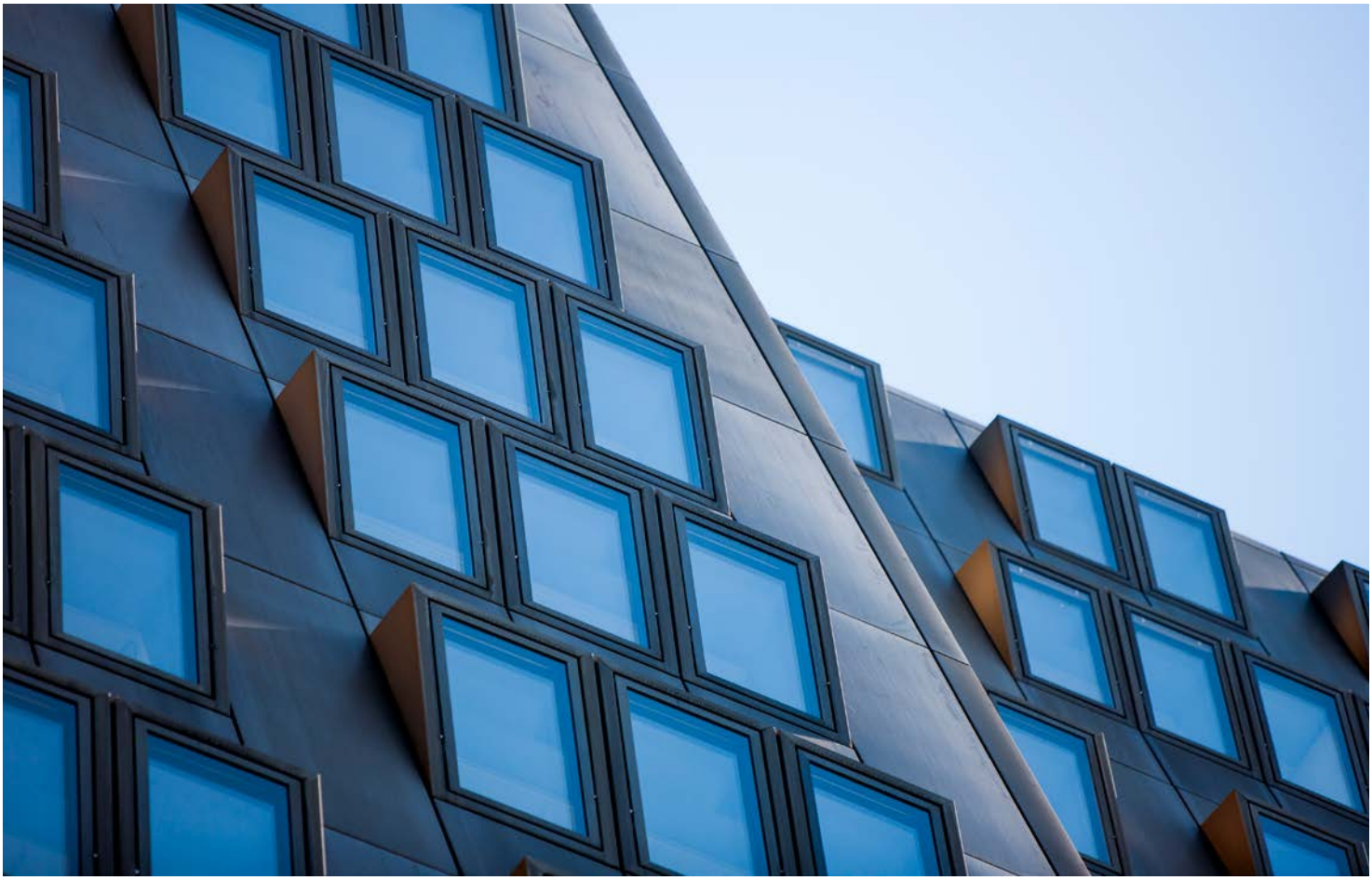
Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Prävention und Bekämpfung von Cyberkriminalität; Follow–up–Überprüfung

Reihe BUND 2024/18

Bericht des Rechnungshofes



III–1175 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 2024–0.419.946 (005.135)

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 Juni 2024

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

FOTOS
Cover, S. 5: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
BGBl.	Bundesgesetzblatt
BMI	Bundesministerium für Inneres
BMJ	Bundesministerium für Justiz
BMKÖS	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
bzw.	beziehungsweise
COVID	corona virus disease (Coronaviruskrankheit)
ERV	Elektronischer Rechtsverkehr
EUR	Euro
f(f).	folgend(e)
GmbH	Gesellschaft mit beschränkter Haftung
i.d.g.F.	in der geltenden Fassung
IHS	Institut für Höhere Studien
IKDA	Integrierte Kriminalpolizeiliche Datenanwendung
IKT	Informations– und Kommunikationstechnologie
IT	Informationstechnologie
Mio.	Million
Mrd.	Milliarde
PAD	zentrales Aktenverwaltungssystem Protokollieren, Anzeigen, Daten
rd.	rund
RH	Rechnungshof
RIVIT	Richtverwendungen für IT–Sonderverträge des Bundes
SeILE	Schaffung einer IKT–Lösung für besondere kriminalpolizeiliche Ermittlungen
StGB	Strafgesetzbuch
TZ	Textzahl
u.a.	unter anderem
z.B.	zum Beispiel

Durch die seit dem Vorbericht weiter gestiegene digitale Vernetzung sind alle gesellschaftlichen, staatlichen und wirtschaftlichen Bereiche von Cyberkriminalität betroffen. Die Kosten bzw. Schäden durch Cyberkriminalität steigen stetig. Eine Studie in Österreich kam im Jahr 2023 zu dem Ergebnis, dass alle befragten 903 Unternehmen bereits Opfer eines Cyber–Angriffs geworden sind. Bei jedem zehnten Unternehmen belief sich der finanzielle Schaden auf über 1 Mio. EUR. Die Zahl der als Cyberkriminalitäts–Delikte bezeichneten Fälle stieg in Österreich im Jahr 2022 im Vergleich zum Vorjahr um 30 % auf 60.195 angezeigte Delikte. Im Jahr 2023 erhöhte sich diese Zahl weiter auf 65.864.

Das Innenministerium bzw. das Bundeskriminalamt hatten die Organisation und die Zuständigkeiten sowie die Prozesse im Bereich der Bekämpfung von Cyberkriminalität seit dem Vorbericht noch nicht weiterentwickelt. Das Innenministerium stellte im September 2023 die – noch umzusetzende – Kriminaldienstreform 2.0 vor, deren Fokus auf dem Aufbau von spezialisierten Kompetenzen im Kriminaldienst vor allem in Bezug auf Cyberkriminalität lag. Für die Reorganisation ging das Innenministerium von einem Bedarf an 300 neuen Arbeitsplätzen im Bereich Prävention und Bekämpfung von Cyberkriminalität aus. Zum Recruiting dieser Arbeitsplätze gab es zur Zeit der Follow–up–Überprüfung noch keine konkreten Überlegungen.

Das Justizministerium setzte seit Beginn 2023 bei Staatsanwaltschaften sogenannte „Kompetenzstellen Cybercrime“ ein, die Ermittlungen bei Verfahren mit Bezug zu Cyberkriminalität unterstützten. Es bot in den Jahren 2020 bis 2023 mehr als 190 Bildungsveranstaltungen zu Cyberkriminalität an. Damit setzte es zwei der zentralen Empfehlungen aus dem Vorbericht um.

WIRKUNGSBEREICH

- Bundesministerium für Inneres
- Bundesministerium für Justiz

Prävention und Bekämpfung von Cyberkriminalität; Follow–up–Überprüfung

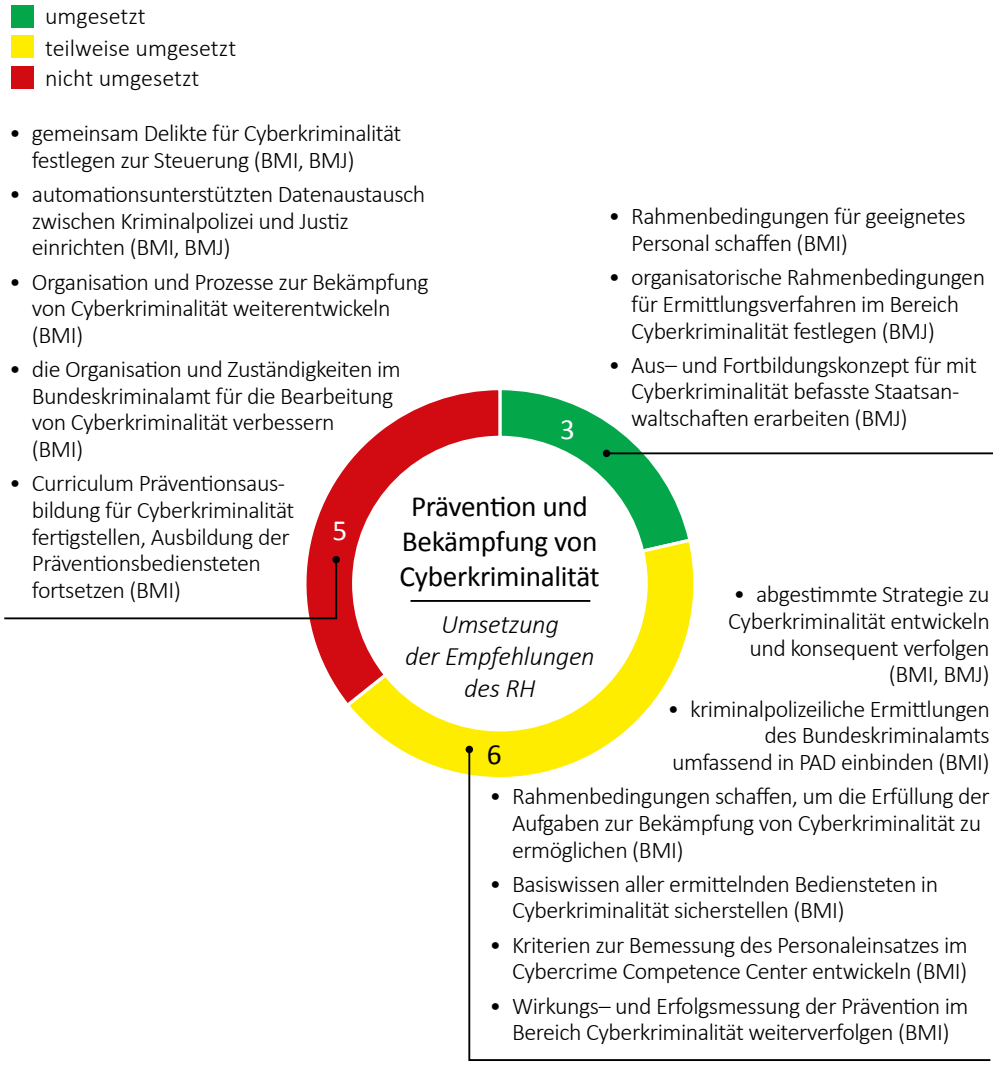
Prüfungsziel

Der RH überprüfte von August bis Oktober 2023 das Bundesministerium für Inneres, das Bundeskriminalamt sowie das Bundesministerium für Justiz, um den Stand der Umsetzung von Empfehlungen aus seinem Vorbericht „Prävention und Bekämpfung von Cyberkriminalität“, Reihe Bund 2021/23, zu beurteilen.

Kurzfassung

Das Bundesministerium für Inneres (in der Folge: **Innenministerium**) und das Bundesministerium für Justiz (in der Folge: **Justizministerium**) setzten von drei an sie gemeinsam gerichteten Empfehlungen, die der RH überprüfte, eine teilweise und zwei nicht um. Das Innenministerium setzte von weiteren fünf überprüften Empfehlungen eine zur Gänze, drei teilweise und eine nicht um, das Bundeskriminalamt setzte von vier überprüften Empfehlungen zwei teilweise und zwei nicht um. Das Justizministerium setzte die zwei überprüften Empfehlungen um. (TZ 16)

Abbildung 1: Umsetzungsstand ausgewählter Empfehlungen aus dem Vorbericht



Empfehlungen an mehrere Adressaten werden in dieser Abbildung nur einmal gezählt. In der Tabelle in TZ 16 hingegen einzeln nach Adressat.

Quelle und Darstellung: RH

Der RH fokussierte bei der nunmehrigen Follow–up–Überprüfung auf folgende Themen:

- Strategie (TZ 3),
- einheitliche Begriffsbestimmungen und Datenaustausch (TZ 4, TZ 5, TZ 6),
- Organisation und Personal, inklusive der Kriminaldienstreform 2.0 im Innenministerium (TZ 7, TZ 8, TZ 9, TZ 10, TZ 14),
- Aus– und Fortbildung (TZ 11, TZ 15) sowie
- Prävention (TZ 12, TZ 13).

Strategie

Das Innen– und das Justizministerium setzten die Empfehlung zu einer abgestimmten Strategie für den Bereich Cyberkriminalität teilweise um. Sie legten jeweils strategische Ziele zur Prävention und Bekämpfung von Cyberkriminalität fest und stimmten sich bei der Umsetzung ab. Die strategischen Ziele selbst hatten sie nicht abgestimmt. (TZ 3)

Begriffsbestimmungen und Datenaustausch

Für Cyberkriminalität bestanden – entgegen der Empfehlung des RH – weiterhin keine einheitlichen, zwischen Innen– und Justizministerium abgestimmten Begriffsbestimmungen. Zudem führten die Ministerien zu Organisationszwecken weitere Begriffsbestimmungen ein, die im jeweils anderen Ressort nicht zur Anwendung kamen. So verwendete z.B. nur das Innenministerium die Kategorie „Internetbetrug“, nicht aber das Justizministerium. Das erschwerte es, auf Basis vergleichbarer Zahlen wirksame Steuerungsmaßnahmen zu ergreifen. (TZ 4)

Das Innenministerium hatte die mit kriminalpolizeilichen Ermittlungen befassten Organisationseinheiten des Bundeskriminalamts an das zentrale Aktenverwaltungssystem Protokollieren, Anzeigen, Daten (**PAD**) angebunden. Es setzte die Empfehlung aber nur teilweise um, weil es den überwiegenden Anteil der Akten immer noch mit der Integrierten Kriminalpolizeilichen Datenanwendung (**IKDA**) führte. Daher blieb der vollständige automationsunterstützte Informations– und Aktenaustausch mit den nachgeordneten Polizeidienststellen sowie mit den Staatsanwaltschaften erschwert. (TZ 5)

Sichergestellte Daten übermittelte die Kriminalpolizei weiterhin über Datenträger an die Justiz. Nur für geringe Datenmengen, spezifische Datei–Formate oder mit individueller Berechtigung konnten Daten zwischen dem Innen– und Justizministerium ausgetauscht werden. Somit fehlten nach wie vor adäquate Zugriffsmöglichkeiten und Zugriffs– sowie Bearbeitungsdokumentationen für elektronische Beweismittel. Diese Empfehlung an die Ministerien war daher weiter offen. (TZ 6)

Organisation und Personal im Innenministerium

Das Innenministerium bzw. das Bundeskriminalamt hatten weder die Organisation – vor allem in dem auf die Bekämpfung von Cyberkriminalität spezialisierten Cybercrime Competence Center – noch die Zuständigkeiten und auch nicht die Prozesse zur Bekämpfung von Cyberkriminalität weiterentwickelt. Auch diese Empfehlung war daher noch offen. Das Innenministerium und das Bundeskriminalamt waren jedoch bestrebt, die Organisation des Cybercrime Competence Centers und damit auch die Zuständigkeiten an die veränderte Kriminalitätslandschaft anzupassen. So

lagen ein Personaleinsatzkonzept für die Weiterentwicklung des Cybercrime Competence Centers zu einer eigenen Abteilung und die entsprechende Geschäftseinteilung zur Abgrenzung der neuen Zuständigkeiten vor. Das Personaleinsatzkonzept für das Cybercrime Competence Center enthielt teilweise nachvollziehbare Mengengerüste als objektive Grundlage für die Bemessung des zukünftigen Personalbedarfs. Das Bundeskriminalamt hatte diese Empfehlung somit teilweise umgesetzt. (TZ 7, TZ 8)

Das Innenministerium entwickelte in einem gemeinsamen Projekt mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport neue „Richtverwendungen für IT–Sonderverträge des Bundes“, die mit Jänner 2022 in Kraft traten. Diese neuen Richtverwendungen schufen Rahmenbedingungen im Sinne eines modernen Personalmanagements. Sie könnten dazu beitragen, dass allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung steht. Im Ergebnis war die Empfehlung damit umgesetzt. Das Innenministerium hatte mit der Einrichtung der auf den neuen Richtverwendungen beruhenden Planstellen jedoch erst in der Zentralstelle begonnen. Für Personal, das für die Bekämpfung von Cyberkriminalität zuständig war, hatte das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport zur Zeit der Follow–up–Überprüfung noch keine derartigen Planstellen genehmigt. (TZ 9)

