen Grundlagen, nationalen rechtlichen und sonstigen Rahmenbedingungen, zu möglichen feindlichen Akteuren und zur Bedrohungslage im Cyber–Raum. Ausgehend davon definierte der Entwurf erforderliche Fähigkeiten für die Cyber–Defence (TZ 15), die größtenteils noch aufzubauen waren. Daraus wurden Folgerungen und Ziele für das Verteidigungsministerium und das Bundesheer abgeleitet, wie insbesondere

- die Schaffung der notwendigen strukturellen Rahmenbedingungen für das Zusammenwirken der Cyber–Truppe mit den anderen militärischen Domänen (insbesondere Land– und Luftstreitkräfte),
- die Zurverfügungstellung von Assistenz– und Unterstützungsleistungen, um schwerwiegende Vorfälle zu bewältigen,
- solidarische Beitragsleistungen bei Cyber–Angriffen auf andere EU–Mitgliedstaaten und
- internationale Kooperationen und nationale Partnerschaften im Bereich Cyber.

Die Leitlinie Cyber–Verteidigung formulierte die Inhalte nur allgemein, Organisationseinheiten für deren Umsetzung waren nicht festgelegt.

(2) Ziel des Querschnittskonzepts „Einsatz im Cyber–Raum“ war es, die Grundlagen für die Entwicklung der Cyber–Kräfte im Bundesheer zu schaffen; es befand sich im November 2022 in Bearbeitung. Die Entwicklung der Cyber–Kräfte war mit der Weiterentwicklung der anderen Teilstreitkräfte im Bundesheer abzustimmen, um Erstere mit den anderen militärischen Domänen synchronisiert einsetzen zu können. Das Querschnittskonzept war als Ausgangsbasis für die weitere Bearbeitung in den Sektionen des Verteidigungsministeriums und im Generalstab vorgesehen.

Die Cyber–Kräfte, diese bestanden aus der Cyber–, der IKT– und der EloKa–Truppe (Elektronischer Kampf), sollten am Einsatz von Streitkräften im Rahmen der militärischen Operationsführung mitwirken, insbesondere durch unterstützende Aktivitäten im Cyber–Raum und im elektromagnetischen Umfeld, durch elektronische Kampfführung und den Kampf in Computernetzwerken.

Zur Sicherstellung der dafür erforderlichen Fähigkeiten waren gemäß dem Konzept insbesondere

- Kräfte mit spezifischen Fähigkeiten für den Einsatz im Cyber–Raum zu rekrutieren,
- leistungsstarke, permanent verfügbare, (teil–)autonome und interoperable Führungs–, Wirkungs– und Aufklärungssysteme zu beschaffen,
- für das Führungssystem Einsatz erforderliche ortsfeste IKT–Systeme („IKT–Backbone“) zu betreiben und
- die Ausbildung an die Komplexität des Cyber–Raums anzupassen.

Das Querschnittskonzept „Einsatz im Cyber–Raum“ gab nur wenig detaillierte Orientierungen und Handlungsanweisungen vor, die zudem keinen Organisationseinheiten zur konkreten Bearbeitung zugewiesen waren.

(3) Für die Direktion 6 trat mit 1. Juli 2021 eine vorläufige Geschäftsordnung in Kraft. In dieser war festgelegt, dass sie ursprünglich für die Dauer der Überleitungsphase der Generaldirektion für Landesverteidigung bis 31. März 2022 gelten sollte und danach unter Einbeziehung der tatsächlichen Strukturen und Aufgabenfelder als Geschäftsordnung der Direktion 6 zu übernehmen wäre. Die vorläufige Geschäftsordnung regelte die Führungsstruktur und Verantwortlichkeiten, Abläufe (Besprechungssystematik etc.), das Informationsmanagement (u.a. Geschäftsfallbearbeitung) und den Dienstbetrieb im Normdienst der Direktion 6.

(4) Für das Militärische Cyberzentrum (TZ 9) gab es eine Geschäftsordnung (Stand 12. Jänner 2022). Diese beschrieb die Organisation des Militärischen Cyberzentrums (es bestand aus fünf Abteilungen samt Referaten), regelte die Ablauforganisation im Normdienst und legte die Aufgabenzuordnung und den Dienstbetrieb fest. Weiters enthielt sie Regelungen über die Behandlung von Geschäftsfällen, z.B. die Meldung von besonderen Vorfällen.

Für andere Organisationseinheiten der Direktion 6, die mit Aufgaben der Cyber–Defence befasst waren, lagen dem RH keine Geschäftsordnungen vor.

12.2 (1) Der RH hielt fest, dass mit der Leitlinie Cyber–Verteidigung und dem Querschnittskonzept „Einsatz im Cyber–Raum“ zwei Dokumente, die wesentliche strategische Vorgaben für die Aufgabe Cyber–Defence im Verteidigungsministerium enthielten, lediglich als Entwürfe vorlagen. Diese Vorgaben waren für die weiteren Bearbeitungsschritte und Maßnahmen grundlegend. Vor dem Hintergrund der steigenden Bedeutung von Cyber–Defence und um die Sicherheit im Cyber–Raum aufrechtzuerhalten, sollten die Entwicklung der Cyber–Fähigkeiten und die Stärkung der Cyber–Kräfte des Bundesheeres ohne weitere Verzögerung zügig vorangetrieben werden.

Der RH wiederholte seine Empfehlung (TZ 4) an das Verteidigungsministerium, die Fertigstellung der Leitlinie Cyber–Verteidigung voranzutreiben und diese ehestmöglich zu erlassen (zu den empfohlenen Inhalten siehe TZ 5).

Er empfahl dem Verteidigungsministerium, auch die Bearbeitung des im Entwurf vorliegenden Querschnittskonzepts „Einsatz im Cyber–Raum“ möglichst rasch abzuschließen und dieses in Kraft zu setzen.

Weiters empfahl er, aus dem in den beiden Dokumenten festgehaltenen Handlungsbedarf Einzelmaßnahmen abzuleiten und für deren Umsetzung einen Zeitplan und die dafür zuständigen Organisationseinheiten festzulegen.

(2) Der RH stellte fest, dass das Verteidigungsministerium im Juli 2021 eine Geschäftsordnung für die Direktion 6 erlassen hatte, die das Zusammenwirken der Cyber–Defence–Fähigkeiten innerhalb der Direktion 6 regelte; die Geschäftsordnung war jedoch aufgrund der nicht abgeschlossenen Organisationsreform nach wie vor nur vorläufig.

Der RH empfahl daher dem Verteidigungsministerium, nach Abschluss der Organisationsreform der Direktion 6 die vorläufige Geschäftsordnung an die neue Organisationsstruktur anzupassen und neu zu erlassen.

12.3 In seiner Stellungnahme hielt das Verteidigungsministerium seine Bestrebungen fest, die strategischen Planungsdokumente wie die Leitlinie Cyber–Verteidigung und dazu erforderliche Konzepte fertigzustellen.

Der Umfang des (für die Direktion 6) angestrebten Organisationsplans orientiere sich strikt am Pfad der weiterführenden bestehenden Kennzahl „Verbesserung der Fähigkeiten der militärischen Landesverteidigung im Cyber–Raum [...] Personeller Aufwuchs des spezialisierten Cyberpersonals“ im Wirkungsziel 1. Die Berechnung folge den bisher weiterentwickelten Planungen für die mögliche Erreichung der zweiten Ausbaustufe.

Cyber–Defence: Umsetzung

Einsatzorganisation

13.1 Die Einsatzkräfte des Bundesheeres setzten sich aus jenen Truppen und Organisationselementen des Bundesheeres zusammen, die in der Friedensgliederung bestanden, und aus jenen, die zu Übungszwecken oder zum Zwecke eines Einsatzes einberufen wurden. Die Direktion 6 hatte in militärischen Bedrohungsfällen rasch zu reagieren; dafür bedurfte es vorab der Ausarbeitung einer Einsatzorganisation (Aufbau– sowie Ablauforganisation) für alle Truppen und Organisationselemente:

- Um im Einsatz den erforderlichen Abstimmungsprozess – gesamtstaatliche, militärstrategische und operative Abstimmung – auf den jeweiligen Führungsebenen sicherzustellen, hatte die Direktion 6 eine Aufbauorganisation für den Einsatz mit Unterstützung von Milizkräften vorzusehen. Damit konnte sie im Einsatz auch auf – sich rasch ändernde – Lageentwicklungen reagieren und die erforderliche Durchhaltefähigkeit gewährleisten, um ihre Aufgaben über einen längeren Zeitraum wahrzunehmen.
- Ebenso erforderlich für den Einsatzbetrieb war die Festlegung der Ablauforganisation, etwa einer Geschäftsordnung für den Einsatz.

Die Direktion 6 hatte einen Entwurf der besonderen Aufbauorganisation sowie einer Geschäftsordnung für den Einsatz ausgearbeitet. Der Entwurf war allerdings im November 2022 noch nicht verfügt (eine Verfügung bedeutet in diesem Kontext eine Anordnung durch den Kommandanten der Einheit).