Reformmaßnahmen zu Cyberkriminalität

Die Empfehlung zu organisatorisch, personell und infrastrukturell geeigneten Rahmenbedingungen für eine zeit– und zweckmäßige Bekämpfung von Cyberkriminalität war teilweise umgesetzt: Am 1. September 2023 präsentierte der Innenminister die Ergebnisse des Projekts zur sogenannten „Kriminaldienstreform 2.0“. Der Fokus lag dabei auf der Stärkung und Straffung der flächendeckenden Ermittlungs– und Assistenzdienstleistungen bei gleichzeitigem Aufbau von spezialisierten Kompetenzen im Kriminaldienst und damit dem Ausbau der Handlungssicherheit in Bezug auf Cyberkriminalität. Darauf aufbauend sollten die Organisation und Ausbildung insbesondere in den Landeskriminalämtern (mit Ausnahme von Wien), den Bezirks– und Stadtpolizeikommanden und den Polizeiinspektionen angepasst werden. Im Rahmen der Reorganisation ging das Innenministerium von einem Bedarf an 300 neuen Arbeitsplätzen für die Prävention und Bekämpfung von Cyberkriminalität aus. Das Recruiting für diese Arbeitsplätze war zur Zeit der Follow–up–Überprüfung allerdings noch nicht festgelegt. Auch war das Landeskriminalamt Wien nicht Teil des Gesamtkonzepts zur Stärkung der Bekämpfung von Cyberkriminalität. (TZ 10)

Aus– und Fortbildung im Innenministerium

Das Innenministerium schulte IT– und Cyberkriminalitäts–Themen in Grundausbildungslehrgängen, in fachlichen Ausbildungen für den Kriminaldienst und in Fortbildungsveranstaltungen. Das Bundeskriminalamt passte zudem die Struktur des Kriminalistischen Leitfadens als Wissensplattform an, um Exekutivbedienstete mit Handlungsanleitungen, Checklisten und Videos gezielt zu Themen der Cyberkriminalität zu informieren. Insgesamt beurteilte der RH die Empfehlung aber als nur teilweise umgesetzt, weil die praktische Ausbildung weiterhin nur für Kriminalsachbearbeiterinnen und –sachbearbeiter vorgesehen war, nicht für allgemein eingeteilte Exekutivbedienstete. Dass im Rahmen der Kriminaldienstreform 2.0 geplant war, alle Exekutivbediensteten in noch einzurichtenden Cybercrime–Training–Centern der Landeskriminalämter praktisch zu Cyberkriminalitäts–Themen zu schulen, war daher positiv. (TZ 11)

Prävention im Innenministerium

Das Bundeskriminalamt erließ im Jahr 2023 eine neue Präventionsrichtlinie. Entgegen der Empfehlung des RH war aber das Curriculum mit fachlichen Standards und Inhalten für die Ausbildung der Präventionsbediensteten für Cyberkriminalität nicht fertiggestellt. Auch hatte das Bundeskriminalamt seit 2019 keine weiteren Ausbildungen für die Präventionsbediensteten im Bereich Cyberkriminalität angeboten bzw. abgehalten. (TZ 12)

Die Empfehlung, das Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität weiterzuverfolgen, die Ergebnisse zu verwerten und umzusetzen, setzte das Bundeskriminalamt teilweise um. Das Projekt war mit Dezember 2020 abgeschlossen. Allerdings waren das ursprüngliche Ziel nicht erreicht und die erzielten Ergebnisse nicht umgesetzt. Die Projektergebnisse dienten nicht wie geplant der Wirkungs– und Erfolgsmessung von Präventionsmaßnahmen oder deren praktischen Erprobung. (TZ 13)

Organisation der Staatsanwaltschaften in Ermittlungsverfahren zu Cyberkriminalität

Das Justizministerium startete Anfang 2023 einen bundesweiten, einjährigen Probebetrieb, mit dem es „Kompetenzstellen Cybercrime“ oder „Kontakt– und Verbindungsstellen“ bei Staatsanwaltschaften und der Zentralen Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption einrichtete. Diese Stellen unterstützten Staatsanwältinnen und Staatsanwälte bei Verfahren mit Cyberkriminalitäts–Bezug. Zur Vernetzung und zum Wissenstransfer veranstaltete das Justizministerium „Vernetzungstreffen Cybercrime“ auf zentraler Ebene und plante Gesprächsplattformen für operative Themen auf regionaler Ebene. Zudem stellte es

eine digitale Plattform zum Informationsaustausch (z.B. über aktuelle Phänomene) zwischen den Kompetenzstellen zur Verfügung. Zur Zeit der Follow–up–Überprüfung beabsichtigte das Justizministerium, den Probebetrieb um zwei Jahre zu verlängern. Mit diesen Maßnahmen setzte das Justizministerium die Empfehlung im Ergebnis um. (TZ 14)

Aus– und Fortbildung im Justizministerium

Auch die Empfehlung zur Aus– und Fortbildung der mit Cyberkriminalität befassten Bediensteten setzte das Justizministerium um. Es bot seit Jänner 2023 eine Basisausbildung Cybercrime für Bezirks– und Staatsanwältinnen bzw. –anwälte an, ab Oktober 2023 auch für Richterinnen und Richter. Für die Staatsanwältinnen und Staatsanwälte der Kompetenzstellen Cybercrime plante es einen Lehrgang. Es entsandte Vortragende zur Sicherheitsakademie des Innenministeriums, ließ Bedienstete des Innenministeriums an eigenen Schulungen teilnehmen und nahm zur Abstimmung des Ausbildungsangebots an Austauschtreffen der Akademien des Bundes, an Qualitätszirkeln und Vernetzungstreffen teil. (TZ 15)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

EMPFEHLUNGEN

Bundesministerium für Inneres; Bundesministerium für Justiz

- Eine zwischen dem Bundesministerium für Inneres und dem Bundesministerium für Justiz abgestimmte Strategie für den Bereich Cyberkriminalität wäre zu entwickeln und konsequent zu verfolgen. (TZ 3)

- Gemeinsam wären jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können. (TZ 4)

Bundesministerium für Inneres

- Angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen wären – insbesondere im Bereich des Landeskriminalamts Wien – zu schaffen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Ministeriums die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen. (TZ 10)

- Die Schritte zur Stärkung der Prävention und Bekämpfung von Cyberkriminalität wären sukzessive umzusetzen, die gesetzten Maßnahmen regelmäßig auf ihre Zielsetzung zu überprüfen und gegebenenfalls anzupassen sowie strategische Überlegungen zum Personalbedarf miteinfließen zu lassen. (TZ 10)

Bundesministerium für Justiz

- Der Probebetrieb der Kompetenzstellen Cybercrime bei den Staatsanwaltschaften wäre fortzusetzen, zu evaluieren und nach allfällig notwendigen Anpassungen in den Regelbetrieb überzuleiten. (TZ 14)

Zahlen und Fakten zur Prüfung

Prävention und Bekämpfung von Cyberkriminalität; Follow–up–Überprüfung					
ausgewählte Rechtsgrundlagen	Übereinkommen über Computerkriminalität vom 23. November 2001 (in Kraft getreten gemäß BGBl. III 140/2012 mit 1. Oktober 2012) Strafgesetzbuch (StGB), BGBl. 60/1974 i.d.g.F.				
Datenbasis	2019	2020	2021	2022	Veränderung 2019 bis 2022
	Anzahl				in %
polizeiliche Anzeigen Cyberkriminalität insgesamt (Fälle)[1]	28.434	35.915	46.179	60.195	112
davon					
im engeren Sinn	*7.622*	*12.914*	*15.484*	*22.376*	*194*
im weiteren Sinn	*20.812*	*23.001*	*30.695*	*37.819*	*82*
davon					
Internetbetrug	*16.831*	*18.780*	*22.440*	*27.629*	*64*
sonstige Kriminalität im Internet[1]	*3.981*	*4.221*	*8.255*	*10.190*	*156*
Erledigungen der Staatsanwaltschaften (personenbezogen) zu Cyberkriminalität im engeren Sinn[2]	2.526	12.319	14.129	19.265	663
davon					
durch Anklage	*699*	*1.218*	*1.289*	*1.550*	*122*
durch Diversion	*114*	*287*	*307*	*348*	*205*
durch Einstellung	*1.171*	*3.018*	*3.620*	*4.038*	*245*
durch Abbrechung	*542*	*7.796*	*8.913*	*13.329*	*2.359*
Erledigungen der Gerichte zu Cyberkriminalität im engeren Sinn	518	567	563	767	48
davon					
Verurteilung	*383*	*437*	*387*	*544*	*42*
Diversion	*85*	*68*	*81*	*116*	*36*
Freispruch	*50*	*62*	*95*	*107*	*114*
Personal zur Bekämpfung von Cyberkriminalität im Innenministerium	2020	2021	2022	2023	Veränderung 2020 bis 2023
	in Vollzeitäquivalenten zum 1. Jänner				in %
Landeskriminalämter (Aufgabenbereich IT–Beweissicherung)	85	88	102	109	28
Bundeskriminalamt (Cybercrime Competence Center)	63,5	67	80	89	40

[1] Das Innenministerium führte die Unterkategorie „sonstige Kriminalität im Internet“ ab dem Jahr 2021 nicht mehr. Der RH ordnete der Kategorie entsprechend der Systematik des Innenministeriums bis zum Jahr 2020 die Restmenge der Straftatbestände aus der Cyberkriminalität im weiteren Sinn zu. Seit 2020 erfasste das Innenministerium § 297 StGB (Verleumdung) nicht mehr als Cyberkriminalität im weiteren Sinn. Um die Jahreswerte vergleichen zu können, wurden diese Anzeigen auch für das Jahr 2019 nicht betrachtet.

[2] Daten zu Cyberkriminalität im weiteren Sinn waren bei der Justiz nicht auswertbar. Das Justizministerium konsolidierte im Jahr 2020 die Kategorien der Erledigungen bei den Staatsanwaltschaften. Der RH wendete diese Zählweise auch für die Werte für 2019 an, daher weichen diese vom Vorbericht ab.

Quellen: BMI; BMJ; Zusammenstellung: RH

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von August bis Oktober 2023 beim Bundesministerium für Inneres (in der Folge: **Innenministerium**), beim Bundeskriminalamt sowie beim Bundesministerium für Justiz (in der Folge: **Justizministerium**) die Umsetzung ausgewählter Empfehlungen, die er bei der Gebarungsüberprüfung zum Thema „Prävention und Bekämpfung von Cyberkriminalität“ abgegeben hatte. Der in der Reihe Bund 2021/23 veröffentlichte Bericht wird in der Folge als Vorbericht bezeichnet. Gespräche fanden auch mit dem Landeskriminalamt Wien und der Staatsanwaltschaft Wien statt.

Der überprüfte Zeitraum der gegenständlichen Follow–up–Überprüfung umfasste im Wesentlichen die Jahre 2020 bis 2023. Soweit möglich und erforderlich, berücksichtigte der RH auch frühere Zeiträume bzw. aktuelle Entwicklungen.

Im Jahr 2015 beschlossen die 193 Mitgliedstaaten der Vereinten Nationen die sogenannte Agenda 2030 („Transformation unserer Welt: die Agenda 2030 für nachhaltige Entwicklung“). Österreich verpflichtete sich, bis zum Jahr 2030 auf die Umsetzung der 17 nachhaltigen Entwicklungsziele („Sustainable Development Goals“ (**SDG**)), die durch 169 Unterziele konkretisiert waren, hinzuarbeiten. Wesentlich für die in der Follow–up–Überprüfung behandelten Themen ist das SDG 16, das die Rechtsstaatlichkeit auf nationaler und internationaler Ebene fördern und den gleichberechtigten Zugang aller zur Justiz gewährleisten soll.

(2) Zur Verstärkung der Wirkung seiner Empfehlungen hatte der RH deren Umsetzungsstand im Jahr 2022 beim Innen– und Justizministerium nachgefragt. Das Ergebnis dieses Nachfrageverfahrens findet sich auf der Website des RH (www.rechnungshof.gv.at).

Der RH weist in diesem Zusammenhang auf seine geübte Vorgehensweise und standardisierte Berichtsstruktur für Follow–up–Überprüfungen hin. Diese haben vor allem das Ziel, den Umsetzungsstand von ausgewählten Empfehlungen des Vorberichts unter Berücksichtigung der Angaben aus dem Nachfrageverfahren zu beurteilen und die Einstufung in „umgesetzt“, „teilweise umgesetzt“, „zugesagt“ und „nicht umgesetzt“ zu begründen.

(3) Zu dem im Jänner 2024 übermittelten Prüfungsergebnis nahmen das Innenministerium und das Justizministerium im April 2024 Stellung. Der RH erstattete seine Gegenäußerungen im Juni 2024.

Allgemeines

2 (1) Seit dem Vorbericht ist die Nutzung von digitalen Geräten, der Informationstechnologie (**IT**) und des Internets weiter gestiegen. Ende Dezember 2021 gab es weltweit über 5 Mrd. Internetzugänge.[1] In Österreich hatten 95 % der Haushalte im Jahr 2021 einen Internetzugang, der überwiegende Anteil (81 %) der Personen verwendete das Internet jeden Tag oder fast jeden Tag; 88 % der Unternehmen waren mit einer Website im Internet vertreten.[2]

(2) Durch die digitale Vernetzung von Systemen mittels Computer, Smartphone, Tablet oder Laptop sind letztlich alle gesellschaftlichen, staatlichen und wirtschaftlichen Bereiche von Cyberkriminalität betroffen. Die Kosten bzw. Schäden durch Cyberkriminalität steigen – auch bedingt durch die COVID–19–Pandemie – stetig. Laut dem Cyberwarfare Report[3] lag im Jahr 2021 der Schaden durch Cyberkriminalität weltweit bei sechs Billionen US–Dollar, für das Jahr 2024 wurden Schäden in Höhe von zehn Billionen US–Dollar prognostiziert. Eine Studie in Österreich kam im Jahr 2023 zu dem Ergebnis, dass alle befragten 903 Unternehmen bereits Opfer eines Cyber–Angriffs geworden waren. Bei jedem zehnten Unternehmen belief sich der finanzielle Schaden auf über 1 Mio. EUR. Knapp die Hälfte der Befragten erlitt einen Schaden von bis zu 100.000 EUR.[4] Laut einer Untersuchung in Deutschland aus 2022 beläuft sich der Schaden durch digitale Angriffe auf 203 Mrd. EUR pro Jahr.[5]

(3) Die Schäden durch Cyberkriminalität liegen aber nicht nur im finanziellen, sondern auch im immateriellen Bereich. Dies betrifft die Verletzung der sexuellen Selbstbestimmung (z.B. Sextortion[6], Cybergrooming[7]), das Recht auf Schutz der Ehre und der persönlichen Integrität sowie den öffentlichen Frieden (z.B. Cybermobbing, Verleumdung, Verhetzung, „Hass im Netz“).

1 siehe Internet World Stats, World internet usage and population statistics; https://www.internetworldstats.com/stats.htm (abgerufen am 26. April 2024)

2 Statistik Austria, IKT–Einsatz von Haushalten 2021, IKT–Einsatz in Unternehmen 2022

3 im Jahr 2021 herausgegeben von Cybersecurity Ventures

4 KPMG „Cybersecurity in Österreich 2023“

5 Untersuchung des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien auf Basis einer Selbsteinschätzung von betroffenen Unternehmen

6 Sextortion umfasst kriminelle Handlungen im Internet, bei denen Nutzerinnen und Nutzer dazu aufgefordert werden, Intimfotos zu verschicken oder in Videochats nackt zu posieren. Das Material wird heimlich aufgezeichnet, um damit von den Opfern Geld zu erpressen, indem diesen mit der Veröffentlichung der Aufnahmen gedroht wird.

7 Dabei sprechen Erwachsene im Internet (z.B. in sozialen Netzwerken oder Online–Spielen) Kinder und Jugendliche gezielt an und erschleichen sich deren Vertrauen, um sexuellen Kontakt bis hin zum sexuellen Missbrauch anzubahnen.

(4) Im Jahr 2022 stieg in Österreich die Zahl der als Cyberkriminalitäts–Delikte bezeichneten Fälle im Vergleich zum Vorjahr um 30 % auf 60.195 angezeigte Delikte. Die Strafverfolgungsbehörden – Polizei, Staatsanwaltschaften und Gerichte – sind bei der Bekämpfung von Cyberkriminalität weiterhin mit wachsenden Anforderungen im Hinblick auf die Anwendung des Cyber–Strafrechts, die digitale Beweismittelsicherung sowie die Ermittlungstaktik und Kriminaltechnik (Forensik) konfrontiert. Die Aufklärungsquote sank von 2010 bis 2022 von 55,3 % auf 33,9 %.

Vor diesem Hintergrund erstellte das Innenministerium ein Konzept zu einer Kriminaldienstreform 2.0 (in der Folge: **Kriminaldienstreform**), das es im September 2023 präsentierte. Der Fokus lag dabei auf der Bekämpfung von Cyberkriminalität. Einzelne Aspekte dieses Konzepts bezog der RH im Rahmen dieser Follow–up–Überprüfung ein (TZ 6 und TZ 10).

Strategie

3.1 (1) Der RH hatte dem Innen– und dem Justizministerium – auch im Hinblick auf das Regierungsprogramm 2020–2024 – in seinem Vorbericht (TZ 9 und TZ 10) empfohlen, eine zwischen dem Innen– und dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität zu entwickeln und konsequent zu verfolgen.

(2) (a) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass seine mehrjährige Ressortstrategie für den Cyber–Bereich einen entwicklungsoffenen Ansatz verfolge, womit die stetige Anpassung der Ermittlungsmethoden und Präventionsmaßnahmen bei der Vorbeugung und Bekämpfung der Cyberkriminalität gewährleistet werden solle. So hätten in Abstimmung mit dem Justizministerium bereits gemeinsame Maßnahmen im Zuge der Einrichtung der Zentralen Anfragestelle Social Media und Online Service Provider im Bundeskriminalamt sowie im Rahmen des Projekts zur Schaffung einer IKT–Lösung für besondere kriminalpolizeiliche Ermittlungen erfolgreich umgesetzt werden können. Zusätzlich seien im Bereich „Recht“ der Kriminaldienstreform gesetzliche Bestimmungen des materiellen und formellen Cyber–Strafrechts evaluiert worden. Konkrete Vorschläge zur Abänderung von Gesetzesbestimmungen, die während des Reformprozesses formuliert worden seien, befänden sich aktuell in Abstimmung mit den zuständigen Stakeholdern.

(b) Das Justizministerium hatte im Nachfrageverfahren ergänzend mitgeteilt, dass im Juni 2022 bei der Konferenz der Behördenleitungen mit dem Innenministerium und der Leitungstagung der Staatsanwaltschaften das Modell der Cybercrime–Kompetenzstellen bei den Staatsanwaltschaften, die Entwicklung von Maßnahmen zur Erkennung von Massenphänomenen und Konnexitäten durch strukturierte Vernet-

zung mit den Polizeibehörden sowie die Aus– und Fortbildung diskutiert worden seien.

(3) (a) Der RH stellte nunmehr fest, dass es zur Zeit der Follow–up–Überprüfung weiterhin keine zwischen dem Innen– und dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität gab.

(b) Es bestanden u.a. folgende nationalen Strategien mit Bezug zu Cyberkriminalität, an denen sich das Innenministerium und das Bundeskriminalamt für die eigene strategische Ausrichtung orientierten:

- die Strategie der Bundesregierung für künstliche Intelligenz[8],
- die Österreichische Strategie für Cybersicherheit 2021[9],
- der Aktionsplan Deepfake[10] sowie
- das Österreichische Programm zum Schutz kritischer Infrastrukturen[11].

Das Innenministerium definierte im Jahr 2021 eine Ressortstrategie[12] mit Schwerpunkten. Sie sah u.a. vor, die Cybersicherheit zu erhöhen sowie Kriminalität kompetent und vernetzt vorzubeugen und sie zu bekämpfen. Dazu sollten beispielsweise Personal und Organisation weiterentwickelt, kriminalpolizeiliche Fähigkeiten ausgebaut, Ermittlungen digitalisiert sowie neue Technologien genutzt werden.

Das Bundeskriminalamt setzte in der Kriminalstrategie 2023 für die Jahre 2023 und 2024 einen Schwerpunkt auf Cyberkriminalität. Es verzichtete – wie auch das Innenministerium – auf eine spezifische Strategie für den Bereich Cyberkriminalität, da eine solche seiner Ansicht nach keinen Mehrwert biete und flexible Reaktionen auf technische Entwicklungen hemmen könnte. Zur Umsetzung des Schwerpunkts Cyberkriminalität verwies es auf

- geplante organisatorische Anpassungen im Rahmen der Kriminaldienstreform (TZ 7 ff.),
- geplante Cybercrime–Training–Center (TZ 11),

[8] abrufbar unter https://www.bmk.gv.at/dam/jcr:93f327ac-b69c-4ac7-a9aa-30eee51cc221/AIM_AT_2030_UA.pdf (abgerufen am 26. April 2024)

[9] abrufbar unter https://www.bundeskanzleramt.gv.at/dam/jcr:79eff5f6-20ed-4cf7-8d71-a6a02e4c49b3/Cyberstrategie2021.pdf (abgerufen am 26. April 2024)

[10] Der Begriff „Deepfake“ wird als Überbegriff für Formen der Manipulation durch Video, Audio oder beides verwendet. Der Aktionsplan sah u.a. vor, diesbezügliche Strafverfolgungskompetenzen zu evaluieren und gegebenenfalls auszubauen. Abrufbar unter https://www.bmi.gv.at/bmi_documents/2779.pdf (abgerufen am 26. April 2024).

[11] abrufbar unter https://www.bundeskanzleramt.gv.at/dam/jcr:bb6a1a41-eb1d-4552-96da-9b460bbc5c0b/%C3%96sterreichisches%20Programm%20zum%20Schutz%20kritischer%20Infrastruktren%20(APCIP).pdf (abgerufen am 29. April 2024)

[12] abrufbar unter https://www.bmi.gv.at/107/files/BMI_Ressortstrategie_RZ_WEB_kleiner_V20211221.pdf (abgerufen am 29. April 2024)

- die Zusammenarbeit mit dem Justizministerium über sogenannte Cybercrime–Gesprächsplattformen in den Bundesländern, mit denen operativen Problemen begegnet werden sollte (TZ 14),
- technische Neuerungen (TZ 6) sowie
- Präventionstätigkeiten (TZ 12 f.).

(c) Das Justizministerium zielte strategisch darauf ab, durch regelmäßige zentrale und dezentrale Vernetzung die Phänomene im Bereich Cyberkriminalität rasch zu erkennen und Best Practices zu etablieren. Zu diesem Zweck organisierte es interne Vernetzungstreffen für die Kompetenzstellen Cybercrime und die Kontakt– und Verbindungsstellen (TZ 14) sowie interministerielle Qualitätszirkel mit Verantwortlichen der Zentralstelle des Innenministeriums, des Bundeskriminalamts und der Direktion für Staatsschutz und Nachrichtendienst. In diesen Formaten behandelte es aktuelle Entwicklungen und berücksichtigte diese bei der eigenen Planung in Bezug auf die Bekämpfung von Cyberkriminalität.

3.2 Das Innenministerium und das Justizministerium setzten die Empfehlung teilweise um. Eine zwischen dem Innen– und dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität lag weiterhin nicht vor. Der RH würdigte positiv, dass die Ministerien jeweils für ihr Ressort strategische Ziele zur Prävention und Bekämpfung von Cyberkriminalität festlegten und sich bei der Umsetzung abstimmten. Er hielt jedoch kritisch fest, dass sie die strategischen Ziele selbst nicht abgestimmt hatten. Das Innenministerium orientierte sich für seine Ziele zu Cyberkriminalität an weiteren themenspezifischen Strategien, wodurch ein gesamtheitlicher Ansatz erkennbar war. Das Justizministerium nutzte interne und interministerielle Vernetzungstreffen, um Ansätze für die eigene strategische Planung zu erhalten.

Der RH hielt daher seine Empfehlung an das Innenministerium und das Justizministerium aufrecht, eine zwischen den Ministerien abgestimmte Strategie für den Bereich Cyberkriminalität zu entwickeln und konsequent zu verfolgen.

3.3 (1) Das Innenministerium teilte in seiner Stellungnahme mit, dass basierend auf dem Regierungsprogramm, der Ressortstrategie, der Österreichischen Strategie für Cybersicherheit 2021 und der Cybercrime–Präventionsstrategie auch in der Strategie des Bundeskriminalamts 2023 der Bekämpfung und Prävention von Internetkriminalität ein Schwerpunkt gewidmet sei. Es habe sich bewusst gegen weitere Strategien im Bereich Cyberkriminalität entschieden, da ein Mehr nicht unbedingt eine Verbesserung mit sich bringe. Weitere – speziell ressortübergreifende, zusätzliche – Strategien würden Dynamik und Flexibilität hemmen, welche gerade in diesem Kriminalitätsspektrum in Bezug auf den raschen technologischen Fortschritt erforderlich seien. Der Fokus liege darauf, Maßnahmen umzusetzen.

(2) Das Justizministerium wiederholte in seiner Stellungnahme die (vom RH in TZ 3 und TZ 14 dargestellten) gesetzten Maßnahmen und verwies darüber hinaus auf den sogenannten Arbeitsschwerpunkt „Massenphänomene – Konnexitäten“. Im Rahmen der Qualitätszirkel und Vernetzungstreffen sowie des Austauschs im Cybercrime–Netzwerk seien als vordringliche Problemstellungen in Verfahren zu Cyberkriminalität die effiziente Bearbeitung und Verfolgung von Massenphänomenen und die Vermeidung von Kompetenzkonflikten im staatsanwaltschaftlichen Bereich identifiziert worden. Um eine diesbezüglich abgestimmte Lösung zu erarbeiten, sei auf interministerieller Ebene ein regelmäßiger Austausch mit dem Innenministerium und dem Bundeskriminalamt initiiert worden.

3.4 Der RH beurteilte die vom Innen– und Justizministerium gesetzten einzelnen Maßnahmen und die entsprechende Abstimmung positiv. Er hielt jedoch fest, dass die strategischen Ziele selbst weiterhin nicht abgestimmt waren.

Der Mehrwert einer abgestimmten Strategie liegt aus Sicht des RH etwa darin, bei gemeinsamen Ermittlungsschwerpunkten oder im Bereich der Aus– und Fortbildung potenzielle Schnittstellenprobleme im kriminalpolizeilichen und im staatsanwaltschaftlichen Ermittlungsverfahren zu verringern. Gerade die große Dynamik im Bereich Cyberkriminalität und die in immer kürzeren Abständen auftretenden neuen Phänomene machen eine darauf abgestimmte Strategie notwendig. Weiters könnten nach Ansicht des RH durch eine gemeinsame strategische Positionierung Effizienzverluste vermieden werden, z.B. durch wirksame Steuerungsmaßnahmen (TZ 4) oder standardisierte automationsunterstützte Prozesse (TZ 6). Er bekräftigte daher seine Empfehlung.

Begriffsbestimmungen und Datenaustausch

Einheitliche Begriffsbestimmungen

4.1 (1) Der RH hatte im Vorbericht festgestellt, dass für den Bereich Cyberkriminalität keine einheitlichen, zwischen Innen– und Justizministerium abgestimmten Begriffsbestimmungen bestanden, wodurch eine abgestimmte Vorgehensweise zur Bekämpfung von Cyberkriminalität erschwert wurde.

Er hatte dem Innenministerium und dem Justizministerium daher empfohlen (TZ 4), gemeinsam jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können.

(2) (a) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass die Delikte durch die Trennung in Cyberkriminalität im engeren Sinn sowie Cyberkriminalität im weiteren Sinn ausreichend klar festgelegt seien. Auch der Internetbetrug, der im Jahr 2021 beinahe die Hälfte aller Anzeigen im Bereich Internetkriminalität ausgemacht habe, werde getrennt ausgewiesen (§§ 146 bis 148 Strafgesetzbuch (**StGB**)[13] bei Örtlichkeit „Internet“). Die Zuordnung einzelner Deliktfelder habe das Innenministerium laufend aktualisiert; beispielsweise habe es § 107c StGB (Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems) und § 119 StGB (Verletzung des Telekommunikationsgeheimnisses) bereits 2017 der Cyberkriminalität im engeren Sinn zugerechnet. Der Cyberkriminalität im weiteren Sinn habe es in weiterer Folge einschlägige Paragrafen des Suchtmittelgesetzes[14], des Verbotsgesetzes 1947[15] und des StGB zugeordnet, um Entwicklungen und Trends statistisch abbilden zu können.

(b) Laut Mitteilung des Justizministeriums im Nachfrageverfahren sei im Dezember 2021 das „Bundesgesetz, mit dem das Strafgesetzbuch und das Zahlungsdienstegesetz 2018 zur Umsetzung der Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln geändert werden“[16] in Kraft getreten. Dieses sehe u.a. Erweiterungen in den Tatbeständen, die Einführung von Qualifikationen bzw. die Anhebung der Strafdrohungen bei mehreren Cyberkriminalitäts–relevanten Delikten vor. Aufgrund der hohen Praxisrelevanz sei insbesondere auf den neuen § 148a Abs. 3 StGB (Betrügerischer Datenverarbeitungsmissbrauch) hinzuweisen. Das Justizministerium habe auch einen Einführungserlass zur Information der Gerichte und Staatsanwaltschaften herausgegeben.

13 BGBl. I 60/1974 i.d.g.F.

14 BGBl. I 112/1997 i.d.g.F.

15 BGBl. 13/1945 i.d.g.F.

16 BGBl. I 201/2021

Zur Zeit des Nachfrageverfahrens fänden politische Verhandlungen über weitere Änderungen bei den Cyberkriminalitäts–Delikten statt. Insbesondere werde eine Anhebung von Strafdrohungen bzw. die Einführung von Qualifikationen diskutiert, um dem – mit Fortschreiten der Digitalisierung und der immer stärkeren Verlagerung der Angelegenheiten des täglichen Lebens ins Internet verbundenen – erhöhten sozialen Störwert der Taten Rechnung zu tragen.

Im internationalen Kontext und im österreichischen strafrechtlichen Schrifttum sei die Unterscheidung zwischen Cyberkriminalität im engeren Sinn und im weiteren Sinn etabliert. Eine exakte Abgrenzung bzw. Festlegung von bestimmten Delikten, die der Cyberkriminalität zuzuordnen seien, sei nicht möglich, weil diese Delikte auch ohne Verwendung von Informations– und Kommunikationstechnik (**IKT**) als Tatmittel begangen werden könnten.

(3) (a) Der RH stellte nunmehr fest, dass das Innenministerium und das Justizministerium nicht gemeinsam jene Delikte festgelegt hatten, die unter den Begriff Cyberkriminalität zu subsumieren sind.

(b) Das Innenministerium führte die Definitionen von Cyberkriminalität im engeren und im weiteren Sinn wie bisher weiter. Zur organisatorischen Abgrenzung im Rahmen der Kriminaldienstreform (TZ 10) plante es eine weitere Unterteilung in „Cyberkriminalität der hybriden Form“. Diese sollte Offline–Delikte mit Angriffen auf IKT umfassen.

Das Innenministerium ordnete in der Polizeilichen Kriminalstatistik einzelne Straftatbestände den Kategorien Cyberkriminalität im engeren Sinn und Cyberkriminalität im weiteren Sinn zu. Letztere unterteilte es weiter in die Unterkategorien Internetbetrug sowie – bis zum Jahr 2021 – sonstige Kriminalität im Internet. Dazu legte es jährlich fest, welche kriminologischen Sachverhalte von welcher Kategorie erfasst wurden.