13.2 Der RH stellte kritisch fest, dass die Direktion 6 im Verteidigungsministerium für den Einsatzfall noch keine Einsatzorganisation verfügt hatte. Er wies darauf hin, dass die Einsatzorganisation in Form einer besonderen Aufbauorganisation und einer Geschäftsordnung rechtzeitig vor einem allfällig notwendigen Einsatz zu gewährleisten ist, damit sie im Einsatzfall rasch umgesetzt werden kann.

Der RH empfahl daher dem Verteidigungsministerium, den Entwurf der Einsatzorganisation für die Direktion 6 fertigzustellen und zu verfügen.

13.3 Das Verteidigungsministerium wies in seiner Stellungnahme auf die laufende Bearbeitung der Thesenpapiere hin (TZ 8), um den zukünftigen Anforderungen für die Weiterentwicklung der Cyber–Kräfte gerecht werden zu können.

Koordination der Cyber–Defence mit dem staatlichen Cyberkrisenmanagement

14.1 (1) Das gesamtstaatliche Cyberkrisenmanagement umfasste sämtliche Maßnahmen zur Bewältigung einer Cyber–Krise einschließlich der militärischen Landesverteidigung im Cyber–Raum, der außenpolitischen Maßnahmen sowie der Zurechnung von Cyber–Angriffen an einen Akteur.

Das Cyberkrisenmanagement stellte nach § 3 Z 23 NISG ein Koordinierungsverfahren zur Bewältigung von Cyber–Krisen dar. Es diente gemäß der Strategie für Cybersicherheit 2021 als eine Plattform für die ressortübergreifende Koordination in krisenhaften Entwicklungen. Dem Innenministerium[37] oblag die Leitung und Koordination des Cyberkrisenmanagements auf operativer Ebene. Am Cyberkrisenmanagement wirkten neben Vertretungen des Bundes auch Vertretungen von Betreibern kritischer Infrastrukturen mit. Dabei orientierte es sich in seiner Zusammensetzung am Staatlichen Krisen– und Katastrophenschutzmanagement[38].

Der Cyberkrisenmanagement–Koordinationsausschuss[39] wurde auf strategischer Ebene eingerichtet, um – neben der Beratung des Innenministers, einer anderen zuständigen Bundesministerin bzw. eines Bundesministers oder der Bundesregierung – operative Maßnahmen und Maßnahmen der Öffentlichkeitsarbeit zur Bewältigung einer Cyber–Krise zu beschließen.

(2) Die Cyber Sicherheit Steuerungsgruppe hielt in ihrem Konzept zum Cyberkrisenmanagement fest, dass die administrativen Verfahren, um Cyber–Krisen zu bewältigen, in Krisen– und Kontinuitätsplänen bzw. Einsatzplänen festzulegen sind. Auf Basis von Risikoanalysen für sektorspezifische und sektorübergreifende Cyber–Bedrohungen sollten öffentliche Einrichtungen und Betreiber von kritischen Infrastrukturen diese Pläne zusammen ausarbeiten und laufend aktualisieren. Zur Zeit der Gebarungsüberprüfung bestanden keine derartigen gesamtstaatlichen Pläne.

---

37 Falls es im Falle einer Cyber–Krise zur Ausrufung des militärischen Einsatzfalles im Cyber–Raum etwa durch Abwehr von souveränitätsgefährdenden Angriffen kommt, geht die Leitung der Einsatzführung vom Innenministerium auf das Verteidigungsministerium über. Um Doppelgleisigkeiten und Informationsverluste zu vermeiden, wären die für das Cyberkrisenmanagement eingerichteten Strukturen auch im Rahmen der militärischen Landesverteidigung im Cyber–Raum zu nutzen.

38 vgl. Ministerratsbeschluss 66.000/939–II/4/03: Neuorganisation des Staatlichen Krisen– und Katastrophenschutzmanagements sowie der internationalen Katastrophenhilfe (SKKM)

39 Zusammensetzung: Generaldirektorin bzw. Generaldirektor für die öffentliche Sicherheit im Innenministerium (Leitung bei Cyber–Krisen), Chefin bzw. Chef des Generalstabs im Verteidigungsministerium (Leitung bei Cyber–Defence), Generalsekretärin bzw. Generalsekretär des Bundeskanzleramts, Generalsekretärin bzw. Generalsekretär für auswärtige Angelegenheiten und eventuell weitere Mitglieder von Bundes– oder Landesbehörden, Betreiber wesentlicher Dienste (BwD) und Computer–Notfallteams sowie Einsatzorganisationen, wenn dies zur Bewältigung der Cyber–Krise erforderlich ist (§ 25 Abs. 1 (f.) NISG).

(3) Die Grundlagen für die Zurechnung von Cyber–Angriffen (Attribuierung) an einen bestimmten Akteur sollten in einem mehrstufigen Prozess der Nachverfolgung, Identifizierung und Aufdeckung des Urhebers eines Cyber–Angriffs ermittelt werden. Die Zurechnung selbst sowie die Wahl der geeigneten zwischenstaatlichen Maßnahmen waren der politischen Ebene[40] vorbehalten. Die Abläufe einer Zurechnung waren noch nicht im Cyberkrisenmanagement umgesetzt. (Ein Souveränitätsfall war bis November 2022 noch nicht eingetreten.)

Das Verfahren der Zurechnung kommt zur Gänze dann zum Einsatz, wenn der Verdacht auf ausländische staatliche Akteure vorliegt. Der für eine Zurechnung erforderliche Prozess umfasst insbesondere

- eine technische Analyse durch Mitglieder des IKDOK,
- eine operative Bewertung der technischen Analyse durch das IKDOK,
- eine völkerrechtliche Einschätzung durch das Außenministerium und das Verteidigungsministerium sowie
- eine außenpolitische Folgenabschätzung durch das Außenministerium.

Im November 2022 war der für eine Zurechnung erforderliche Prozess noch nicht detailliert festgelegt (TZ 5).

14.2 Der RH hielt kritisch fest, dass die bereits im Juli 2019 von der Cyber Sicherheit Steuerungsgruppe empfohlenen gesamtstaatlichen Krisen– und Kontinuitätspläne für das Cyberkrisenmanagement noch nicht vorlagen, obwohl das Verteidigungsministerium eine wichtige Funktion im Cyberkrisenmanagement, im Cyber–Defence–Einsatz sogar die Leitung und Koordination innehatte. Da insbesondere in Krisensituationen eine rasche Reaktion notwendig ist, sollten vorbereitende Planungen dazu bereits vorhanden sein.

Der RH empfahl daher dem Verteidigungsministerium, gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium) die von der Cyber Sicherheit Steuerungsgruppe empfohlenen Krisen– und Kontinuitätspläne für das Cyberkrisenmanagement auszuarbeiten und in Kraft zu setzen.

Der RH verwies im Zusammenhang mit dem noch nicht abschließend festgelegten Attribuierungsverfahren (Zurechnung eines Cyber–Angriffs an einen staatlichen Akteur) auf seine Empfehlung in TZ 5.

[40] Diese Entscheidung war auf innerstaatlicher Ebene von der zuständigen Bundesministerin oder dem zuständigen Bundesminister bzw. der Bundesregierung von Fall zu Fall zu treffen.

Bedrohungsbild und erforderliche Fähigkeiten

15.1 (1) Das Verteidigungsministerium stellte 2018 in seinem Strategiepapier „Trends und Konfliktbild 2030" dar, dass das ehemals völkerrechtlich klar normierte Kriegsbild teilweise durch einen subkonventionellen Angriff in allen Bereichen (Land, Luft, Cyber und Informationsumfeld) in hybrider Form[41] ersetzt wurde. Das Verteidigungsministerium arbeitete daher auch für den Bereich Cyber an Konzepten von konkreten Bedrohungsbildern und –szenarien. Diese sollten etwa in Form einer Querschnittsdarstellung[42] auch die Voraussetzungen für den Einsatz und das Zusammenwirken der Streitkräfte im Cyber–Raum beschreiben und einer zielgerichteten Weiterentwicklung der Cyber–Kräfte im Bundesheer dienen. Im November 2022 lagen detaillierte Bedrohungsbilder erst in Entwurfsform vor.

(2) Das Bedrohungsbild 2030 und das Militärstrategische Konzept 2017 enthielten grundlegende Vorgaben zur Streitkräfteentwicklung mit Relevanz für den Bereich Cyber, z.B.

- zum koordinierten Kampf in allen Domänen inklusive des Cyber–Raums,
- zum gleichzeitigen militärischen Eigenschutz gegen Bedrohungen in allen Bereichen (Land, Luft, Cyber),
- zur Sicherstellung des erforderlichen Personals durch eine effektive Personalaufbringung und eine qualitativ hochstehende Ausbildung.

In Umsetzung dieser Vorgaben arbeitete das Verteidigungsministerium an weiteren Grundlagendokumenten für den Bereich Cyber:

- Die Planungsziele[43] aus dem Jahr 2019 zum Militärstrategischen Konzept 2017 stellten bereits ausführlicher den Bedarf an Fähigkeiten im Bereich Cyber dar. Das Verteidigungsministerium aktualisierte 2022 diese Planungsziele, um auch den aktuellen Entwicklungen Rechnung zu tragen.
- Basierend auf den Planungszielen zum Militärstrategischen Konzept 2017 arbeitete die Direktion 6 im Jahr 2020 einen Katalog von Detailfähigkeiten[44] aus, der allerdings zur Zeit der Gebarungsüberprüfung nicht[45] weiterbetrieben wurde.