Im Detail ordnete es die Straftaten im Jahr 2022 nach verwirklichten Delikten wie in folgender Tabelle dargestellt zu:

Tabelle 1: Kategorisierung von Cyberkriminalität in der Polizeilichen Kriminalstatistik

Kategorie		Straftatbestand (Delikt)
Cyberkriminalität im engeren Sinn		• Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 107c StGB) • Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB) • Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) • Missbräuchliches Abfangen von Daten (§ 119a StGB) • Datenbeschädigung (§ 126a StGB) • Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) • Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB) • Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB) • Datenfälschung (§ 225a StGB)
Cyberkriminalität im weiteren Sinn	Internet-betrug	• Betrug, Schwerer Betrug und Gewerbsmäßiger Betrug (§§ 146 bis 148 StGB)
		• Nötigung und Schwere Nötigung (§§ 105 f. StGB) • Gefährliche Drohung (§ 107 StGB) • Beharrliche Verfolgung (§ 107a StGB) • Beleidigung (§ 115 StGB) • Erpressung und Schwere Erpressung (§§ 144 f. StGB) • Pornographische Darstellung Minderjähriger (§ 207a StGB) • Sexueller Missbrauch von Jugendlichen (§ 207b StGB) • Anbahnung von Sexualkontakten zu Unmündigen (§ 208a StGB) • Sexuelle Belästigung und öffentliche geschlechtliche Handlungen (§ 218 StGB) • Fälschung von Urkunden bzw. besonders geschützter Urkunden (§§ 223 f. StGB) • Mittelbare unrichtige Beurkundung oder Beglaubigung (§ 228 StGB) • Urkundenunterdrückung (§ 229 StGB) • Gebrauch fremder Ausweise (§ 231 StGB) • Geldfälschung bzw. Fälschung unbarer Zahlungsmittel (§§ 232 und 241a StGB) • Verhetzung (§ 283 StGB) • Straftaten nach §§ 27 ff. Suchtmittelgesetz sowie nach § 4 Neue–Psychoaktive–Substanzen–Gesetz (BGBl. I 146/2011 i.d.g.F.) • Straftaten nach §§ 3a ff. Verbotsgesetz 1947

StGB = Strafgesetzbuch Quelle: BMI

(c) Das Justizministerium hielt seine Mitteilung im Nachfrageverfahren aufrecht und definierte Cyberkriminalität im engeren und weiteren Sinn wie zur Zeit des Vorberichts. Es ordnete dem Begriff Cyberkriminalität im engeren Sinn dieselben Delikte zu wie das Innenministerium. Es grenzte Delikte der Cyberkriminalität im weiteren Sinn nicht genauer ab und konnte daher mit den eigenen Systemen keine steuerungsrelevanten Aspekte, z.B. zu Internetbetrug, auswerten. Um die Aufgaben der „Kompetenzstellen Cybercrime“ (TZ 14) abzugrenzen, definierte das Justizministerium zusätzlich „Cyberkriminalitäts–Agenden“. Davon waren Cyberkriminalität im engeren und weiteren Sinn sowie Fragen zur Beweisführung im Zusammenhang mit IKT umfasst.

4.2 Das Innenministerium und das Justizministerium setzten die Empfehlung nicht um. Sie behielten ihre Begriffsbestimmungen zu Cyberkriminalität bei oder führten zu Organisationszwecken weitere Begriffsbestimmungen ein, die im jeweils anderen Ressort nicht zur Anwendung kamen. So verwendete nur das Innenministerium die Kategorie „Internetbetrug“, nicht aber das Justizministerium. Zudem konnte das Justizministerium keine steuerungsrelevanten Aspekte zu Cyberkriminalität im weiteren Sinn auswerten. Aus Sicht des RH würden einheitliche, zwischen Innen– und Justizministerium abgestimmte Begriffsbestimmungen und vergleichbare Statistiken zu Cyberkriminalität im weiteren Sinn eine abgestimmte Vorgehensweise zur Bekämpfung der Cyberkriminalität fördern.

Der RH wiederholte daher seine Empfehlung an das Innenministerium und das Justizministerium, gemeinsam jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können.

4.3 (1) Das Innenministerium wiederholte in seiner Stellungnahme seine Angaben aus dem Nachfrageverfahren 2022, u.a. dass die Delikte durch die Trennung in Cyberkriminalität im engeren Sinn sowie Cyberkriminalität im weiteren Sinn ausreichend klar festgelegt seien. Zusätzlich teilte es mit, dass es sich regelmäßig mit dem Justizministerium austausche.

(2) Das Justizministerium verwies in seiner Stellungnahme zu den Delikten bezüglich Cyberkriminalität im engeren Sinn auf eine gesetzliche Änderung im Jahr 2023[17], bei der die Strafdrohungen dieser Delikte erhöht worden seien, aber weitere inhaltliche Änderungen nicht angezeigt schienen.

Cyberkriminalitäts–Delikte im weiteren Sinn seien Straftaten, bei denen IKT als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt würden. Neben den zahlenmäßig weit überwiegenden Betrugsdelikten kämen theoretisch auch alle anderen gerichtlich strafbaren Delikte in Betracht. Eine exakte Abgrenzung bzw. Festlegung von bestimmten Delikten, die der Cyberkriminalität zuzuordnen seien, sei daher nicht möglich.

Aus legistischer Sicht sei es wichtig, dass die Straftatbestände technologieneutral formuliert seien. Die generell–abstrakte Umschreibung der Strafbarkeitsvoraussetzungen mache die Tatbestände offen für Entwicklungen, die zum Zeitpunkt ihrer Erlassung noch nicht voraussehbar seien – gerade auch im technologischen Bereich. Die vom Innenministerium als Cyberkriminalität im weiteren Sinn definierten Straftaten könnten daher nur einen Ausschnitt deliktischen Verhaltens und verletzter Rechtsgüter ohne Anspruch auf Vollständigkeit abbilden.

[17] Bundesgesetz, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden, BGBl. I 99/2023

Soweit die Festlegung von Cyberkriminalitäts–Delikten im weiteren Sinn dazu dienen solle, wirksame Steuerungsmaßnahmen zu ergreifen, sei auch zu bedenken, dass auf Ebene der Staatsanwaltschaften infolge des Prinzips der Amtswegigkeit im Strafverfahren nicht Ermittlungsverfahren in bestimmten Kriminalitätsbereichen schwerpunktmäßig durchgeführt werden könnten.

Eine Festlegung von Cyberkriminalitäts–Delikten im engeren Sinn und deren Auswertung seien technisch möglich.

Auf der Definition von Cyberkriminalitäts–Agenden aufbauend würden die Kompetenzstellen Cybercrime diesbezüglich in beratender Funktion beigezogen. Die Befassung der Kompetenzstellen erfolge im elektronischen Akt bei Fragen von Staatsanwältinnen und –anwälten oder Bezirksanwältinnen und –anwälten in einzelnen Verfahren bzw. zur Information mit Tasks. Auch dies könne statistisch ausgewertet werden.

4.4 Der RH anerkannte den regelmäßigen institutionalisierten Austausch zwischen Innen– und Justizministerium. Er hielt allerdings kritisch fest, dass wegen der unterschiedlichen Begriffsbestimmungen bzw. fehlenden Abstimmung Zahlen zu polizeilichen Anzeigen und justiziellen Erledigungen im Bereich der Cyberkriminalität im weiteren Sinn weiterhin nicht vergleichbar waren. Das erschwerte nach Ansicht des RH zuverlässige Aussagen zu aktuellen Entwicklungen und damit auch Steuerungsmaßnahmen.

Datenaustausch
Bundeskriminalamt und nachgeordnete Dienststellen

5.1 (1) Der RH hatte im Vorbericht festgestellt, dass das Bundeskriminalamt nicht umfassend in das bei allen anderen kriminalpolizeilichen Dienststellen verwendete zentrale Aktenverwaltungssystem Protokollieren, Anzeigen, Daten (**PAD**) eingebunden war. Dies erschwerte den internen Informationsaustausch im Rahmen übergreifender Ermittlungen, z.B. bei Cyberkriminalitäts–Massendelikten oder bei Sonderkommissionen. Weiters war dadurch eine automationsunterstützte Berichterstattung bzw. Aktenübermittlung an die Staatsanwaltschaft mittels Elektronischem Rechtsverkehr (**ERV**) nicht möglich.

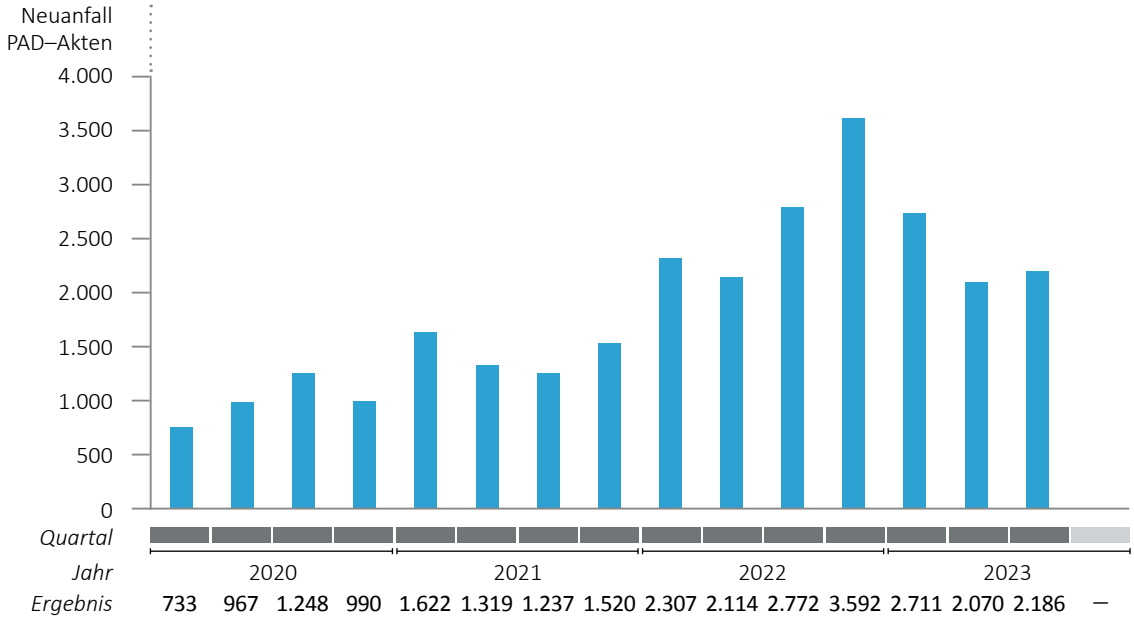
Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 39) daher empfohlen, alle mit kriminalpolizeilichen Ermittlungen befassten Organisationseinheiten des Bundeskriminalamts umfassend in die zentrale Applikation PAD einzubinden, um einen vollständig automationsunterstützten Informations– und Aktenaustausch mit den nachgeordneten Polizeidienststellen wie auch mit den Staatsanwaltschaften sicherzustellen.

(2) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass das Projekt zur Umstellung von der Integrierten Kriminalpolizeilichen Datenanwendung (**IKDA**) auf PAD wie geplant umgesetzt werde. Aufgrund der Komplexität des Projekts und der Ressourcenknappheit im umsetzenden Unternehmen werde jedoch die gesamte Umsetzung bis 2024 dauern.

(3) Der RH stellte nunmehr fest, dass zur Zeit der Follow–up–Überprüfung alle operativ tätigen Abteilungen des Bundeskriminalamts an PAD angebunden waren. Damit war es möglich, PAD–Akten zwischen dem Bundeskriminalamt und nachgeordneten Dienststellen zu übertragen. Im Bundeskriminalamt wurden in den Jahren 2020 bis 2023 (September) insgesamt 27.388 Akten in PAD neu verarbeitet.

Die Anzahl der neu angefallenen PAD–Akten entwickelte sich folgendermaßen:

Abbildung 2: Neu angefallene PAD–Akten im Bundeskriminalamt in den Jahren 2020 bis 2023 (Stand September 2023)



Quelle: Bundeskriminalamt; Darstellung: RH

Insgesamt stieg der Neuanfall von Akten in PAD; zwischen den Quartalen schwankte der Neuanfall stark.

Das Bundeskriminalamt hielt die Applikation IKDA weiterhin in Betrieb, da seiner Ansicht nach wesentliche Module (z.B. zu Import–Prozessen) noch nicht in PAD integriert waren. Den Organisationseinheiten war freigestellt, welche Applikation sie nutzten. Das Bundeskriminalamt bereitete die Aktenführung in IKDA statistisch nicht auf. Nach seiner Schätzung würden jährlich 115.000 IKDA–Akte erzeugt. Ein wesentlicher Teil davon betreffe automatisierte Prozesse, z.B. täglich bis zu 2.000 Meldungen der internationalen kriminalpolizeilichen Organisation Interpol.

Das Bundeskriminalamt konnte PAD–Akten bzw. Berichte dazu automationsunterstützt über den ERV an die Staatsanwaltschaften übermitteln. IKDA–Akten bzw. Berichte dazu übermittelte es über E–Mail oder Fax. Ein Projekt, um IKDA durch PAD abzulösen, startete im August 2021 und sollte plangemäß Ende 2024 abgeschlossen werden. Zur Zeit der Follow–up–Überprüfung (September 2023) war das Projekt zu geschätzt 28 % umgesetzt und wurden Projekt–Meilensteine bis Ende 2025 geplant.

5.2 Das Innenministerium setzte die Empfehlung teilweise um. Es hatte mit kriminalpolizeilichen Ermittlungen befasste Organisationseinheiten des Bundeskriminalamts an PAD angebunden. Jedoch führte es den überwiegenden Teil der Akten weiterhin mit IKDA. Der RH kritisierte, dass den Bediensteten freigestellt war, welche Applikation sie nutzten. Dies konnte zu Doppelgleisigkeiten führen und der automationsunterstützte Informationsaustausch blieb weiterhin erschwert. Der RH hielt zudem kritisch fest, dass das Innenministerium das Projekt zur Ablöse von IKDA durch PAD nach mehr als der Hälfte der geplanten Projektlaufzeit lediglich zu 28 % umgesetzt hatte.

Der RH hielt daher seine Empfehlung an das Innenministerium aufrecht, alle mit kriminalpolizeilichen Ermittlungen befassten Organisationseinheiten des Bundeskriminalamts umfassend in die zentrale Applikation PAD einzubinden, um Doppelgleisigkeiten zu vermeiden, die Praktikabilität sicherzustellen und einen vollständig automationsunterstützten Informations– bzw. Aktenaustausch mit den nachgeordneten Polizeidienststellen wie auch mit den Staatsanwaltschaften sicherzustellen.

5.3 Laut Stellungnahme des Innenministeriums werde das Projekt wie geplant umgesetzt, wobei aufgrund der Komplexität die gesamte Umsetzung bis 2025 dauern werde.

Datenaustausch Kriminalpolizei und Justiz

6.1 (1) Der RH hatte im Vorbericht festgestellt, dass das Innen– und das Justizministerium die 2016 im Rahmen der gemeinsamen Arbeitsgruppe IKT–Großstrafverfahren erarbeiteten Vorschläge für eine interministerielle Datenaustauschplattform samt umfassender Archivierungslösung für elektronische Beweismittel nicht weiterverfolgt hatten. Damit gab es weiterhin keinen automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten sowie keine zuverlässige und vollständige Dokumentation sämtlicher Bearbeitungsschritte. Die lückenlose Dokumentation der Bearbeitung elektronischer Beweismittel war unerlässlich, um volle Beweiskraft zu sichern.

Der RH hatte dem Innenministerium und dem Justizministerium daher empfohlen (TZ 47), ein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, vollständiger Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel einzurichten.

(2) (a) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass der Aufbau einer derartigen Infrastruktur bereits seit längerem im Gange sei. Seit 2021 sei das Projekt unter dem Namen „Schaffung einer IKT–Lösung für besondere kriminalpolizeiliche Ermittlungen“ (in der Folge: **SeILE**) unter Einbindung des Justizministeriums neu organisiert und damit entsprechend der Vorgabe forciert worden. Zur Zeit des Nachfrageverfahrens sei eine IKT–Lösung für die kriminalpolizeilichen Dienste für besondere Ermittlungs– und Analyse–Tätigkeiten, forensische Auswertungen und Aufbereitung der IT–Beweismittel für Gerichte bzw. Staatsanwaltschaften mit Schnittstellen zur Übermittlung erarbeitet worden.

(b) Das Justizministerium hatte im Nachfrageverfahren mitgeteilt, dass im Rahmen des Projekts zum Ausbau des Einsatzes von IT–Expertinnen und –Experten im Strafverfahren die IT–seitigen Voraussetzungen für die „Inhouse–Speicherung“ und Analyse von Beweismitteln geschaffen worden seien. Darüber hinaus sei ein System zum Datenaustausch (sogenannte Justiz–Box) umgesetzt worden, wobei noch an der Integration in die polizeilichen Informationssysteme gearbeitet werde.

(3) (a) Der RH stellte nunmehr fest, dass das Innen– und das Justizministerium zur Zeit der Follow–up–Überprüfung weiterhin kein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, vollständiger Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel eingerichtet hatten.

(b) Bis zum Jahr 2021 tauschten Kriminalpolizei und Justiz Berichte und Beilagen mit einer Größe von bis zu 50 Megabyte aktgebunden über den ERV aus. Größere Datenmengen übermittelte die Kriminalpolizei nach individueller Zugriffsberechtigung über „Cryptshare“, die Datenaustausch–Plattform des Innenministeriums, oder über physische Datenträger. Nach Vereinbarung behielt die Kriminalpolizei Daten für Staatsanwaltschaften auf (z.B. um weitere Anfragen zu beantworten).