[41] Bei einer hybriden Bedrohung werden mehrere bis alle verfügbaren machtpolitischen Instrumente (Außenpolitik, Wirtschaft, Zivilgewalt, Information, Technologie und Militär) eines feindlich gesinnten (staatlichen oder nichtstaatlichen) Akteurs unterhalb der Schwelle eines bewaffneten Konflikts zur strategischen Zielerreichung eingesetzt.

[42] Die Querschnittskonzepte beschreiben Grundsätze und Prinzipien der militärischen Aufgabenerfüllung in Querschnittsbereichen, die nicht waffengattungsspezifisch bzw. nicht ausschließlich einem Fähigkeitsbereich zuzuordnen sind.

[43] Die Planungsziele sind langfristige Ziele der Streitkräfteentwicklung, aus denen nach Priorisierung und Ressourcenverfügbarkeit Realisierungsziele mit unterschiedlichen zeitlichen Erfüllungsgraden abgeleitet werden.

[44] Die Fähigkeitenkataloge beschreiben den für die Erfüllung der Gesamtheit der militärischen Aufgaben des Bundesheeres erforderlichen Bedarf an Fähigkeiten einer Waffengattung.

[45] Laut Verteidigungsministerium wird der Fähigkeitenkatalog erst nach Fertigstellung der strategischen Ausrichtung weiterbearbeitet.

- Die Abteilung IKT Cyber–Planung der Direktion 6 entwarf eine Leitlinie Cyber–Verteidigung. Auch diese Leitlinie sollte zu einer raschen und nachhaltigen Streitkräfteentwicklung der Cyber–Kräfte beitragen. Das dafür zu entwickelnde Profil an Fähigkeiten fasste die in einem Entwurf vorliegende Leitlinie Cyber–Verteidigung in neun Bereiche zusammen:

1. Fähigkeiten zur Sicherstellung der Handlungsfähigkeit im Cyber–Raum (Souveränitätsschutz),

2. Fähigkeit zur Ausbildung von Cyber–Kräften,

3. Fähigkeit zum Schutz und zur Verteidigung der eigenen IKT–Systeme und Netzwerke,

4. Fähigkeit zum Objektschutz im Cyber–Raum bei kritischen Infrastrukturen und staatlichen Führungseinrichtungen,

5. Fähigkeit zur Sicherstellung eines Cyber–Lagebildes (Frühwarnsystem),

6. Fähigkeit zur Ausnützung von Systemen im Cyber–Raum,

7. Fähigkeit zum Angriff auf Computer–Netzwerke bzw. –Systeme,

8. Fähigkeit zur Zusammenarbeit mit Partnerorganisationen,

9. Fähigkeit hinsichtlich Wissensmanagement in Bezug zum Cyber–Raum Verteidigungsministerium.

Die Direktion 6 gab an, dass der Fähigkeitenaufbau zum Schutz und zur Verteidigung der eigenen IKT–Systeme und Netzwerke zur Zeit der Gebarungsüberprüfung fast vollständig umgesetzt sei.

15.2 (1) Der RH stellte kritisch fest, dass im Verteidigungsministerium detaillierte Bedrohungsbilder bzw. –szenarien, z.B. in Form einer Querschnittsdarstellung über den Einsatz im Cyber–Raum, erst als Entwurf vorlagen.

Er empfahl dem Verteidigungsministerium, detaillierte Bedrohungsbilder und –szenarien zum Einsatz im Cyber–Raum auszuarbeiten, um eine zielgerichtete Weiterentwicklung der Cyber–Kräfte voranzutreiben.

(2) Der RH kritisierte, dass im November 2022 detaillierte aktuelle Fähigkeitenplanungen für den Bereich Cyber (z.B. der Katalog der Detailfähigkeiten, die Leitlinie Cyber–Verteidigung (TZ 12)) nur als Entwurf vorlagen und noch keiner abschließenden Behandlung zugeführt wurden.

Er empfahl daher dem Verteidigungsministerium, die Konzepte zur Fähigkeitenentwicklung und Fähigkeitenplanung für den Bereich Cyber – u.a. in der Leitlinie Cyber–Verteidigung und im Katalog der Detailfähigkeiten – fertigzustellen.

Der RH stellte weiters kritisch fest, dass von den im Entwurf der Leitlinie Cyber–Verteidigung beschriebenen neun Fähigkeiten das Verteidigungsministerium zur Zeit der Gebarungsüberprüfung lediglich bei einer – der zentralen – Fähigkeit (Schutz und Verteidigung der eigenen IKT–Systeme und Netzwerke) in der Umsetzung weiter fortgeschritten war. Weitere Cyber–Fähigkeiten befanden sich erst im Aufbau.

15.3 In seiner Stellungnahme hielt das Verteidigungsministerium seine Bestrebungen fest, die strategischen Planungsdokumente wie die Leitlinie Cyber–Verteidigung und dazu erforderliche Konzepte fertigzustellen.

Weiters wies es auf die laufende Bearbeitung der Thesenpapiere hin, um den zukünftigen Anforderungen für die Weiterentwicklung der Cyber–Kräfte gerecht werden zu können.

Budget, Cyber–Sicherheitspaket

16.1 (1) Das Budget des Verteidigungsministeriums (Untergliederung 14 – Militärische Angelegenheiten) sah für die Jahre 2021 und 2022 ein eigenes Cyber–Sicherheitspaket mit 40 Mio. EUR vor.

In einer schriftlichen Weisung des Chefs des Generalstabs aus dem Jahr 2021 zu wesentlichen Vorgaben für die Realisierung des Cyber–Sicherheitspakets war u.a. festgelegt, wie diese Mittel verwendet werden sollten. Dies betraf z.B. das Abwehramt und das Heeres–Nachrichtenamt, die Streitkräfte, eine Ausbildungsbasis für die Cyber–Truppe (militärische Cyber–Range), ein Security Operation Center (SOC), das Führungsunterstützungsbataillon für den elektronischen Kampf und ein Hochsicherheitsnetz. Außerdem sollte Infrastruktur für cyberspezifische Zwecke beschafft werden. Mit Erledigung des Pakets sollte eine Abschlussmeldung inklusive Darstellung der realisierten Vorhaben an den Chef des Generalstabs erfolgen.

(2) Das Verteidigungsministerium teilte mit, dass vom Cyber–Sicherheitspaket im Jahr 2021 17,08 Mio. EUR und bis 1. September 2022 16,21 Mio. EUR aufgewendet worden seien. Im Oktober 2022 standen weitere Beschaffungen für das Jahr 2022 in Höhe von 2,86 Mio. EUR und für die Folgejahre in Höhe von 4,70 Mio. EUR vor dem Zuschlag. Die Auszahlungen aus dem Cyber–Sicherheitspaket entfielen auf Systeme für die nachrichtendienstliche Aufklärung und Abwehr von Cyber–Angriffen, den generellen Ankauf von spezieller Hard– und Software für den Cyber–

Bereich, Maßnahmen zum Eigenschutz der Cyber–Sicherheit und den Bereich der elektronischen Kampfführung.

Die diesbezügliche Abschlussmeldung inklusive Darstellung der realisierten Vorhaben an den Chef des Generalstabs lag im November 2022 nicht vor.

(3) Weitere Vorhaben auf Grundlage der Weisung des Chefs des Generalstabs verfolgte die Direktion 6 intern mit hoher Priorität, sie konnten aber laut deren Auskunft mangels dafür notwendiger Personalressourcen noch nicht umgesetzt werden. Im November 2022 lagen im Verteidigungsministerium zu den Vorhaben militärische Cyber–Range, Einsatzteam, Security Operation Center und Cyber–Intelligence erst Planungsunterlagen vor:

- Die militärische Cyber–Range beinhaltet eine Plattform als Trainingszentrum für Cyber–Soldaten und Spezialisten für Aus–, Fort– und Weiterbildung. Durch die Simulation unterschiedlicher Verteidigungs–, Aufklärungs– und Angriffsszenarien sollen die implementierten Schutzmaßnahmen ständig trainiert, geprüft und adaptiert werden können. In einer ersten Phase bis 2022 sollte diese Plattform initial eingerichtet und in einer zweiten Phase bis 2024 die Umsetzung abgeschlossen werden.
- Die Einrichtung von bis zu acht ständig verfügbaren Einsatzteams (Rapid Response Teams) zu je acht Personen war vorgesehen. Diese sollten bei schwerwiegenden Cyber–Angriffen auf Netze des Verteidigungsministeriums zur Bekämpfung der Auswirkungen oder im Rahmen einer Assistenzleistung bei Cyber–Krisen zur Bewältigung von Angriffen unmittelbar eingesetzt werden. In der ersten Phase sollten bis Ende 2022 zunächst zwei Einsatzteams im Bereich des Militärischen Cyberzentrums aufgebaut werden; in der zweiten Phase waren bis zu sechs weitere Einsatzteams im Bereich der Cyber–Truppe für die Cyber–Verteidigung geplant.
- Mit dem Security Operation Center sollte ein Informationssicherheits–Team inklusive Räumlichkeiten und Ausstattung zur Überwachung der Netzwerke des Verteidigungsministeriums aufgebaut werden. Dieses sollte Anomalien erkennen, die auf eine mögliche Kompromittierung der Systeme schließen lassen.
- Die Cyber–Intelligence umfasste das Ziel, Bedrohungen in Systemen des Verteidigungsministeriums früh zu erkennen und damit Cyber–Angriffe möglichst rasch abzuwehren. Dazu sollten die Nachrichtendienste (Abwehramt und Heeres–Nachrichtenamt) ihre Fähigkeiten in diesem Bereich ausbauen und Informationen zu potenziellen Cyber–Bedrohungen und Bedrohungsakteuren sammeln und auswerten. Gemäß dem Entwurf der Leitlinie Cyber–Verteidigung vom September 2022 sollten innerhalb des Verteidigungsministeriums die notwendigen rechtlichen Rahmenbedingungen geschaffen werden, um die Fähigkeiten der Nachrichtendienste (zu einem Cyber–Intelligence, –Surveillance, –Reconnaissance–Zentrum) entsprechend auszubauen.

16.2 Der RH hielt fest, dass mit der Verwendung von 40,85 Mio. EUR in den Jahren 2021 und 2022 (inklusive der Verpflichtungen für Folgejahre) das eigens dotierte Cyber–Sicherheitspaket finanziell ausgeschöpft wurde. Eine Abschlussmeldung an den Chef des Generalstabs inklusive Darstellung der realisierten Vorhaben lag nicht vor.

Der RH empfahl dem Verteidigungsministerium, eine Abschlussmeldung, die die zweckentsprechende Verwendung der finanziellen Mittel des Cyber–Sicherheitspakets dokumentiert, mit einer Darstellung der realisierten Vorhaben zu erstellen und vorzulegen.

Der RH betonte die Notwendigkeit der geplanten Vorhaben (militärische Cyber–Range, Rapid Response Teams, Security Operation Center und Cyber–Intelligence). Er kritisierte, dass sich diese Vorhaben erst im Planungsstadium befanden, obwohl die ersten Phasen – Einrichtung von zwei Einsatzteams und initiale Einrichtung der Plattform militärische Cyber–Range – bis Ende 2022 umzusetzen waren. Darüber hinaus kritisierte der RH, dass diese noch nicht realisierten Vorhaben in der Weisung des Chefs des Generalstabs zum Cyber–Sicherheitspaket enthalten waren, das genannte Budget jedoch bereits aufgebraucht war.

Er empfahl dem Verteidigungsministerium, das Vorhaben von zumindest zwei Einsatzteams, das Vorhaben des Security Operation Centers und das Vorhaben der Cyber–Plattform als Trainingszentrum (militärische Cyber–Range) umzusetzen.

16.3 Das Verteidigungsministerium teilte in seiner Stellungnahme – siehe auch TZ 9 – mit, dass Maßnahmen hinsichtlich der fehlenden Personalressourcen des Militärischen Cyberzentrums und zur Schließung der dargestellten Fähigkeitslücken eingeleitet würden (Rapid Response Teams, Information Security Management System, Cyber–Truppenübungsplatz, Einsatz–Security Operation Center etc.). Die Strukturerweiterung sei unabhängig von noch offenen Strukturentscheidungen im Bundesheer zu sehen, da diese in allen bisherigen Planungsvarianten in dieser Form auch zwingend erforderlich sei, um bestehende Defizite zu beheben.

Der Umfang des (für die Direktion 6) angestrebten Organisationsplans orientiere sich strikt am Pfad der weiterführenden bestehenden Kennzahl „Verbesserung der Fähigkeiten der militärischen Landesverteidigung im Cyber–Raum [...] Personeller Aufwuchs des spezialisierten Cyberpersonals“ im Wirkungsziel 1. Die Berechnung folge den bisher weiterentwickelten Planungen für die mögliche Erreichung der zweiten Ausbaustufe.

Rekrutierung und Ausbildung von Cyber–Personal

17.1 Das Verteidigungsministerium verfolgte verschiedene Ansätze, um für den Bereich Cyber–Sicherheit neues Personal aufzubauen bzw. bestehendes Personal auszubilden:

1. Im Zuge des Vorhabens „Sonderinvest 38“ wurden Leiharbeitskräfte bei entsprechender Eignung für den personellen Aufbau des Militärischen Cyberzentrums im IKT & Cybersicherheitszentrum der Direktion 6 aufgenommen, um diese später auf einen systemisierten Arbeitsplatz im Verteidigungsministerium zu übernehmen. Der Aufwand des Verteidigungsministeriums für diese Leiharbeitskräfte belief sich im Jahr 2020 auf 0,84 Mio. EUR, im Jahr 2021 auf 0,47 Mio. EUR und mit Stand 1. September 2022 auf 0,18 Mio. EUR.

2. Grundwehrdiener mit speziellen Kenntnissen im IKT–Bereich[46] bildete das Bundesheer nach der militärischen Grundausbildung in einem der Cyber–Schulungszentren des Verteidigungsministeriums aus. Den weiteren Präsenzdienst leisteten diese Cyber–Grundwehrdiener in IKT–Bereichen des Bundesheeres ab. Im Oktober 2022 standen insgesamt 60 Cyber–Grundwehrdiener im Bundesheer im Einsatz. Nach Ende des Präsenzdienstes erging an die fachlich Geeigneten ein Angebot für eine weitere Beschäftigung in diesem Tätigkeitsfeld im Bundesheer.

3. Die Führungsunterstützungsschule in der Starhemberg–Kaserne war die Ausbildungsstätte zur Kader–Aus–, –Fort– und –Weiterbildung im Cyber–Bereich, zur elektronischen Kampfführung sowie für die Durchführung der taktischen und gefechtstechnischen Ausbildung aller Cyber–Kräfte. Im Zuge von Lehrgängen und Seminaren wurden dort jährlich über 1.000 Lehrgangsteilnehmerinnen und –teilnehmer ausgebildet.

4. Seit September 2022 lief an der Theresianischen Militärakademie in Wiener Neustadt ein sechssemestriger Fachhochschul–Bachelorstudiengang[47] für militärische informations– und kommunikationstechnologische Führung (FH–BaStg Mil–IKTFü). Bei diesem Studiengang mit anwendungsorientiertem IKT–Schwerpunkt wurden zukünftige IKT–Offizierinnen und –Offiziere zu Expertinnen und Experten für den Einsatz von IKT–Systemen, der elektronischen Kampfführung sowie zu Spezialisten für den Betrieb und die Überwachung von militärischen Einsatznetzwerken ausgebildet. Im ersten Semester nahmen 24 Militärpersonen teil.

[46] z.B. höhere technische Lehranstalten Informatik, Informationstechnologie, Netzwerktechnik, Medientechnik, höhere allgemeinbildende Schulen mit Schwerpunkt IT, nachweisliche Zusatzqualifikationen und Weiterbildung im IT–Bereich

[47] mit 180 ECTS–Anrechnungspunkten (ECTS = European Credit Transfer and Accumulation System (Europäisches System zur Übertragung und Akkumulierung von Studienleistungen))

5. Auf einer künftig zu errichtenden Plattform als Trainingszentrum für Cyber–Soldaten und Spezialisten für Aus–, Fort– und Weiterbildung (militärische Cyber–Range) sollten durch die Simulation unterschiedlicher Verteidigungs–, Aufklärungs– und Angriffsszenarien die implementierten Schutzmaßnahmen ständig trainiert, geprüft und adaptiert werden (TZ 20).

17.2 Der RH begrüßte sowohl die Initiativen zur Rekrutierung von neuem als auch zur Ausbildung von bestehendem Cyber–Personal innerhalb des Verteidigungsministeriums.

Er empfahl dem Verteidigungsministerium, die Möglichkeit zur Ableistung des Präsenzdienstes als Cyber–Grundwehrdiener in der diesbezüglichen Zielgruppe aktiv zu bewerben (z.B. bei den Stellungskommissionen), da hierbei auch einschlägige Kenntnisse und Berufserfahrung vermittelt werden. Außerdem sollten innerhalb des Verteidigungsministeriums vermehrt Einsatzmöglichkeiten für diese Grundwehrdiener geschaffen werden.

Zusammenarbeit auf Bundesebene

Leistungen des Verteidigungsministeriums im Cyber–Bereich gemäß NISG

18.1 (1) Zweck des NISG war es, ein hohes Sicherheitsniveau von Netz– und Informationssystemen zu gewährleisten. In diesem Bundesgesetz waren Maßnahmen festgelegt, durch die die Betreiber wesentlicher Dienste in sieben Sektoren (Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur) sowie die Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung dieses Niveau erreichen sollten.