Parallel dazu startete das Innenministerium im Jahr 2021 das Projekt SeILE. Themen des Projekts waren u.a., elektronische Beweismittel zu sichten, auszuwerten, abzuspeichern und mit der Justiz auszutauschen. Dafür waren standardisierte Zugänge mit Bindung an den PAD–Akt, eine durchgängige Dokumentation sowie eine zentrale Datensicherung vorgesehen. Zum Datenaustausch zwischen Kriminalpolizei und Justiz bestanden konzeptionelle Vorarbeiten.

Nach Angaben des Innenministeriums war der Erfolg von SeILE auch eine wesentliche Voraussetzung für die Umsetzung der Kriminaldienstreform (TZ 10). Zur Zeit der Follow–up–Überprüfung hatte es Sachressourcen für das Projekt SeILE angeschafft. Aufgrund fehlender Personalressourcen bei einem Leistungspartner waren zeitkritische und wichtige Programmentwicklungen (z.B. das Detailkonzept zu finali-

sieren) nur eingeschränkt möglich. Ab 2024 sollte ein Prototyp getestet werden, im Juni 2025 sollte das Projekt nach Umsetzung in allen Landeskriminalämtern beendet werden.

(c) Das Justizministerium betrieb seit November 2020 über die Bundesrechenzentrum GmbH die sogenannte Justiz–Box. Damit war es möglich, über den ERV Audio–, Video– und PDF[18]–Dateien mit bis zu vier Gigabyte zu übermitteln, nicht aber weitere Datei–Arten. Der Zugriff auf Daten in der Justiz–Box war über referenzierende ERV–Akten möglich und wurde lückenlos dokumentiert, wobei Benutzerinnen bzw. Benutzer nur über eine Leseberechtigung verfügten.

Im Justizministerium bestand keine Archivlösung für sichergestellte Daten. Das Justizministerium wartete zur Zeit der Follow–up–Überprüfung eine abschließende rechtliche Beurteilung ab, ob und inwiefern es eine derartige zweck– und rechtmäßige Archivierungslösung bereitzustellen hatte.

6.2 Das Innenministerium und das Justizministerium setzten die Empfehlung nicht um. Sichergestellte Daten übermittelte die Kriminalpolizei weiterhin über Datenträger oder über separate Systeme mit individueller Berechtigung. Nur geringe Datenmengen oder spezifische Datei–Formate konnten über standardisierte automationsunterstützte Prozesse zwischen dem Innen– und dem Justizministerium ausgetauscht werden, nicht aber größere Datenmengen anderer Datei–Formate. Der RH kritisierte, dass damit weiterhin adäquate Zugriffsmöglichkeiten und Zugriffs– sowie Bearbeitungsdokumentationen für elektronische Beweismittel fehlten. Zum entsprechenden Projekt des Innenministeriums bestanden zur Zeit der Follow–up–Überprüfung lediglich konzeptionelle Vorarbeiten zum Datenaustausch mit der Justiz. Diese sollten Anfang 2024 mit einem Prototypen getestet werden. Das Justizministerium machte die wesentliche Frage der Datenübernahme inklusive Archivierung von einer abschließenden rechtlichen Beurteilung abhängig.

Der RH wiederholte daher seine Empfehlung an das Innenministerium und das Justizministerium, ein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, vollständiger Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel einzurichten.

Weiters hielt der RH kritisch fest, dass für das Projekt SeILE des Innenministeriums zeitkritische und wichtige Programmentwicklungen (z.B. das Detailkonzept zu finalisieren) zur Zeit der Follow–up–Überprüfung aufgrund fehlender Personalressourcen bei einem Leistungspartner nur eingeschränkt möglich waren.

[18] Portable Document Format

Er empfahl daher dem Innenministerium, das Projekt zur Schaffung einer IKT–Lösung für besondere kriminalpolizeiliche Ermittlungen zu konkretisieren und sukzessive umzusetzen, um damit eine stabile IKT–Grundlage für die Kriminaldienstreform 2.0 gewährleisten zu können.

6.3 (1) Das Innenministerium wiederholte in seiner Stellungnahme seine Angaben aus dem Nachfrageverfahren im Jahr 2022, u.a. dass der Aufbau einer derartigen IKT–Infrastruktur bereits seit Längerem im Gange sei.

(2) Das Justizministerium verwies in seiner Stellungnahme auf ein Erkenntnis des Verfassungsgerichtshofes vom Dezember 2023. Aufgrund des Erkenntnisses sei der Rechtsrahmen einer grundlegenden und den Anforderungen des Verfassungsgerichtshofes entsprechenden Neuregelung zu unterziehen. Nachdem Auswirkungen auf die aktuelle Praxis zur Übergabe elektronischer Beweismittel zu erwarten seien, sei vor Schaffung entsprechender technischer Lösungen der Gesetzwerdungsprozess abzuwarten.

Innenministerium

Organisation und Personal

Organisation des Cybercrime Competence Centers

7.1 (1) Laut den Feststellungen des Vorberichts hatte das Innenministerium im Bundeskriminalamt mit dem Cybercrime Competence Center eine auf die Bekämpfung von Cyberkriminalität spezialisierte Organisationseinheit – als Büro in der Abteilung Kriminalpolizeiliche Assistenzdienste – eingerichtet. Das Cybercrime Competence Center hatte mit dem Grundkonzept zur Bekämpfung von Cyberkriminalität auch umfassende Vorschläge zu Organisation, Personal sowie Aus– und Fortbildung sowohl im Bundeskriminalamt selbst als auch bundesweit vorgelegt. Obwohl im Bereich Cyberkriminalität die Fallzahlen stark stiegen, hatte das Innenministerium nicht adäquat reagiert und war die Umsetzung des Grundkonzepts noch offen.

In den vergangenen Jahren verlagerten sich klassische Delikte zusehends in den Cyber–Raum und entwickelte sich die Bekämpfung von Cyberkriminalität zu einer Querschnittsmaterie. Die ermittlungszuständigen Abteilungen des Bundeskriminalamts waren damit wiederholt mit Fällen konfrontiert, die nicht nur klassische, sondern immer öfter auch technische Ermittlungsansätze und Expertise erforderten. Allerdings waren in derartigen Fällen die Zuständigkeitsregelungen für effiziente und zielführende Ermittlungen nicht immer zweckmäßig bzw. ausreichend und konnten zu Abgrenzungsproblemen führen.

Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 26) daher empfohlen, die Organisation – vor allem im Bereich des Cybercrime Competence Centers – und die Prozesse im Bereich der Bekämpfung von Cyberkriminalität auf Basis bestehender Konzepte weiterzuentwickeln bzw. der veränderten Kriminalitätslandschaft anzupassen.

Weiters hatte er dem Bundeskriminalamt empfohlen (TZ 27), die Organisation und Zuständigkeiten für die Bearbeitung von Cyberkriminalität im Hinblick auf die gestiegene Bedeutung technischer Ermittlungsansätze und Expertise unter Berücksichtigung eines Ausbildungs– und Personalkonzepts zu verbessern und eindeutig festzulegen.

(2) (a) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, die Empfehlung aufgegriffen zu haben. Neben einer entsprechenden Personaldotierung plane es auch organisatorische Anpassungen im Bereich des Cybercrime Competence Centers, um speziell auf neue Technologien oder Modi Operandi eingehen zu können. So habe das Innenministerium beispielsweise die Zentrale Anfragestelle Social Media und Online Service Provider im Bundeskriminalamt mit dem Ziel

geschaffen, Anfragen künftig bundesweit zentral abzuwickeln, Abläufe zu optimieren und Ermittlungen gezielter zu unterstützen.

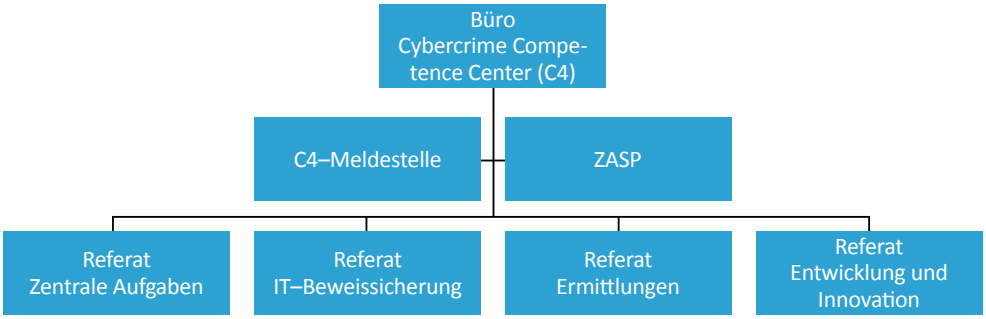
(b) Das Bundeskriminalamt hatte im Nachfrageverfahren ebenfalls mitgeteilt, die Empfehlung aufgegriffen zu haben und bei der geplanten Umsetzung eines umfassenden Personal– und Einsatzkonzepts zu berücksichtigen. In diesem Zusammenhang erarbeite es auch eine klare Aufgabenfestlegung und –abgrenzung zwischen der Abteilung Wirtschaftskriminalität und dem Cybercrime Competence Center.

(3) Der RH stellte nunmehr fest, dass sich die Zuständigkeiten und die Organisation des Cybercrime Competence Centers sowie der nachgeordneten Dienststellen (zu diesen siehe TZ 10) seit dem Vorbericht nicht geändert hatten. Das Cybercrime Competence Center war weiterhin ein Büro in der Abteilung Kriminalpolizeiliche Assistenzdienste im Bundeskriminalamt, das Grundkonzept zur Bekämpfung von Cyberkriminalität war nicht umgesetzt.

Mit Beginn des Jahres 2022 richtete das Innenministerium in Kooperation mit dem Justizministerium – entsprechend der Intention des RH in seinem Vorbericht (TZ 31)[19] – eine zentrale Anfragestelle für Social Media und Online Service Provider im Cybercrime Competence Center ein.[20]

Die Struktur des Cybercrime Competence Centers stellte sich zur Zeit der Follow–up–Überprüfung wie folgt dar:

Abbildung 3: Organigramm Cybercrime Competence Center als Büro



ZASP = Zentrale Abfragestelle für Social Media und Online Service Provider

Quelle: Bundeskriminalamt; Darstellung: RH

[19] Der RH hatte dem Innenministerium empfohlen, im Einvernehmen mit dem Justizministerium eine zentrale Koordinierungsstelle für Auskunftsverlangen an Betreiber sozialer Medien und Internetprovider zeitnah einzurichten und mit ausreichenden Personalressourcen und Know–how auszustatten.

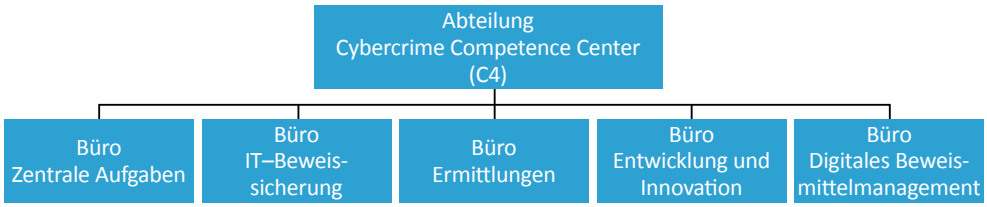
[20] Der Probebetrieb dazu startete im September 2020.

Das Bundeskriminalamt evaluierte im Jahr 2021 den Personaleinsatz im Bundeskriminalamt inklusive Cybercrime Competence Center (TZ 8). In der Folge übermittelte es ein Personaleinsatzkonzept zur Einrichtung des Cybercrime Competence Centers als eigene Abteilung im Bundeskriminalamt an das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (**BMKÖS**) zur Abstimmung. Dieses Konzept enthielt umfassende Vorschläge zu Organisation, Personal sowie Aus– und Fortbildung.

Erste Gespräche zu diesem Personaleinsatzkonzept führte das Bundeskriminalamt mit dem BMKÖS im Sommer 2023. Aufgrund dieser Gespräche überarbeitete das Bundeskriminalamt das Personaleinsatzkonzept für das Cybercrime Competence Center als Abteilung – es legte ihm als Ergebnis der Evaluierung einen Bedarf an 128 Planstellen zugrunde[21] – und übermittelte es erneut an das BMKÖS. Zur Zeit der Follow–up–Überprüfung (Oktober 2023) ging das Bundeskriminalamt von einer zeitnahen Genehmigung der Planstellen bzw. Umsetzung des Konzepts aus.

Das Bundeskriminalamt plante die Einrichtung des Cybercrime Competence Centers entsprechend der nachstehenden Abbildung:

Abbildung 4: Organigramm Cybercrime Competence Center als Abteilung im Bundeskriminalamt



Quelle: Bundeskriminalamt; Darstellung: RH

Demnach sollte die Abteilung Cybercrime Competence Center fünf Büros mit Referaten und Fachbereichen umfassen. Das Cybercrime Competence Center als Abteilung sollte die zentrale Assistenzdienststelle in allen Belangen von Cyberkriminalität werden, insbesondere bei der Sicherung elektronischer Beweismittel, der Leitung und Koordinierung von Sicherheitsbehörden und –dienststellen, den Ermittlungen sowie der internationalen polizeilichen Kooperation in Angelegenheiten der Cyberkriminalität.

[21] Zum 1. Jänner 2023 verfügte das Cybercrime Competence Center über 63 Planstellen.

Die nachstehende Tabelle zeigt wesentliche Aufgaben der fünf Büros der Abteilung Cybercrime Competence Center:

Tabelle 2: Aufgaben der geplanten Büros im Cybercrime Competence Center

Bezeichnung Büro	wesentliche Aufgaben (Auswahl)
Zentrale Aufgaben	Das Büro Zentrale Aufgaben sollte eine koordinierende Funktion übernehmen und für die Bereitstellung aller notwendigen Ressourcen für den Dienstbetrieb in der Abteilung verantwortlich sein. Es sollte nationale und internationale Cyberkriminalitäts–Projekte koordinieren, steuern und durchführen sowie bundesweit Aus– und Fortbildungsmaßnahmen im Bereich Cyberkriminalität koordinieren.
IT–Beweissicherung	Das Büro IT–Beweissicherung sollte die nationale und internationale Ansprechstelle bei der Datenanalyse, –sicherung, –aufbereitung und –auswertung von elektronischen Beweismitteln werden. Es sollte u.a. die Analyse, Datensicherung und –aufbereitung von elektronischen Beweismitteln, wie Audio–, Video– und IT–Medien, mobilen Endgeräten sowie elektronischen Geräten im Zusammenhang mit Fahrzeugen und Internet of Things, leiten, koordinieren und durchführen.
Ermittlungen	Das Büro Ermittlungen sollte die operative Ermittlungseinheit im Cybercrime Competence Center und das Gegenstück zu internationalen zentralen Cyberkriminalitäts–Ermittlungsdienststellen werden. Es sollte komplexe oder umfangreiche Ermittlungsverfahren mit Bezug zu Cyberkriminalität im engeren Sinn und hybriden Formen koordinieren, leiten und übernehmen sowie kooperative Fallbearbeitung und Ermittlungsunterstützung bieten.
Entwicklung und Innovation	Das Büro Entwicklung und Innovation sollte in cyberrelevanten Gebieten wissenschaftlich arbeiten und forschen. Es sollte Phänomene im Bereich der IT–Kommunikation, insbesondere im Internet, erforschen und bewerten sowie eine IT–spezifische Wissensdatenbank aufbauen und betreiben. Außerdem sollte es Ermittlungen und Forensik bei der Fallbearbeitung wissenschaftlich unterstützen sowie komplexe und aufwändige Ermittlungstätigkeiten analysieren.
Digitales Beweismittelmanagement	Das Büro Digitales Beweismittelmanagement sollte ein modernes Fallmanagement für technisch komplexe Kriminalfälle ermöglichen. Es sollte fallspezifisch angepasste digitale Arbeitsumgebungen für Ermittlerinnen bzw. Ermittler und Forensikerinnen bzw. Forensiker bereitstellen, um Anforderungen abzudecken, die durch klassische IT–Lösungen nicht mehr gewährleistet werden können. Außerdem sollte es als Schnittstelle zwischen Forensik, Ermittlungen, Technik und der Justiz fungieren.

Quelle: Bundeskriminalamt

Gleichzeitig mit der Überarbeitung des Personaleinsatzkonzepts erstellte das Bundeskriminalamt den Entwurf für eine neue Geschäftseinteilung. Mit dieser sollten die Zuständigkeiten des Cybercrime Competence Centers neu geregelt und in der Folge auch eine klare Aufgabenfestlegung und –abgrenzung zur Abteilung Wirtschaftskriminalität hergestellt werden.

7.2 Das Innenministerium und das Bundeskriminalamt setzten die Empfehlungen nicht um. Weder hatten sie die Organisation – vor allem des Cybercrime Competence Centers – und die Prozesse im Bereich der Bekämpfung von Cyberkriminalität weiterentwickelt noch die Organisation und Zuständigkeiten für die Bearbeitung von Cyberkriminalität im Hinblick auf die gestiegene Bedeutung technischer Ermittlungsansätze und Expertise verbessert und eindeutig festgelegt.

Der RH anerkannte jedoch, dass das Innenministerium und das Bundeskriminalamt weiterhin bestrebt waren, die Organisation des Cybercrime Competence Centers und damit auch die Zuständigkeiten weiterzuentwickeln und an die veränderte Kriminalitätslandschaft anzupassen. So lagen ein Personaleinsatzkonzept für die Aufwertung des Cybercrime Competence Centers zu einer eigenen Abteilung sowie die entsprechende Geschäftseinteilung zur Abgrenzung der neuen Zuständigkeiten bereits vor und das Bundeskriminalamt ging zur Zeit der Follow–up–Überprüfung von einer zeitnahen Genehmigung durch das BMKÖS aus.

Der RH empfahl dem Innenministerium weiterhin, die Organisation – vor allem im Bereich des Cybercrime Competence Centers – und die Prozesse im Bereich der Bekämpfung von Cyberkriminalität auf Basis bestehender Konzepte weiterzuentwickeln bzw. der veränderten Kriminalitätslandschaft anzupassen.

Weiters empfahl er dem Bundeskriminalamt, die Änderung der Organisation und der Zuständigkeiten für die Bearbeitung von Cyberkriminalität im Hinblick auf die gestiegene Bedeutung technischer Ermittlungsansätze und Expertise unter Berücksichtigung des bereits erstellten Personalkonzepts und in Abstimmung mit dem BMKÖS zeitnah umzusetzen.

7.3 Das Innenministerium wiederholte in seiner Stellungnahme seine Angaben aus dem Nachfrageverfahren im Jahr 2022; demnach habe es die Empfehlung aufgegriffen und plane neben einer entsprechenden Personaldotierung auch organisatorische Anpassungen im Bereich des Cybercrime Competence Centers, um speziell auf neue Technologien oder Modi Operandi eingehen zu können.

Darüber hinaus wies es darauf hin, dass seit Jänner 2022 ein Neubewertungsantrag im BMKÖS liege, der die Grundlage für eine Reorganisation auf Basis bestehender Konzepte bilde.

Auch werde im Rahmen der Kriminaldienstreform die Bekämpfung von Cyberkriminalität auf Landesebene durch strukturelle Maßnahmen unterstützt. Die Ergebnisse der Bewertungsverhandlungen zur Kriminaldienstreform würden abgewartet und danach umgesetzt.

Bemessung Personaleinsatz

8.1 (1) Der RH hatte dem Bundeskriminalamt in seinem Vorbericht (TZ 28) empfohlen, Kriterien zur Bemessung des Personaleinsatzes im Cybercrime Competence Center – unter Bedachtnahme auch auf zukünftige Aufgaben und Organisationsstrukturen – zu entwickeln, die Annahmen zu dokumentieren und laufend zu evaluieren. Dies vor dem Hintergrund, dass zur Zeit des Vorberichts nur bedingt feststellbar war, welcher Personalstand im Cybercrime Competence Center angemessen war.

(2) Das Bundeskriminalamt hatte im Nachfrageverfahren mitgeteilt, dass das Cybercrime Competence Center auf evidenzbasierte Erfahrungswerte zurückgreife. Dabei prüfe das Bundeskriminalamt laufend, ob die tatsächlichen Entwicklungen den getroffenen Annahmen entsprächen, um erforderlichenfalls Änderungen in der Personalplanung vornehmen zu können.

(3) Der RH stellte nunmehr – wie auch in TZ 7 ausgeführt – fest, dass das Bundeskriminalamt im Jahr 2021 den Personaleinsatz evaluierte und für das Cybercrime Competence Center ein Personaleinsatzkonzept erstellte.

Die Begründung für den Personalbedarf von 128 Planstellen bzw. die neuen Bewertungen der Bediensteten der Abteilung Cybercrime Competence Center enthielten neben den Arbeitsplatzbeschreibungen beispielsweise Angaben zu Arbeitsanfall und Fallzahlen, zu zukünftigen Aufgaben und technischen Entwicklungen, zur vorhandenen Ausrüstung oder zur Anzahl zu schulender Bediensteter des Innenministeriums. Die vom Bundeskriminalamt im Nachfrageverfahren angesprochenen evidenzbasierten Erfahrungswerte waren im Personaleinsatzkonzept nicht dokumentiert.

8.2 Das Bundeskriminalamt setzte die Empfehlung teilweise um. Das zur Zeit der Follow–up–Überprüfung vorliegende Personaleinsatzkonzept für das Cybercrime Competence Center enthielt zum Teil nachvollziehbare Mengengerüste als objektive Grundlage für die Bestimmung des zukünftigen Personalbedarfs. Das Bundeskriminalamt hatte aber keine Kriterien zur Bemessung des Personaleinsatzes bzw. evidenzbasierte Erfahrungswerte entwickelt.

Der RH empfahl daher dem Bundeskriminalamt weiterhin, Kriterien zur Bemessung des Personaleinsatzes im Cybercrime Competence Center – unter Bedachtnahme auch auf zukünftige Aufgaben und Organisationsstrukturen – zu entwickeln, die Annahmen zu dokumentieren und laufend zu evaluieren.

8.3 Das Innenministerium wiederholte in seiner Stellungnahme die Angaben des Bundeskriminalamts aus dem Nachfrageverfahren im Jahr 2022, u.a. dass das Cybercrime Competence Center auf evidenzbasierte Erfahrungswerte zurückgreife.

8.4 Der RH wies neuerlich darauf hin, dass evidenzbasierte Erfahrungswerte als Grundlage für das Personaleinsatzkonzept nicht dokumentiert und somit nicht nachvollziehbar waren. Ebenso fehlten weiterhin Kriterien zur Bemessung des Personaleinsatzes. Der RH hielt seine Empfehlung daher aufrecht.

Personalrekrutierung

9.1 (1) Der RH hatte im Vorbericht festgestellt, dass die Personalrekrutierung im Bereich Cyberkriminalität eine große Herausforderung darstellte – auch aufgrund der Rahmenbedingungen, z.B. formelle Kriterien abseits der fachlichen Eignung, Gehaltsschema des öffentlichen Dienstes, Planstellenbewertungen, langwierige Aufnahmeprozesse, mangelnde Möglichkeiten für Quereinsteigende.

Er hatte dem Innenministerium in seinem Vorbericht (TZ 30) daher empfohlen, in Zusammenarbeit mit dem BMKÖS Rahmenbedingungen im Sinne eines modernen Personalmanagements (Personalrekrutierung, –entwicklung und –bindung) zu schaffen, die es ermöglichen, dass allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung steht.

(2) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass die Notwendigkeit evident sei, entsprechende Rahmenbedingungen im Sinne eines modernen Personalmanagements zu schaffen, um das Innenministerium als attraktiven Arbeitgeber auch für technische oder IT–Berufe zu positionieren. Das Innenministerium sei an einem interministeriell ausgelegten Projekt des BMKÖS beteiligt. Mit dem Projekt sollten – zur gezielteren Ausrichtung auf die Anforderungen des Marktes – neue Richtlinien geschaffen werden für die ADV–Arbeitsplätze[22] sowie die damit verbundene Modernisierung der zur Auswahl stehenden IT–Arbeitsplätze.

Zur Erschließung des Marktes für geeignete Bewerberinnen und Bewerber arbeite das Innenministerium auf der Ebene der strategischen Personalentwicklung an einem Maßnahmenbündel. Dieses ziele u.a. auf Kooperationen mit universitären Einrichtungen sowie technisch ausgerichteten Schulen ab und schaffe über die Bewertung der betreffenden Arbeitsplätze hinaus attraktive Rahmenbedingungen für die Rekrutierung und Bindung.

(3) (a) Der RH stellte nunmehr fest, dass sich das Innenministerium ab 2020 an einem Projekt des BMKÖS zur Schaffung neuer Richtlinien für IT–Arbeitsplätze beteiligte. Projektziele waren insbesondere, den Bund als Arbeitgeber im IT–Bereich attraktiver zu machen, eine bessere Bezahlung zu gewährleisten, die Ausschreibungen ansprechender zu gestalten und den Ausschreibungsprozess zu beschleunigen.

[22] **ADV** = automationsunterstützte Datenverarbeitung; Sondervertragsschema

Als Ergebnis verlautbarte das BMKÖS im Jänner 2022 neue „Richtverwendungen für IT–Sonderverträge des Bundes“ (**RIVIT**). Um RIVIT–Arbeitsplätze ausschreiben und nach dem vorgesehenen Besoldungsschema entlohnen zu können, waren diese vorab dem BMKÖS zur Bewertung vorzulegen. Eine darüber hinausgehende Befassung des BMKÖS war nicht mehr vorgesehen. Die zugrunde liegenden Arbeitsplatzbeschreibungen konnten als Basis für Ausschreibungstexte herangezogen werden.

Das Innenministerium nutzte eine Reorganisation der Zentralstelle im Juli 2022 – bei dieser richtete es die Direktion Digitale Services in der Sektion IV (IT und Services) ein –, um im dafür notwendigen Personaleinsatzkonzept die entsprechenden RIVIT–Rollen festzulegen. Bestehende Bedienstete konnten auf Wunsch in das neue Bewertungsschema wechseln. Zusätzliches Personal suchte das Innenministerium bereits mit neuen Ausschreibungstexten. Nach Angaben des Innenministeriums konnten seit Beginn der Suche über 70 Planstellen neu besetzt werden und hatte sich der Rücklauf an Bewerbungen erhöht. Zusätzlich setzte die Sektion IV eigene Bedienstete für die Personalrekrutierung und –entwicklung im IKT–Bereich ein.

Nachdem das neue Planstellenkonzept des Cybercrime Competence Centers vom BMKÖS zur Zeit der Follow–up–Überprüfung noch nicht genehmigt war (TZ 7), hatte das Bundeskriminalamt noch keine Erfahrungen mit Ausschreibungen nach den neuen Richtverwendungen.

(b) Um technisch versiertes Personal ansprechen zu können, hielten Bedienstete des Cybercrime Competence Centers (Recruiting–)Vorträge an Höheren technischen Lehranstalten oder Universitäten. Das Innenministerium und das Bundeskriminalamt schlossen im Jahr 2023 eine Kooperation mit dem Bundesministerium für Bildung, Wissenschaft und Forschung bzw. den österreichischen Handelsakademien ab. Inhalt der Kooperation war die Einrichtung eines Schulzweiges mit dem Titel „Management (Cyber) Security“, in dem das Thema Cyber verstärkt behandelt werden sollte. Begleitend dazu plante das Innenministerium in Zusammenarbeit mit den Landespolizeidirektionen, an den Standorten der Handelsakademien gezielte Recruiting–Maßnahmen zur Gewinnung von Absolventinnen und Absolventen zu setzen.

9.2 Das Innenministerium setzte die Empfehlung im Ergebnis um. Es hatte in einem gemeinsamen Projekt mit dem BMKÖS neue „Richtverwendungen für IT–Sonderverträge des Bundes“ entwickelt, die mit Jänner 2022 in Kraft traten und Rahmenbedingungen im Sinne eines modernen Personalmanagements schufen. Sie könnten dazu beitragen, dass den mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung steht.

Die Beurteilung der neuen „Richtverwendungen für IT–Sonderverträge des Bundes“ war nicht Gegenstand dieser Follow–up–Überprüfung. Der RH wies jedoch kritisch darauf hin, dass das Innenministerium mit der Einrichtung von RIVIT–Planstellen erst in der Zentralstelle begonnen hatte und noch nicht für Personal, das für die Bekämpfung von Cyberkriminalität zuständig war.

Die ergänzenden Maßnahmen und die Kooperation mit dem Bundesministerium für Bildung, Wissenschaft und Forschung zur Einrichtung eines Schulzweiges mit dem Titel „Management (Cyber) Security“ beurteilte der RH positiv.

Der RH empfahl dem Innenministerium, die „Richtverwendungen für IT–Sonderverträge des Bundes“ in Abstimmung mit dem BMKÖS regelmäßig auf ihre Aktualität zu überprüfen. Die Richtverwendungen sollten jedenfalls geeignete Rahmenbedingungen schaffen, um den mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung zu stellen.

9.3 Das Innenministerium gab in seiner Stellungnahme an, dass die Empfehlung aus dem Vorbericht bereits gänzlich umgesetzt sei. So seien mit der im Jänner 2022 in Kraft getretenen Richtlinie zur Umsetzung von IT–Sonderverträgen die Grundlagen für höhere Einstiegsgehälter für IT–Expertinnen und –Experten im öffentlichen Dienst geschaffen worden.

9.4 Der RH wies darauf hin, dass er die Empfehlung auch als im Ergebnis umgesetzt beurteilt hatte. Dessen ungeachtet wäre es aus seiner Sicht zweckmäßig, die „Richtverwendungen für IT–Sonderverträge des Bundes“ in Abstimmung mit dem BMKÖS regelmäßig auf ihre Aktualität zu überprüfen. Dies, um nachhaltig sicherzustellen, dass geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen für mit der Bekämpfung von Cyberkriminalität befasste Organisationseinheiten gewonnen werden kann.

Reformmaßnahmen zu Cyberkriminalität

10.1 (1) Der RH hatte im Vorbericht festgestellt, dass im überprüften Zeitraum nicht alle mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Innenministeriums über die dafür zweckmäßige technische und räumliche Ausstattung verfügten.

Er hatte dem Innenministerium in seinem Vorbericht (TZ 37) daher empfohlen, angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen zu schaffen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Ministeriums die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen.

(2) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass Computer– und Internetkriminalität – bedingt durch die fortschreitende Digitalisierung aller Lebensbereiche – stark ansteigend sei und auch im Bereich der Landespolizeidirektionen zunehmend in den Fokus strategischer Überlegungen rücke. In diesem Zusammenhang sei in den Außenstellen der Landeskriminalämter ein Bedarf an Assistenzleistung festgestellt worden. Zur Unterstützung bei Ermittlungen im Bereich Internetkriminalität habe das Innenministerium bereits im Jahr 2019 im Zuge eines Probebetriebs einer Außenstelle des Landeskriminalamts Wien IT–Ermittler des Assistenzbereichs IT–Beweissicherung zur Assistenzleistung zugewiesen.

Das Innenministerium intendiere, diesen Probebetrieb auf alle Außenstellen des Landeskriminalamts Wien zu erweitern und damit weitere Erkenntnisse zu gewinnen.

(3) (a) Der RH stellte nunmehr fest, dass das Innenministerium im Rahmen seines Projekts Kriminaldienstreform einen Schwerpunkt auf die Bekämpfung von Cyberkriminalität legte. Im Zentrum der am 1. September 2023 präsentierten Ergebnisse standen nach den Angaben des Innenministeriums der vernetzte Kampf gegen neue Kriminalitätsformen und eine Aufstockung des Personals.

- Auf Ebene der Polizeiinspektionen sollten ab einem Soll–Personalstand von 19 Bediensteten[23] sogenannte **Kriminaldienstgruppen** eingesetzt werden. In jeder Kriminaldienstgruppe sollte zumindest eine Bedienstete bzw. ein Bediensteter die Sonderausbildung zur Cybercrime–Ermittlerin bzw. zum Cybercrime–Ermittler[24] in einem Cybercrime–Training–Center absolvieren, um entsprechende Kompetenzen zu erlangen und Internetermittlungen führen zu können.

[23] Bei einem Soll–Personstand von weniger als 19 Bediensteten konnten diese Kriminaldienstgruppen eingerichtet werden.

[24] Diese sollten in der Folge die Bezirks–IT–Ermittlerinnen und –Ermittler ablösen.