Die diesbezüglichen Aufgaben des Verteidigungsministeriums zeigt die folgende Tabelle:

Tabelle 5: Organisation und Aufgaben nach dem Netz– und Informationssystemsicherheitsgesetz (NISG)

Einrichtung/Gremium	gesamtstaatliche Aufgabe	Aufgabe des Verteidigungsministeriums
Innenministerium	Erstellen des Cyber–Lagebildes durch das Innenministerium für verfassungsmäßige Einrichtungen[1] und kritische Infrastrukturen[2]	Einbringen von Informationen über die militärische Lage und aktuelle Entwicklungen zu Cyber–Ereignissen
	NIS–Meldeanalysesystem[3] (IKT–basiert) des Innenministeriums zur Erfassung und Analyse der Meldungen von Cyber–Risiken, –Vorfällen und –Sicherheitsvorfällen	Meldung von Cyber–Risiken, –Vorfällen und –Sicherheitsvorfällen
	IKT–Frühwarnsysteme[3] des Innenministeriums: Sensornetzwerk zur Erfassung von Indikatoren, die auf eine Kompromittierung eines IT–Systems hinweisen, für das Innenministerium sowie optional für daran teilnehmende Organisationen	Teilnahme und Datenübermittlung (optional)
IKDOK (Innerer Kreis der Operativen Koordinierungsstruktur)	bestehend aus den vier Sicherheitsressorts (Innen–, Außen– und Verteidigungsministerium, Bundeskanzleramt) unter Leitung des Innenministeriums: Informationsaustausch und Erörterung des Cyber–Lagebildes und der Erkenntnisse aus IKT–Frühwarnsystemen	Einbringen von Informationen über die militärische Lage und aktuelle Entwicklungen zu Cyber–Ereignissen; Analyse des Lagebildes
OpKoord (Operative Koordinierungsstruktur)	bestehend aus dem IKDOK, den Computer–Notfallteams und allenfalls von Vorfällen betroffenen Einrichtungen: Informationsaustausch und Erörterung des Cyber–Lagebildes und der Erkenntnisse aus IKT–Frühwarnsystemen (Sitzungen fanden wegen Personenidentität zum IKDOK teilweise nicht eigens statt; das Gremium OpKoord wird neu strukturiert)	Einbringen von Informationen über die militärische Lage und aktuelle Entwicklungen zu Cyber–Ereignissen; Analyse des Lagebildes
GovCERT	Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) unter Leitung des Bundeskanzleramts: Information und Beratung zu Cyber–Ereignissen	Informationsaustausch über Risiken, Vorfälle und Sicherheitsvorfälle
Cyberkrisenmanagement	Koordinierungsverfahren zur Bewältigung von Cyber–Krisen nach dem NISG	Beratung des Innenministeriums über das Vorliegen einer Cyber–Krise und in der Cyber–Krise
Cyberkrisenmanagement–Koordinationsausschuss	Koordinationsausschuss unter der Leitung des Generaldirektors für die öffentliche Sicherheit zur Beratung der Innenministerin bzw. des Innenministers betreffend das Vorliegen einer Cyber–Krise sowie während der Krise	Teilnahme des Generalstabschefs im Koordinationsausschuss zur Beratung des Innenministeriums

[1] z.B. Bundespräsident, Bundesregierung, Nationalrat, oberste Organe der Vollziehung und Gerichtsbarkeit
[2] nach § 22 Abs. 1 Z 6 Sicherheitspolizeigesetz, BGBl. 566/1991 i.d.g.F.
[3] zur Zeit der Gebarungsüberprüfung noch nicht in Betrieb

Quellen: BMLV; NISG

Diese Aufgaben hatte das Verteidigungsministerium bzw. Bundesheer in den vom Innenministerium geleiteten Gremien – bestehend aus den vier Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium und Verteidigungsministerium) – teilweise permanent, teilweise im Anlassfall zu erfüllen. Die Leistungen wurden weitgehend vom Militärischen Cyberzentrum, vom Abwehramt und vom Heeres–Nachrichtenamt erbracht.

(2) Die nachfolgende Tabelle zeigt die mitwirkenden Akteure des Verteidigungsministeriums an Gremien zur Cyber–Sicherheit:

Tabelle 6: Mitwirkung in Gremien mit Bezug zur Cyber–Defence

Gremium	Vorsitz	Mitglieder	Vertretung des Verteidigungsministeriums
Gremien gemäß NISG			
IKDOK (Innerer Kreis der Operativen Koordinierungsstruktur)	Innenministerium	Bundeskanzleramt, Innen–, Außen– und Verteidigungsministerium	Militärisches Cyberzentrum, Abwehramt, Heeres–Nachrichtenamt
OpKoord (Operative Koordinierungsstruktur)	Innenministerium	Mitglieder des IKDOK und der Computer–Notfallteams; soweit erforderlich, Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung	sofern eigene Sitzungen stattfanden: Militärisches Cyberzentrum, Abwehramt, Heeres–Nachrichtenamt
GovCERT	Bundeskanzleramt	geführt vom nationalen Computer–Notfallteam CERT.at unter Leitung des Bundeskanzleramts	Militärisches Cyberzentrum: Informationsaustausch im IKDOK, Mitglied des Beirats des GovCERT, direkte anlassbezogene Zusammenarbeit bei Vorfällen und Sicherheitsvorfällen
Cyberkrisenmanagement	Innenministerium	Bundeskanzleramt, Innen–, Außen– und Verteidigungsministerium	Direktion 6 in Bezug auf Cyber–Aufgaben
Cyberkrisenmanagement–Koordinationsausschuss	Innenministerium	Bundeskanzleramt, Innen–, Außen– und Verteidigungsministerium: der Generaldirektor für die öffentliche Sicherheit, die Generalsekretäre des Bundeskanzleramts und Außenministeriums und der Chef des Generalstabs; soweit erforderlich, Vertretungen von Bundes– und Landesbehörden und Betreibern wesentlicher Dienste	Chef des Generalstabs
sonstige[1] Gremien			
Cyber Sicherheit Steuerungsgruppe und –Team	Bundeskanzleramt	Bundeskanzleramt, Innen–, Außen–, Verteidigungs– und Justizministerium; themenorientiert weitere Bundesministerien, Länder (Vorbereitung und Bearbeitung von Cyber–Sicherheitsthemen)	Generaldirektion Verteidigungspolitik (Sektion I)
CERT–Verbund	Bundeskanzleramt	Computer–Notfallteams	militärisches Computer–Notfallteam (MilCERT) als (Fähigkeiten–)Bereich des Militärischen Cyberzentrums
Austrian Trust Circle (ATC)	Bundeskanzleramt	Bundeskanzleramt, Innen– und Außenministerium (eine Initiative von CERT.at (nic.at GmbH) und dem Bundeskanzleramt)	Militärisches Cyberzentrum und Abwehramt

NISG = Netz– und Informationssystemsicherheitsgesetz Quellen: BMLV; NISG

[1] Sonstige Gremien waren:
- Die gesamtstaatliche Cyber Sicherheit Steuerungsgruppe (CSS) und das CSS–Team bearbeiteten und bereiteten spezifische Cyber–Sicherheitsthemen vor.
- Der CERT–Verbund war ein auf freiwilliger Basis bestehendes Gremium für Informationsaustausch und Networking von österreichischen Computer–Notfallteams. Das militärische Computer–Notfallteam des Militärischen Cyberzentrums nahm am österreichischen CERT–Verbund teil.
- Der Austrian Trust Circle (ATC) war eine nationale Initiative für den fachlichen Informationsaustausch zu Sicherheit und Vorfällen in der Informations– und Kommunikationstechnik.

18.2 Der RH hielt fest, dass das Verteidigungsministerium – neben dem permanenten Eigenschutz der militärischen IKT–Systeme und den anlassbezogenen Cyber–Assistenzleistungen – wesentliche Aufgaben nach dem NISG als Beitrag zur gesamtstaatlichen Cyber–Sicherheit zu erfüllen hatte. Diese wurden vom Militärischen Cyberzentrum, vom Abwehramt und vom Heeres–Nachrichtenamt erbracht.

Cyber–Lagebild

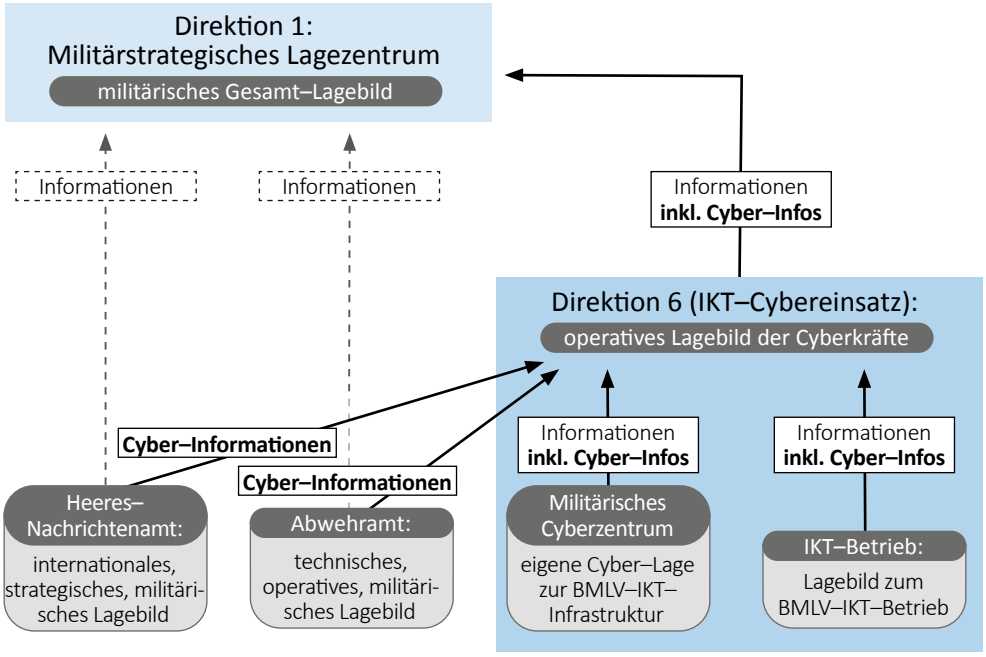
19.1 (1) Eine zentrale Aufgabe für die gesamtstaatliche Cyber–Sicherheit war es, auf Grundlage von aktuellen Cyber–Ereignissen – Risiken, Vorfällen und Sicherheitsvorfällen – ein Cyber–Lagebild zu erstellen. Dieses bildete z.B. Schadsoftware, Schwachstellen in kommerzieller Software und insbesondere Cyber–Angriffe auf Institutionen als Risikoszenario ab.