- Auf Ebene der Bezirks– und Stadtpolizeikommanden sollten österreichweit 38 Regionen mit je einer **Kriminal–Assistenzdienststelle** eingerichtet werden, in denen (auch zur Unterstützung der Polizeiinspektionen) hauptamtliche IT–Forensikerinnen und –Forensiker digitale Spuren sicherstellen und auswerten sowie Cybercrime–Ermittlerinnen und –Ermittler Internetermittlungen führen sollten.
- Auf Ebene der Landeskriminalämter (mit Ausnahme von Wien) sollten die bestehenden Ermittlungs– und Assistenzbereiche in sogenannte „**Kriminalbereiche**“ umbenannt und in sieben Referaten organisiert werden. Eine wesentliche Neuerung war das in jedem Kriminalbereich vorgesehene Referat Cybercrime mit drei Fachbereichen zu IT–Forensik, Cybercrime–Ermittlungen und Cybercrime–Training–Center. Der Fachbereich Cybercrime–Training–Center sollte – neben seinen Aufgaben zur strukturierten Datenerfassung von Cyberkriminalitäts–Delikten, Zusammenführung von Massendelikten und unmittelbaren Unterstützung der nachgeordneten Dienststellen – auch die Cybercrime–Ermittlerinnen und –Ermittler ausbilden. Außerdem sollten die Referate Cybercrime komplexere Ermittlungen eigenständig führen, wobei Cyberkriminalität im weiteren Sinn grundsätzlich bei den Kriminalbereichen verbleiben sollte.
- Für die Referate Cybercrime plante das Innenministerium österreichweit 176 Arbeitsplätze als Mindestausstattung:
  - 16 Arbeitsplätze für die Referate Cybercrime selbst,
  - 74 Arbeitsplätze für den Fachbereich IT–Forensik (inklusive Landeskriminalamt Wien, für dieses waren 38 Arbeitsplätze vorgesehen),
  - 68 Arbeitsplätze für den Fachbereich Cybercrime–Ermittlungen (exklusive Landeskriminalamt Wien),
  - 18 Arbeitsplätze für den Fachbereich Cybercrime–Training–Center (neun Standorte, inklusive zwei Arbeitsplätze für Wien).

Auch im Bundeskriminalamt plante das Innenministerium Änderungen aufgrund der Kriminaldienstreform. Das Cybercrime Competence Center war nicht Teil der Kriminaldienstreform, da das Innenministerium zur Zeit des Projektstarts davon ausgegangen war, dass dessen Reorganisation bereits früher abgeschlossen sein würde.

Das Innenministerium sah zur Zeit der Follow–up–Überprüfung (Oktober 2023) 300 von 735 neu einzurichtenden Arbeitsplätzen für Cyberkriminalität vor. Das Personaleinsatzkonzept dazu war noch in Ausarbeitung und musste nach Fertigstellung dem BMKÖS zur Bewertung übermittelt werden. Das Recruiting für diese 300 zu schaffenden Arbeitsplätze hatte das Innenministerium noch nicht festgelegt.

Die infrastrukturellen Rahmenbedingungen für die Umsetzung der Kriminaldienstreform wollte das Innenministerium mit der Entwicklung einer IKT–Lösung für besondere kriminalpolizeiliche Ermittlungen im Rahmen des Projekts SeILE schaffen (TZ 6).

(b) Das Landeskriminalamt Wien war nicht Teil der Kriminaldienstreform. Um jedoch auch im Landeskriminalamt Wien den Fokus auf Cyberkriminalität zu legen, ersuchte das Innenministerium im September 2023 um die Gewährung von zusätzlichen Planstellen bzw. um teilweise Aufwertung bestehender Planstellen.

Wie die Einschau des RH vor Ort zeigte, entsprach die räumliche Situation des Assistenzbereichs IT–Beweissicherung des Landeskriminalamts Wien weiterhin nicht den aktuellen Anforderungen. Nach Angaben der Leitung des Assistenzbereichs IT–Beweissicherung und der Leitung des Assistenzdienstes hatten das Innenministerium und die Landespolizeidirektion Wien die im Vorbericht genannten Anträge des Landeskriminalamts Wien zur Verbesserung der Situation bislang nicht genehmigt. Als Folge der mangelnden technischen und personellen Ressourcen war der Assistenzbereich IT–Beweissicherung mit der Untersuchung von Geräten bzw. der Aktenbearbeitung weiter in Rückstand und behielt daher sein Priorisierungssystem bei. Im Zeitraum Jänner 2023 bis September 2023 langten 1.091 Mobiltelefone und SIM–Karten zur Untersuchung ein. Der älteste im Oktober 2023 zur Bearbeitung offene Akt lag dem Assistenzbereich seit mehr als einem Jahr vor. Nach Angaben der Staatsanwaltschaft Wien und des Ermittlungsbereichs Sittlichkeitsdelikte des Landeskriminalamts Wien wurden in den letzten Jahren sichergestellte Beweismittel in 70 % bis 80 % der Fälle mit Verdacht auf § 207a StGB[25] regelmäßig unmittelbar nach der Sicherstellung an externe Sachverständige zur Sicherung und Auswertung übergeben, um rascher Ergebnisse zu bekommen.

Der 2019 in Wien gestartete Probebetrieb der IT–Ermittlerinnen und –Ermittler, deren Aufgabe es war, die Ermittlungsbereiche in den Außenstellen des Landeskriminalamts Wien durch technische Assistenzleistungen bei Cyberkriminalitäts–Sachverhalten zu unterstützen, lief Ende 2022 aus. Die Landespolizeidirektion Wien verlängerte ihn danach „stillschweigend“.

10.2 Das Innenministerium setzte die Empfehlung teilweise um. So legte es im Rahmen des Projekts Kriminaldienstreform einen Fokus auf die Stärkung von flächendeckenden Ermittlungs– und Assistenzdienstleistungen und den Aufbau von spezialisierten Kompetenzen im Bereich Cyberkriminalität. Dies beurteilte der RH positiv. Mit der Umsetzung des Projekts hatte das Innenministerium zur Zeit der Follow–up–Überprüfung aber erst begonnen. Die Beurteilung der Kriminaldienstreform war daher nicht Gegenstand dieser Follow–up–Überprüfung.

Aus Sicht des RH war nicht nachvollziehbar, warum im Zuge des Gesamtkonzepts zur Stärkung der Bekämpfung von Cyberkriminalität keine konkreten Überlegungen des Innenministeriums zum Recruiting der 300 neu einzurichtenden Arbeitsplätze für den Bereich Cyberkriminalität vorlagen. Wie der RH in seinem Vorbericht (TZ 30)

[25] Pornografische Darstellungen Minderjähriger

festgestellt hatte, war die Personalrekrutierung insbesondere im Bereich Cyberkriminalität eine große Herausforderung. Gerade ressortinterne Interessentensuchen sollten aus Sicht des RH nicht zur Folge haben, dass qualifiziertes Personal der Basis entzogen wird.

Der RH hielt kritisch fest, dass das Landeskriminalamt Wien nicht Teil des Gesamtkonzepts zur Stärkung der Bekämpfung von Cyberkriminalität war. Da Wien das mit Abstand größte Landeskriminalamt Österreichs war, wäre dies aus Sicht des RH umso wichtiger gewesen.

Der RH hielt – wie in seinem Vorbericht – kritisch fest, dass eingeschränkte Ressourcen beim Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien bei gleichzeitig gestiegenen Anforderungen zur Folge hatten, dass der Assistenzbereich IT–Beweissicherung Akten – bzw. in Zusammenhang mit diesen zur Auswertung übergebene Endgeräte – über Monate nicht bearbeitete.

Nach Ansicht des RH war – neben einer zweckmäßigen Organisation, einer adäquaten personellen Ausstattung der Organisationseinheiten und dem fachlichen Know–how der Bediensteten – auch eine geeignete technische und räumliche Infrastruktur unerlässlich, um Cyberkriminalität effektiv bekämpfen zu können. Daher sollten den mit Cyberkriminalität befassten Bediensteten geeignete Arbeitsplätze und die für die zeitgemäße Erledigung der ihnen übertragenen Aufgaben notwendige, dem Stand der Technik entsprechende Soft– und Hardware in zweckmäßigem Umfang zur Verfügung stehen.

Zu den infrastrukturellen Rahmenbedingungen verwies der RH auf seine Feststellungen in TZ 6 zum Projekt SeILE.

Der RH empfahl dem Innenministerium weiterhin, – insbesondere im Bereich des Landeskriminalamts Wien – angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen zu schaffen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Ministeriums die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen.

Weiters empfahl er dem Innenministerium, die Schritte zur Stärkung der Prävention und Bekämpfung von Cyberkriminalität sukzessive umzusetzen, die gesetzten Maßnahmen regelmäßig auf ihre Zielerreichung zu überprüfen und gegebenenfalls anzupassen sowie strategische Überlegungen zum Personalbedarf miteinfließen zu lassen.

Der RH stellte kritisch fest, dass die Landespolizeidirektion Wien trotz der positiven Erfahrungen aus dem Probebetrieb der IT–Ermittlerinnen und –Ermittler (siehe dazu Vorbericht TZ 25) diesen weiterhin nicht in den Regelbetrieb übernommen hatte.

Der Probebetrieb war Ende 2022 ausgelaufen und seither „stillschweigend“ verlängert worden. Der RH verwies daher auf seine Empfehlung in TZ 25 des Vorberichts an das Innenministerium, dafür zu sorgen, dass der probeweise Einsatz von IT–Ermittlerinnen und –Ermittlern des Assistenzbereichs IT–Beweissicherung in den Außenstellen des Landeskriminalamts Wien in den Regelbetrieb übernommen wird und die Planstellen dem Assistenzbereich IT–Beweissicherung zugeordnet werden.

10.3 Das Innenministerium wiederholte in seiner Stellungnahme die Angaben aus dem Nachfrageverfahren 2022, u.a. dass geplant sei, den Probebetrieb der IT–Ermittlerinnen und –Ermittler auf alle Außenstellen des Landeskriminalamts Wien auszudehnen. Zusätzlich wies es darauf hin, dass es die organisatorischen, personellen und infrastrukturellen Rahmenbedingungen laufend an neue Herausforderungen anpasse, um der Kriminalität in Österreich effizient entgegenwirken zu können. In diesem Zusammenhang seien die bereits eingeleitete Kriminaldienstreform und damit einhergehende Optimierungen im Bereich der Prävention von Cyberkriminalität besonders hervorzuheben.

Im Rahmen der Strategie „Sicheres Internet“ würden bestehende Maßnahmen zielgerichtet gebündelt sowie neue Herangehensweisen sukzessive umgesetzt. Die Zielsetzung werde laufend überprüft und strategische Überlegungen zum Personalbedarf würden maßgeblich in Prozesse und Entscheidungen einfließen.

10.4 Der RH konnte das wiederholte Vorbringen des Innenministeriums zum Probebetrieb nicht nachvollziehen. Dieser Probebetrieb war – wie vom RH in dieser TZ bzw. im Vorbericht in TZ 25 festgestellt – bereits eingerichtet und mit Ende des Jahres 2022 ausgelaufen.

Da das Landeskriminalamt Wien auch nicht Teil der geplanten Kriminaldienstreform war, vermisste der RH weiterhin angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Innenministeriums die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen.

Aus– und Fortbildung

11.1 (1) Der RH hatte dem Innenministerium in seinem Vorbericht (TZ 35) empfohlen, sicherzustellen, dass alle ermittelnden Bediensteten über das für ihre Tätigkeit notwendige Basiswissen in den Bereichen IT und Cyberkriminalität verfügen, und diese Themen daher verstärkt in der Fortbildung zu berücksichtigen.

(2) Das Innenministerium hatte im Nachfrageverfahren mitgeteilt, dass aus seiner Sicht diese Empfehlung durch die Implementierung von Schulungsangeboten bereits umgesetzt sei. Bedienstete hätten z.B. im Rahmen der Fachausbildung für den Kriminaldienst das Modul „IT–Kriminalität“ zu absolvieren. Dabei handle es sich um ein dezentrales Fortbildungsangebot für alle im Kriminaldienst verwendeten und geeigneten Bediensteten. Weiters würden in kriminalpolizeilichen Fortbildungsmaßnahmen seit 2017 spezifische Schulungen in den Bereichen IT und Cyberkriminalität durchgeführt. Dauer und Inhalt richteten sich dabei nach den individuellen Bedarfen der Ermittlungs– bzw. Assistenzbereiche, sie würden daher jedes Jahr evaluiert und gegebenenfalls entsprechend adaptiert. Darüber hinaus seien im „Kriminalistischen Leitfaden“ jederzeit und für alle Bediensteten frei zugänglich aktuelle Informationen zu IT–Kriminalität abrufbar. Diesbezügliche Maßnahmen werde das Innenministerium auch in Zukunft konsequent weiterverfolgen.

(3) Der RH stellte nunmehr fest, dass das Innenministerium IT– und Cyberkriminalitäts–Themen in Grundausbildungslehrgängen, in fachlichen Ausbildungen für den Kriminaldienst und in Fortbildungsveranstaltungen schulte. Zur Zeit der Follow–up–Überprüfung bildete es zudem weiterhin Bezirks–IT–Ermittlerinnen und –Ermittler aus und beabsichtigte, Schulungen aufrechtzuerhalten, bis die Kriminaldienstreform umgesetzt war.

In der Ausbildung berücksichtigte das Innenministerium zur Zeit der Follow–up–Überprüfung Cyberkriminalität in folgendem Umfang:

Tabelle 3: Ausbildungen des Innenministeriums mit Bezug zu Cyberkriminalität

Art der Ausbildung	Inhalte mit Bezug zu Cyberkriminalität
Grundausbildung der eingeteilten Exekutivbediensteten	– 10 Unterrichtseinheiten in den Themenblöcken Straf– und Privatrecht sowie Kriminalistik – spezifische Inhalte in weiteren Themenblöcken (z.B. Auskunft über Stamm– und Zugangsdaten)
Grundausbildung der dienstführenden Exekutiv-bediensteten	– 8 Unterrichtseinheiten explizit zu Cyberkriminalität – 4 Unterrichtseinheiten zu Betrugs– und Internetbetrugskriminalität im Themenblock Kriminalistik – spezifische Inhalte im Themenblock Strafrecht (z.B. Cyberkriminalität im weiteren Sinn als Erscheinungsform)
Fachausbildung für den Kriminaldienst	– 8 Unterrichtseinheiten zu IT–Kriminalität – spezifische Inhalte in weiteren Themenblöcken (z.B. Online–Suchtmittelkriminalität)
Ausbildung für Bezirks–IT–Ermittlerinnen und –Ermittler	– 64 Unterrichtseinheiten zum Modul Technik – 32 Unterrichtseinheiten zum Modul Kriminalistik – 24 Unterrichtseinheiten zum Modul Recht – 6 Unterrichtseinheiten zum Modul Prävention – 2 Monate praktische Ausbildung

Quelle: BMI

Das Innenministerium sah für die berufsbegleitende Fortbildung im Kriminaldienst für den Zyklus 2020 bis 2023 zumindest drei Unterrichtseinheiten je Fachbereich für Cyberkriminalitäts–Inhalte vor. Bedienstete von Landeskriminalämtern waren verpflichtet teilzunehmen. Bedienstete des operativen Kriminaldienstes in Stadtpolizeikommanden[26] hatten im Ausmaß einer bestimmten Quote teilzunehmen.

Das Bundeskriminalamt adaptierte die Struktur des Kriminalistischen Leitfadens als Wissensplattform, um Exekutivbedienstete mit Handlungsanleitungen, Checklisten und Videos gezielt zu Themen der Cyberkriminalität zu informieren. Die Inhalte passte es abgestimmt mit den jeweiligen Fachabteilungen in einem strukturierten Prozess grundsätzlich jährlich an. Das Cybercrime Competence Center war berechtigt, die Inhalte zu Cyberkriminalität direkt zu bearbeiten, um auf Änderungen zeitnah reagieren zu können. Für die eigenen Bediensteten und Bedienstete der Fachbereiche der Landeskriminalämter organisierte es bedarfsorientiert zusätzliche Weiterbildungen.

[26] Angehörige der Bezirkspolizeikommanden wurden auf nachgeordneter Ebene über ein Train–the–Trainer–System der Landeskriminalämter fortgebildet.

Die Kriminaldienstreform sah vor, dass alle Exekutivbediensteten an praktischen Schulungen im Ausmaß von 32 Unterrichtseinheiten in noch einzurichtenden Cybercrime–Training–Centern der Landeskriminalämter teilnehmen. Themen der Schulungen waren u.a. Hardware, Netzwerktechnik, Darknet, soziale Medien, Messenger, Tatortverhalten, Beweismittelsicherung oder Blockchain–Technologie. Es sollten Exekutivbedienstete innerhalb eines Jahres nach der Grundausbildung einberufen und verbleibende Ausbildungsplätze nach freiwilligen Meldungen vergeben werden. Damit sollte in fünf Jahren etwa die Hälfte der Bediensteten je Landespolizeidirektion erreicht werden. Das Bundeskriminalamt plante, die ersten Schulungen im Jahr 2024 im Cybercrime–Training–Center der Landespolizeidirektion Oberösterreich zu starten.