Gemäß NISG hatte das Innenministerium das staatliche Cyber–Lagebild zu erstellen, das dann im IKDOK analysiert und mit entsprechenden Empfehlungen für Sicherheitsmaßnahmen ergänzt wurde.

Informationen zum gesamtstaatlichen Cyber–Lagebild brachte das Verteidigungsministerium im Zuge des IKDOK ein. Hierbei waren vom Verteidigungsministerium das Militärische Cyberzentrum sowie das Abwehramt und das Heeres–Nachrichtenamt vertreten. Darüber hinaus unterstützten das Bundeskanzleramt – auch im Wege des Computer–Notfallteams der öffentlichen Verwaltung (GovCERT) – und das Außenministerium bei diesem Prozess das Innenministerium durch cybersicherheitsrelevante Informationen u.a. auch von europäischen bzw. internationalen Institutionen. Die Ergebnisse wurden im wöchentlichen IKDOK–Jour–fixe behandelt sowie im monatlichen, ressortübergreifenden gesamtstaatlichen Cyber–Lagebild zusammengefasst; dieses wurde im Rahmen des GovCERT u.a. an die obersten Organe des Bundes und im Rahmen der Operativen Koordinierungsstruktur (OpKoord) auch an die Länder übermittelt. Im Bedarfsfall, z.B. einer Cyber–Krise, wurden Sonderlagebilder erstellt.

(2) Das Verteidigungsministerium erstellte eigene militärische Lagebilder, die auch Cyber–Aspekte enthielten:

Abbildung 4: Militärische Lagebilder des Verteidigungsministeriums



Quelle: BMLV; Darstellung: RH

Die dafür notwendigen Cyber–relevanten Informationen[48] stellten nicht nur die zuständigen Organisationen des Verteidigungsministeriums bzw. des Bundesheeres zur Verfügung, sie ergaben sich auch aus Informationen durch den IKDOK, durch das Computer–Notfallteam der öffentlichen Verwaltung (GovCERT) sowie von Partnerorganisationen und aus Berichten.

Der Prozess der Abstimmung und Zusammenarbeit zur Lagebilderstellung im Verteidigungsministerium erfolgte weitgehend manuell, teilweise automatisiert und war nicht schriftlich festgelegt; eine IT–Anwendung zur weitergehenden Unterstützung bei der Lagebilderstellung war in Umsetzung.

- Die Direktion 6 (Abteilung IKT–Cybereinsatz) erstellte täglich ein operatives Lagebild der Cyber–Kräfte, das wöchentlich und monatlich zusammengeführt wurde. Dieses stützte sich dabei auf Informationen aus
  - dem Cyber–Lagebild des Militärischen Cyberzentrums (Referat Lagezentrum) bezüglich der eigenen IKT–Infrastruktur des Verteidigungsministeriums,

[48] z.B. Sicherheitsmeldungen, Cyber–Ereignisse und –Vorfälle, die Bewertung entdeckter Sicherheitsschwachstellen und Warnmeldungen

- dem Lagebild zum IKT–Betrieb sowie
- den cyberspezifischen Informationen aus den täglichen Lagebildern vom Heeres–Nachrichtenamt sowie Abwehramt.

- Das Heeres–Nachrichtenamt erstellte täglich ein eigenes strategisches, militärisches Lagebild zur internationalen Lage, das im Anlassfall auch Cyber–Aspekte enthielt; diese Lagebilder wurden direkt an die Direktion 6 weitergeleitet.
- Das Abwehramt wiederum erstellte täglich ein eigenes Lagebild mit militärisch operativen Gesichtspunkten auch unter Berücksichtigung cyberrelevanter Informationen; diese Lagebilder wurden ebenfalls an die Direktion 6 weitergeleitet.
- Die genannten Teillagebilder, die nicht nur cyberspezifische Aspekte enthielten, sowie weitere militärische Lagebilder des Verteidigungsministeriums bzw. des Bundesheeres wurden in der Abteilung Militärstrategisches Lagezentrum zu einem militärischen Gesamt–Lagebild zusammengeführt.

(3) Das Verteidigungsministerium hatte nicht festgelegt, ob die Ergebnisse des militärischen Cyber–Lagebildes[49] zur künftigen Beurteilung einer Souveränitätsgefährdung infolge von Cyber–Ereignissen herangezogen werden sollen. Auch die Fragen einer 24/7–Verfügbarkeit eines militärischen Cyber–Lagezentrums sowie der strukturierten Informationsweiterleitung an das militärische Computer–Notfallteam (MilCERT) und an die künftigen Rapid Response Teams hatte das Verteidigungsministerium nicht entschieden.

19.2 Der RH konnte die Logik der bedarfsgerecht getrennt erstellten zivilen und militärischen Lagebilder nachvollziehen. In seinem Bericht „Koordination der Cyber–Sicherheit“ (Reihe Bund 2022/13) hatte er empfohlen, im Innenministerium ein permanentes (ziviles) Lagezentrum einzurichten.

In diesem Zusammenhang empfahl er auch dem Verteidigungsministerium, ein permanentes – militärisches – Cyber–Lagezentrum einzurichten und hierbei die Frage der zeitlichen Verfügbarkeit dieser Einrichtung zu klären. Weiters wäre zu regeln, wie Informationen strukturiert an das militärische Computer–Notfallteam und die künftigen Rapid Response Teams weitergeleitet werden.

Da das Cyber–Lagebild die aktuellen Cyber–Ereignisse (Risiken, Vorfälle und Sicherheitsvorfälle) darstellte, war es eine Grundlage dafür, das Ausmaß ihrer Auswirkungen zu beurteilen. Damit stellte das Cyber–Lagebild für das Verteidigungsministerium eine wesentliche Information zur Beurteilung einer möglichen Souveränitätsgefährdung dar.

[49] hinsichtlich Information, Analyse, Prävention, Maßnahmen, Steuerung, Koordinierung oder Frühwarnung

Der RH empfahl dem Verteidigungsministerium, die Anforderungen an ein militärisches Cyber–Lagebild hinsichtlich Information, Analyse, Prävention, Maßnahmen, Steuerung, Koordinierung oder Frühwarnung mit den noch festzulegenden Kriterien bzw. Optionen zur Beurteilung von Souveränitätsgefährdungen (TZ 5) abzustimmen.

Er empfahl weiters, das mögliche Vorliegen einer Souveränitätsgefährdung auch im gesamtstaatlichen Lagezentrum des Innenministeriums gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Innenministerium, Außenministerium) zu behandeln.

19.3 Das Verteidigungsministerium wies in seiner Stellungnahme wiederholt (siehe TZ 8) auf die laufende Bearbeitung der Thesenpapiere hin, um den zukünftigen Anforderungen für die Weiterentwicklung der Cyber–Kräfte gerecht werden zu können.

Übungen im Cyber–Bereich

20.1 (1) Ziel von Übungen im Cyber–Bereich war es, spezifische Erfahrungen zu sammeln, aktuellen Entwicklungen in der Praxis Rechnung zu tragen sowie Fähigkeiten aufzubauen bzw. zu erweitern, um einen Ernstfall zu erproben sowie die Praxistauglichkeit der dafür vorgesehenen Maßnahmen zu verifizieren. In den Jahren 2018 bis 2022 nahm das Verteidigungsministerium an 32 Cyber–Übungen teil; an diesen beteiligten sich neben dem Militärischen Cyberzentrum auch das Abwehramt sowie das Heeres–Nachrichtenamt. Beispielhafte nationale Übungen im Cyber–Bereich waren ASDEM („Austrian Strategic Decision Making Exercise“, gesamtstaatliche Cyber–Übung) und Cyber–Europe, beispielhafte internationale Übungen waren Locked Shields, Common Roof, Crossed Sword oder Cyber Phalanx. Laut Aussage des Verteidigungsministeriums konnte durch Übungen im Cyber–Bereich die Cyber–Resilienz verbessert werden.

Inhalte der Übungen waren neben technischen Aspekten – z.B. die Identifizierung und Abwehr verschiedener Cyber–Angriffe, das Incident Handling oder die Netzwerkanalyse – auch begleitende Aspekte wie die Cyber–Rechtslage oder Öffentlichkeitsarbeit. Eine militärische Cyber–Range als zentrale technische Übungsumgebung war geplant, im November 2022 jedoch nicht verfügbar (zur Empfehlung, eine Cyber–Range umzusetzen, siehe TZ 16).

(2) Im Rahmen der gesamtstaatlichen Cyber–Übung ASDEM 2018 hatten das Verteidigungsministerium bzw. das Bundesheer gemeinsam mit dem Innenministerium – neben verschiedenen anderen Aspekten – den Übergang vom Cyberkrisenmanagement des Innenministeriums zum militärisch geleiteten Cyber–Defence–Fall ansatzweise geübt. Hinsichtlich der Feststellung einer Souveränitätsgefährdung und den dann erforderlichen Maßnahmen wurden Schwachstellen identifiziert.

Spezifische Übungen eines Cyber–Defence–Falls aufgrund einer Souveränitätsgefährdung hatten das Verteidigungsministerium bzw. das Bundesheer nicht durchgeführt: Es waren weder Konzepte zur Feststellung einer Souveränitätsgefährdung, notwendige Maßnahmen beim Übergang von einer Cyber–Krise in einen Cyber–Defence–Einsatz noch Konzepte zur Zurechnung eines Angriffs an einen staatlichen Akteur erprobt worden.

(3) Die internationale Kooperation des Verteidigungsministeriums bzw. des Bundesheeres im Cyber–Bereich leistete einen Beitrag dazu, die Interoperabilität von Systemen sicherzustellen; weiters konnten die Fähigkeiten im Cyber–Bereich gesteigert[50] sowie spezifische Informationen ausgetauscht werden. Die Kooperation stellte auch einen solidarischen Beitrag zur gemeinsamen Sicherheits– und Verteidigungspolitik[51] der EU dar. Das Verteidigungsministerium bzw. das Bundesheer arbeitete im internationalen Bereich u.a. mit Deutschland und der Schweiz regelmäßig und intensiv zusammen. Die internationale Zusammenarbeit des Verteidigungsministeriums bzw. des Bundesheeres im Cyber–Bereich umfasste u.a.

- nachrichtendienstliche Kooperationen und Informationsaustausch,
- gemeinsame Cyber–Übungen,
- Zusammenarbeit im Bereich Forschung und Entwicklung sowie
- Kooperationen bei Aus– und Weiterbildung.

Hierdurch konnten cyberspezifisches Wissen und Cyber–Fähigkeiten aufgebaut, erweitert oder vertieft werden.

20.2 Die bisherige Teilnahme des Verteidigungsministeriums bzw. des Bundesheeres an nationalen und internationalen Übungen im Cyber–Raum war wesentlich, um spezifisches Wissen und Fähigkeiten aufzubauen, zu erweitern und zu testen. Der RH merkte kritisch an, dass eine militärische Cyber–Range als ein Instrument zur effektiven Durchführung von Übungen im Cyber–Raum auf Ebene des Bundesheeres noch nicht umgesetzt war, und verwies auf seine Empfehlung in TZ 16.

Der RH kritisierte, dass das Verteidigungsministerium bzw. das Bundesheer noch keine spezifischen Übungen zu einem Cyber–Defence–Fall aufgrund einer Souveränitätsgefährdung durchgeführt hatten. Damit war eine in der Verantwortung des Verteidigungsministeriums bzw. des Bundesheeres liegende Aufgabe weder in Konzepten festgelegt noch in Übungsszenarien erprobt worden. Die 2018 mit dem Innenministerium vorgenommene Übung betreffend das Cyberkrisenmanagement hatte Schwachstellen beim Übergang auf den Cyber–Defence–Fall identifiziert.

[50] u.a. durch Beobachtungen aktueller einschlägiger Entwicklungen und Verbesserungen beim Lagebild

[51] Diese definiert allgemeine Zielsetzungen im Bereich Cyber–Defence für die einzelnen Mitgliedstaaten. Das Verteidigungsministerium bzw. Bundesheer leistet, wie in allen anderen Teilbereichen der Streitkräfte, auch im Cyber–Bereich einen solidarischen Beitrag.

Der RH empfahl daher dem Verteidigungsministerium, Übungen zu einem Cyber–Defence–Fall mit Souveränitätsgefährdung verstärkt durchzuführen. Dabei wären u.a. die Fragen der Feststellung eines Souveränitätsfalls, des Übergangs von einer Cyber–Krise in einen Cyber–Defence–Einsatz und der Zurechnung eines Angreifers an einen staatlichen Akteur zu behandeln. Weitere zu übende Szenarien wären der Schutz der verfassungsmäßigen Einrichtungen und der kritischen Infrastruktur sowohl in Bezug auf einen Cyber–Defence–Einsatz als auch hinsichtlich einer Assistenzleistung.

Schlussempfehlungen

21 Zusammenfassend empfahl der RH dem Bundesministerium für Landesverteidigung:

(1) Die Fertigstellung der Leitlinie Cyber–Verteidigung wäre voranzutreiben und diese ehestmöglich zu erlassen. (TZ 4, TZ 12)

(2) Die Konkretisierung des Konzepts Gesamtstaatliches Cyber Krisenmanagement (CKM 2019) wäre im Zusammenwirken mit den anderen Sicherheitsressorts (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für europäische und internationale Angelegenheiten) im Hinblick auf einen Cyber–Defence–Fall weiterzuverfolgen, um die angestrebten Ziele – Klarstellung von Verantwortlichkeiten, Einrichtung von Kommunikationskanälen innerhalb einer und zwischen mehreren Gebietskörperschaften und effiziente Koordination – zu erreichen. (TZ 5)

(3) In der Leitlinie Cyber–Verteidigung oder anderen geeigneten Dokumenten wären – als Grundlage der Entscheidung über einen Cyber–Defence–Einsatz – Kriterien bzw. Optionen festzulegen, um Souveränitätsverletzungen oder –gefährdungen infolge von Cyber–Angriffen zu beurteilen. Diese hätten jedenfalls die Fragen

- der Feststellung und Bewertung einer Beeinträchtigung der Unabhängigkeit und Funktionsfähigkeit der Einrichtungen von Gebietskörperschaften und
- der Bedeutung einzelner kritischer Infrastrukturen hinsichtlich einer Verletzung der Souveränität Österreichs zu behandeln.
- Darüber hinaus wäre auch zu klären, welches Ausmaß mögliche Auswirkungen eines Cyber–Angriffs erreichen müssten, um einen militärischen Einsatz zu rechtfertigen.

Damit soll im Anlassfall eine koordinierte, strategisch geleitete und rasche Bewältigung von Gefährdungssituationen sichergestellt werden. (TZ 5)

(4) Die Umsetzung des Vorschlags für ein Verfahrenskonzept hinsichtlich der Zurechnung (Attribuierung) eines Cyber–Angriffs an einen staatlichen bzw. staatsnahen Akteur wäre gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für europäische und internationale Angelegenheiten) voranzutreiben; das Verfahrenskonzept wäre in Form eines aktualisierten Konzepts operativ zu setzen. (TZ 5)

(5) Das Bundesministerium für Landesverteidigung sollte gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für europäische und internationale Angelegenheiten) in einen permanenten Austausch hinsichtlich der Parameter für Assistenzleistungen im Cyber–Bereich eintreten. (TZ 6)

(6) Gemeinsam mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport wäre – in Umsetzung eines gesamtstaatlichen Cyber–Sicherheitskonzepts sowie der Empfehlung des Nationalen Sicherheitsrates vom Februar 2020 – für eine ausreichende personelle und technische Ausstattung zu sorgen, um die permanente Einsatzfähigkeit von Cyber–Kräften zu gewährleisten. (TZ 6)

(7) Die im Bundesministerium für Landesverteidigung und im Österreichischen Bundesheer vorhandene Expertise im Cyber–Bereich wäre aktiv auch im Sinne der Prävention in die notwendigen gesamtstaatlichen Prozesse einzubringen (Netz– und Informationssystemsicherheitsgesetz, Amtshilfe, Unterstützungsleistungen). (TZ 7)

(8) Die neue Direktion 6 – IKT und Cyber wäre per Erlass zu verfügen und die Aufgaben ihrer Organisationseinheiten sowie die Gesamtziele wären schriftlich festzulegen. (TZ 8)

(9) Die Verhandlungen mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport über die Systemisierung der Arbeitsplätze in der Direktion 6 – IKT und Cyber wären mit dem Ziel einer Einigung und einer zügigen Umsetzung der Organisationspläne im Bundesministerium für Landesverteidigung rasch wieder aufzunehmen und abzuschließen. (TZ 9)

(10) Die Überarbeitung der Abläufe und Prozesse in der Direktion 6 – IKT und Cyber wäre nach Verfügung der Organisationspläne so rasch wie möglich abzuschließen und in Kraft zu setzen. (TZ 9)

(11) Die im Militärischen Cyberzentrum vorhandenen Arbeitsplätze wären rasch zu besetzen. (TZ 9)

(12) Die für den weiteren Aufbau von Cyber–Kompetenzen im Militärischen Cyberzentrum geplanten Personalstände wären umzusetzen. (TZ 9)

(13) Die zur Feststellung der Cyber–Lage notwendigen Prozesse und die Zusammenarbeit wären sowohl innerhalb der Direktion 6 – IKT und Cyber als auch mit den militärischen Nachrichtendiensten (Abwehramt, Heeres–Nachrichtenamt) schriftlich festzulegen und deren Einhaltung zu verfügen. (TZ 11)

(14) Die Bearbeitung des im Entwurf vorliegenden Querschnittskonzepts „Einsatz im Cyber–Raum“ wäre möglichst rasch abzuschließen und dieses in Kraft zu setzen. (TZ 12)

(15) Aus dem in den Dokumenten Leitlinie Cyber–Verteidigung und Querschnittskonzept „Einsatz im Cyber–Raum“ festgehaltenen Handlungsbedarf wären Einzelmaßnahmen abzuleiten und für deren Umsetzung ein Zeitplan und die dafür zuständigen Organisationseinheiten festzulegen. (TZ 12)

(16) Nach Abschluss der Organisationsreform der Direktion 6 – IKT und Cyber wäre die vorläufige Geschäftsordnung an die neue Organisationsstruktur anzupassen und neu zu erlassen. (TZ 12)

(17) Der Entwurf der Einsatzorganisation für die Direktion 6 – IKT und Cyber wäre fertigzustellen und zu verfügen. (TZ 13)

(18) Die von der Cyber Sicherheit Steuerungsgruppe empfohlenen Krisen– und Kontinuitätspläne für das Cyberkrisenmanagement wären gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für europäische und internationale Angelegenheiten) auszuarbeiten und in Kraft zu setzen. (TZ 14)

(19) Detaillierte Bedrohungsbilder und –szenarien zum Einsatz im Cyber–Raum wären auszuarbeiten, um eine zielgerichtete Weiterentwicklung der Cyber–Kräfte voranzutreiben. (TZ 15)

(20) Die Konzepte zur Fähigkeitenentwicklung und Fähigkeitenplanung für den Bereich Cyber – u.a. in der Leitlinie Cyber–Verteidigung und im Katalog der Detailfähigkeiten – wären fertigzustellen. (TZ 15)

(21) Eine Abschlussmeldung, die die zweckentsprechende Verwendung der finanziellen Mittel des Cyber–Sicherheitspakets dokumentiert, wäre mit einer Darstellung der realisierten Vorhaben zu erstellen und vorzulegen. (TZ 16)

(22) Das Vorhaben von zumindest zwei Einsatzteams, das Vorhaben des Security Operation Centers und das Vorhaben der Cyber–Plattform als Trainingszentrum (militärische Cyber–Range) wären umzusetzen. (TZ 16)

(23) Die Möglichkeit zur Ableistung des Präsenzdienstes als Cyber–Grundwehrdiener wäre in der diesbezüglichen Zielgruppe aktiv zu bewerben (z.B. bei den Stellungskommissionen), da hierbei auch einschlägige Kenntnisse und Berufserfahrung vermittelt werden. Außerdem sollten innerhalb des Bundes-

ministeriums für Landesverteidigung vermehrt Einsatzmöglichkeiten für diese Grundwehrdiener geschaffen werden. (TZ 17)

(24) Es wäre ein permanentes militärisches Cyber–Lagezentrum einzurichten und hierbei die Frage der zeitlichen Verfügbarkeit dieser Einrichtung zu klären. Weiters wäre zu regeln, wie Informationen strukturiert an das militärische Computer–Notfallteam und die künftigen Rapid Response Teams weitergeleitet werden. (TZ 19)

(25) Die Anforderungen an ein militärisches Cyber–Lagebild hinsichtlich Information, Analyse, Prävention, Maßnahmen, Steuerung, Koordinierung oder Frühwarnung wären mit den noch festzulegenden Kriterien bzw. Optionen zur Beurteilung von Souveränitätsgefährdungen (TZ 5) abzustimmen. (TZ 19)

(26) Das mögliche Vorliegen einer Souveränitätsgefährdung wäre auch im gesamtstaatlichen Lagezentrum des Bundesministeriums für Inneres gemeinsam mit den anderen Sicherheitsressorts (Bundeskanzleramt, Bundesministerium für Inneres, Bundesministerium für europäische und internationale Angelegenheiten) zu behandeln. (TZ 19)

(27) Übungen zu einem Cyber–Defence–Fall mit Souveränitätsgefährdung wären verstärkt durchzuführen. Dabei wären u.a. die Fragen der Feststellung eines Souveränitätsfalls, des Übergangs von einer Cyber–Krise in einen Cyber–Defence–Einsatz und der Zurechnung eines Angreifers an einen staatlichen Akteur zu behandeln. Weitere zu übende Szenarien wären der Schutz der verfassungsmäßigen Einrichtungen und der kritischen Infrastruktur sowohl in Bezug auf einen Cyber–Defence–Einsatz als auch hinsichtlich einer Assistenzleistung. (TZ 20)

Rechnungshof Österreich

Wien, im Oktober 2023
Die Präsidentin:

Dr. Margit Kraker

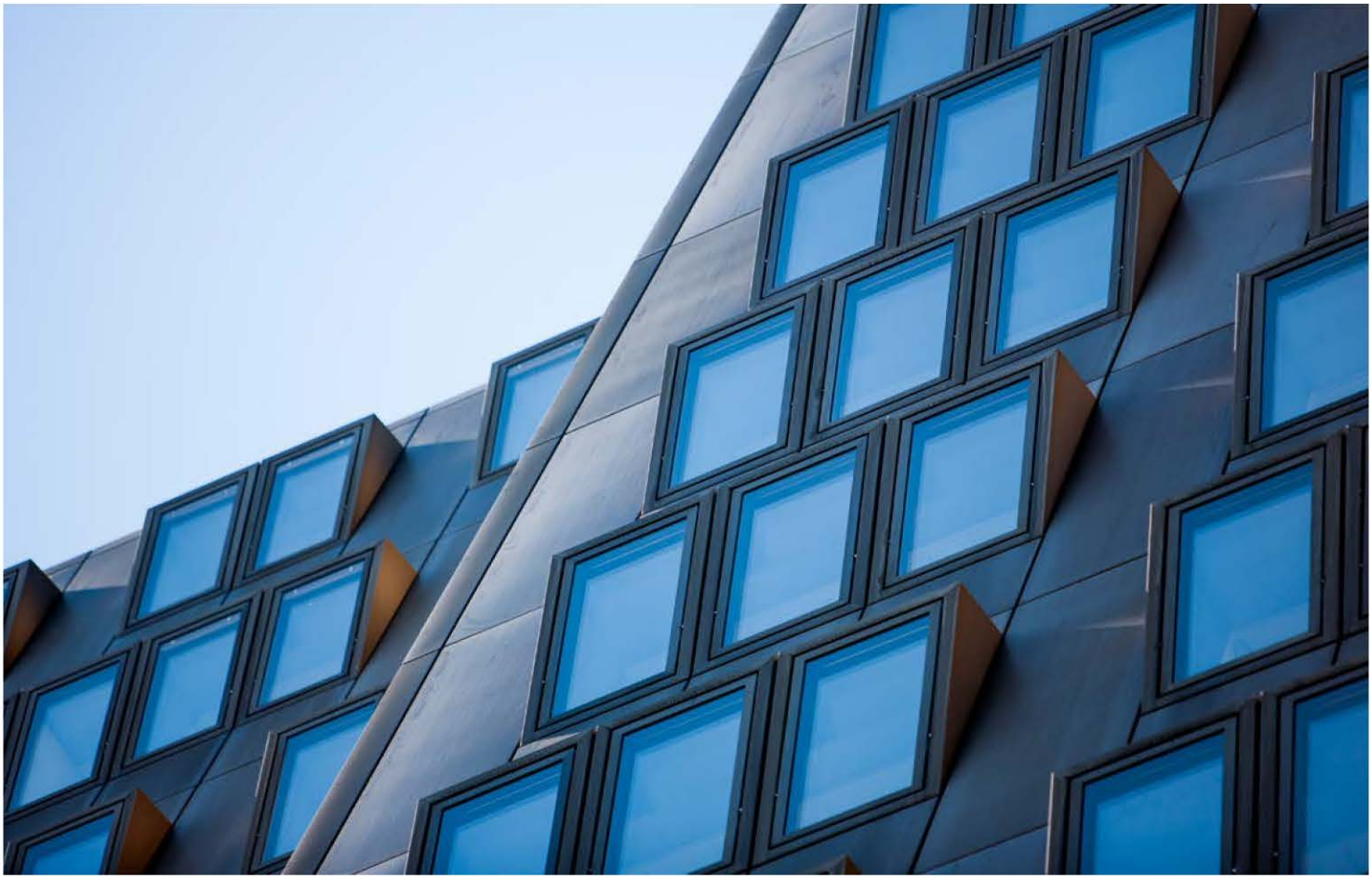
Anhang

Ressortbezeichnung und –verantwortliche

Tabelle A: Verteidigungsministerium

Zeitraum	Ressortbezeichnung	Bundesministerin
seit 7. Jänner 2020	Bundesministerium für Landesverteidigung	Mag. Klaudia Tanner

Quelle: Parlament



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2023-10-20T09:22:16+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	