11.2 Das Innenministerium setzte die Empfehlung teilweise um. Nach Ansicht des RH waren die Grundausbildungslehrgänge, Fachausbildungen, berufsbegleitenden Fortbildungen sowie die Wissensplattform des Kriminalistischen Leitfadens geeignet, ermittelnden Bediensteten das notwendige Basiswissen zu vermitteln. Der RH kritisierte jedoch, dass das Innenministerium eine praktische Ausbildung weiterhin nur für Kriminalsachbearbeiterinnen und –sachbearbeiter, nicht aber für allgemein eingeteilte Exekutivbedienstete vorsah. Er anerkannte, dass das Innenministerium im Rahmen der Kriminaldienstreform plante, eine praktische Fortbildung zu ergänzen.

Der RH empfahl dem Innenministerium, die im Zuge der Kriminaldienstreform 2.0 geplanten Cybercrime–Training–Center zeitnah einzurichten, um allen ermittelnden Bediensteten die für ihre Tätigkeit notwendigen Basisfähigkeiten in den Bereichen IT und Cyberkriminalität vermitteln zu können.

11.3 Das Innenministerium wiederholte in seiner Stellungnahme seine Angaben aus dem Nachfrageverfahren im Jahr 2022, u.a. dass aus seiner Sicht die Empfehlung aus dem Vorbericht durch die Implementierung von Schulungsangeboten bereits umgesetzt sei. Zusätzlich teilte es mit, dass es Schulungsangebote auch in Zukunft evaluieren und erweitern werde, damit alle ermittelnden Bediensteten über das für ihre Tätigkeit notwendige Basiswissen in den Bereichen IT und Cyberkriminalität verfügen würden. So würden im Rahmen der Kriminaldienstreform Cybercrime–Training–Center in allen Landeskriminalämtern eingerichtet.

Prävention

12.1 (1) Der RH hatte im Vorbericht festgestellt, dass das Bundeskriminalamt in seiner Präventionsrichtlinie 2017 Cyberkriminalität als eigenen Präventionsbereich festgelegt hatte. Es hatte mit den Ausbildungen der Präventionsbediensteten jedoch erst im Jahr 2019 begonnen und das Curriculum noch nicht fertiggestellt.

Der RH hatte dem Bundeskriminalamt in seinem Vorbericht (TZ 16) daher empfohlen, das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität fertigzustellen, seine Anwendung sicherzustellen und in der Folge die Ausbildung der Präventionsbediensteten fortzuführen.

(2) Das Bundeskriminalamt hatte im Nachfrageverfahren mitgeteilt, dass es die Empfehlung aufgreifen und im Rahmen einer Evaluierung berücksichtigen werde.

(3) Der RH stellte nunmehr fest, dass das Bundeskriminalamt im Jahr 2023 eine neue Präventionsrichtlinie erließ. Das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität stellte es nicht fertig. Zur Zeit der Follow–up–Überprüfung plante es, das Curriculum im ersten Quartal 2024 zu finalisieren.

Das Bundeskriminalamt bot seit 2019 auch keine weiteren Ausbildungen für die Präventionsbediensteten an. Als Grund nannte es – neben den Verzögerungen durch die COVID–19–Pandemie – fehlende personelle Ressourcen. Das Bundeskriminalamt beabsichtigte, im Herbst 2023 einen Ausbildungslehrgang auf Grundlage einzelner, fertiggestellter Teile des Curriculums anzubieten. Weitere vier Schulungstermine nach dem neuen Curriculum der Präventions–Ausbildung für Cyberkriminalität sollte es im Jahr 2024 geben.

12.2 Das Bundeskriminalamt setzte die Empfehlung nicht um. Es hatte zur Zeit der Follow–up–Überprüfung weder das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität fertiggestellt noch die Ausbildung der Präventionsbediensteten fortgeführt. Der RH erachtete die standardisierte Ausbildung von Präventionsbediensteten weiterhin für wesentlich.

Er empfahl daher dem Bundeskriminalamt neuerlich, das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität fertigzustellen, seine Anwendung sicherzustellen und in der Folge die Ausbildung der Präventionsbediensteten entsprechend fortzuführen.

12.3 Das Innenministerium gab in seiner Stellungnahme an, dass sich das Curriculum der Präventions–Ausbildung für Cyberkriminalität in der Fertigstellung befinde. Der Start der Anwendung und der ebenfalls angesprochenen Schulungen werde voraussichtlich mit 30. September 2024 erfolgen.

13.1 (1) Der RH hatte im Vorbericht festgestellt, dass das Bundeskriminalamt ein Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität gestartet hatte. Allerdings lagen dazu aufgrund der COVID–19–Pandemie zur Zeit der Vorprüfung noch keine Erkenntnisse vor.

Der RH hatte dem Bundeskriminalamt daher empfohlen (TZ 19), das Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität weiterzuverfolgen, die Ergebnisse in der Folge zu verwerten und umzusetzen.

(2) Das Bundeskriminalamt hatte im Nachfrageverfahren mitgeteilt, dass die Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität ein essenzieller Faktor sei, um Erkenntnisse – insbesondere im Hinblick auf die Qualität der Zielgruppen– und Bedarfsorientierung – zu gewinnen. Weitere Kennzahlen könnten sich, vor allem nach Abschluss verschiedener Projekte, entwickeln. Das konkrete Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen sei abgeschlossen. Die Ergebnisse der Experteninterviews würden ein umfassendes Bild zeigen und teilweise bereits in die Ausbildung und Maßnahmen der Kriminalprävention eingebaut.

(3) (a) Der RH stellte nunmehr fest, dass das mit dem Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität beauftragte Institut für Höhere Studien (**IHS**) im Dezember 2020 einen Endbericht mit dem Titel „Optimierung von kriminalpräventiven Angeboten“ vorlegte.

Entsprechend der Zielsetzung des Projekts sollten mittels Literaturrecherche geeignete Instrumente aufgezeigt werden, um die Wirkung und den Erfolg von Präventionsmaßnahmen messen und beurteilen zu können. Außerdem war geplant, diese Wirkung und diesen Erfolg unter Einsatz der erarbeiteten Instrumente in der Praxis zu messen. So sollten Teilnehmende an Präventionsveranstaltungen zu Cyberkriminalität unmittelbar nach der Teilnahme u.a. zur Qualität der Veranstaltung und einige Zeit später zu allfällig geänderten Einstellungs– und Verhaltensmustern bzw. dem individuellen Sicherheitsgefühl befragt werden.

Dazu verschickte das IHS Fragebögen an die Teilnehmenden. Aufgrund der COVID–19–Pandemie fanden kaum Präsenzveranstaltungen statt, außerdem war die Rücklaufquote sehr gering. Das IHS sah daher von einer quantitativen Auswertung ab und verbesserte den Fragebogen aufgrund von Erfahrungen während der Erhebung. Diesen stellte es dem Bundeskriminalamt zur weiteren Verwendung zur Verfügung.

Sonstige Instrumente, um die Wirkung und den Erfolg von Präventionsmaßnahmen messen und beurteilen zu können, wurden im Zuge des Projekts nicht erarbeitet. Statt die Präventionsmaßnahmen in der Praxis anhand der erarbeiteten Instrumente zu messen, wie im Projekt geplant, führte das IHS Interviews mit Expertinnen und Experten im Bundeskriminalamt bzw. aus Organisationen, die im Bereich der Prävention mit dem Bundeskriminalamt zusammenarbeiteten. Daraus leitete es Handlungsansätze u.a. zur Qualitätssicherung der Aus– und Weiterbildung, Verbesserung der Datenerfassung und –analyse, Bekanntmachung von Präventionsangeboten, zu kriminalpräventiven Schwerpunkten und zur kriminalpräventiven Zusammenarbeit ab.

(b) Der Innenminister präsentierte im August 2023 die ressortweite Präventionsstrategie „Sicheres Internet“. In dieser legte das Bundeskriminalamt Handlungsfelder – wie Aus– und Fortbildungen, Zusammenarbeit mit Wissenschaft und Forschung sowie zielgruppenorientierte Konzepte – fest und plante, auf Grundlage dieser einen Maßnahmenplan zur praktischen Umsetzung zu erstellen. Das Handlungsfeld „Wissenschaft und Forschung“ sah eine Evaluierung der noch zu definierenden Maßnahmen mit anschließender quantitativer und qualitativer Optimierung vor. Konkrete Angaben über eine allfällige Wirkungs– und Erfolgsmessung enthielt die Strategie nicht.

Das Bundeskriminalamt setzte eine Arbeitsgruppe ein, um in Abstimmung mit betroffenen Organisationseinheiten des Innenministeriums, wie den Landespolizeidirektionen, die Handlungsfelder abzuarbeiten. Die erste Sitzung dazu fand im September 2023 statt. Als Ergebnis dieser Sitzung plante das Bundeskriminalamt, einen Projektstrukturplan für einzelne Zielgruppen zu erstellen. Zur Zeit der Follow–up–Überprüfung war die Umsetzung zeitlich noch nicht abschätzbar.

13.2 Das Bundeskriminalamt setzte die Empfehlung teilweise um. Das Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität war mit Dezember 2020 abgeschlossen, jedoch war die ursprüngliche Zielsetzung nicht erreicht und die erzielten Ergebnisse noch nicht umgesetzt. Die Projektergebnisse waren insbesondere Handlungsansätze, um die bestehenden Präventionsangebote zu optimieren. Der RH kritisierte, dass sie nicht auf die Wirkungs– und Erfolgsmessung von Präventionsmaßnahmen oder deren praktische Erprobung abzielten. Er erachtete die Wirkungs– und Erfolgsmessung von Präventionsmaßnahmen als wesentlich, um diese möglichst zielgruppen– und bedarfsorientiert ausrichten zu können.

Der RH anerkannte, dass das Bundeskriminalamt aus den Handlungsansätzen zur Optimierung der Präventionsangebote die Strategie „Sicheres Internet“ entwickelte und im Rahmen des Handlungsfelds „Wissenschaft und Forschung“ eine Evaluierung nach quantitativen und qualitativen Parametern vorsah.

Der RH empfahl dem Bundeskriminalamt, den in der Präventionsstrategie „Sicheres Internet“ des Innenministeriums vorgesehenen Maßnahmenplan sowie die konkreten darauf aufbauenden Maßnahmen zu erarbeiten und eine Wirkungs– und Erfolgsmessung wissenschaftlich begleitet zu entwickeln und einzusetzen.

13.3 Laut Stellungnahme des Innenministeriums befinde sich der Maßnahmenplan zur Präventionsstrategie „Sicheres Internet“ in Ausarbeitung, wobei auch die Wirkungs– und Erfolgsmessung mitbedacht würden. Erste Maßnahmen seien bereits umgesetzt worden.

Justizministerium

Organisation der Staatsanwaltschaften in Cyberkriminalitäts–Ermittlungsverfahren

14.1 (1) Laut den Feststellungen des Vorberichts waren die Staatsanwaltschaften im Hinblick auf die besonderen Herausforderungen bei der wirksamen Bekämpfung von Cyberkriminalität organisatorisch und methodisch nicht ausreichend gerüstet. Es fehlten eine Spezialisierung und die organisatorische Verankerung bei den Staatsanwaltschaften im Bereich Cyberkriminalität.

Der RH hatte dem Justizministerium daher empfohlen (TZ 43), basierend auf internationalen Beispielen und den Erfahrungen besonders betroffener Staatsanwaltschaften organisatorische Rahmenbedingungen für eine spezialisierte Bearbeitung von Ermittlungsverfahren im Bereich Cyberkriminalität festzulegen.

(2) Das Justizministerium hatte im Nachfrageverfahren mitgeteilt, dass im Frühjahr 2022 bei den Staatsanwaltschaften Graz und Wien als Pilotversuch je eine Cybercrime–Kompetenzstelle mit besonders geschulten Staatsanwältinnen und Staatsanwälten eingerichtet worden sei. Diese stünden in laufendem Austausch mit den spezialisierten Polizeieinheiten und als Ansprechpersonen für Spezialfragen sowie für die Abklärung von Konnexitäten zur Verfügung.

(3) (a) Der RH stellte nunmehr fest, dass im März 2022 die Staatsanwaltschaft Graz und die Staatsanwaltschaft Wien als Pilotprojekt jeweils eine „Kompetenzstelle Cybercrime“ einsetzten. Ab Jänner 2023 startete aufgrund der Erfahrungen in Graz und Wien ein bundesweiter, einjähriger Probebetrieb, mit Kompetenzstellen Cybercrime bei den Staatsanwaltschaften Graz, Innsbruck, Klagenfurt, Linz, Ried im Innkreis, Salzburg, Steyr, Wels, Wiener Neustadt und Wien. Die Staatsanwaltschaften

Eisenstadt, Feldkirch, Korneuburg[27], Krems, Leoben und St. Pölten sowie die Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption[28] benannten sogenannte Kontakt– und Verbindungsstellen. Die Kompetenzstellen und Kontakt– und Verbindungsstellen unterstützten staatsanwaltliche Ermittlungen bei Verfahren mit Bezug zu Cyberkriminalität. Bei den Oberstaatsanwaltschaften fungierte je eine Cybercrime–Koordinatorin bzw. ein Cybercrime–Koordinator als Ansprechstelle für die Kompetenzstellen sowie die Kontakt– und Verbindungsstellen.

(b) Im Zeitraum Jänner bis August 2023 unterstützten die Kompetenzstellen bei Ermittlungen in zumindest 869 Fällen. Wegen unterschiedlicher Betrachtungszeiträume und Zählweise[29] waren Auswertungen dazu zur Zeit der Follow–up–Überprüfung eingeschränkt aussagekräftig. Das Justizministerium beabsichtigte, die Zählweise zu vereinheitlichen und die Anzahl der Unterstützungsleistungen periodisch einzuholen.

(c) Die Kompetenzstellen verfügten über keine Sonderzuständigkeit für Cyberkriminalität. Die Leitung der Staatsanwaltschaft konnte ihnen jedoch bestimmte Verfahren zuweisen, für die eine besondere Expertise in Cyberkriminalität erforderlich war. Die Staatsanwaltschaft Wien verfügte zudem in ihrer Geschäftsverteilung, dass Delikte der Cyberkriminalität im engeren Sinn im bezirksgerichtlichen Zuständigkeitsbereich spezialisierten Bezirksanwältinnen bzw. –anwälten zugewiesen werden.

(d) Das Justizministerium veranstaltete interministerielle Cybercrime–Qualitätszirkel sowie Vernetzungstreffen für Kompetenz– sowie Kontakt– und Verbindungsstellen und stellte eine digitale Plattform zum Informationsaustausch zur Verfügung, um den Wissenstransfer zu Cyberkriminalität zu fördern. Auf regionaler Ebene beabsichtigte das Innenministerium unter Einbindung des Justizministeriums zudem, durch sogenannte Cybercrime–Gesprächsplattformen operative Probleme, Lösungsstrategien und Best Practices zu erkennen.

(e) Im Evaluierungszeitraum Jänner bis September 2023 beurteilten das Justizministerium sowie die Kompetenzstellen selbst den Aufbau und die Zusammenarbeit der Kompetenzstellen positiv. Um die Vernetzung intern sowie zur Kriminalpolizei zu intensivieren, die Organisation zu professionalisieren, Problemen zu begegnen und diese Maßnahmen evaluieren zu können, plante das Justizministerium zur Zeit der Follow–up–Überprüfung, den Probebetrieb um zwei Jahre zu verlängern.

[27] Diese errichtete ab 19. April 2023 ebenfalls eine Kompetenzstelle Cybercrime.

[28] Diese errichtete ab 1. Oktober 2023 ebenfalls eine Kompetenzstelle Cybercrime.

[29] Zum Beispiel zählten einige Kompetenzstellen mündliche Unterstützungsleistung ohne formelle Befassung als Fallbearbeitung, andere nicht.

14.2 Das Justizministerium setzte die Empfehlung im Ergebnis um. Insbesondere durch die Einrichtung der Kompetenzstellen Cybercrime bei Staatsanwaltschaften und die Cybercrime–Qualitätszirkel entwickelte das Justizministerium eine zweckmäßige Organisation, um die Staatsanwaltschaften bei Fällen von Cyberkriminalität zu unterstützen. Der RH bemängelte jedoch, dass die Kompetenzstellen Cybercrime noch im Probebetrieb waren und bei den Staatsanwaltschaften noch keine Sonderzuständigkeiten für Cyberkriminalität eingerichtet waren.

Der RH empfahl dem Justizministerium daher, den Probebetrieb der Kompetenzstellen Cybercrime bei den Staatsanwaltschaften fortzusetzen, zu evaluieren und nach allfällig notwendigen Anpassungen in den Regelbetrieb überzuleiten.

14.3 Das Justizministerium teilte in seiner Stellungnahme mit, dass nach umfassender Evaluierung der Stellungnahmen der Staatsanwaltschaften und Oberstaatsanwaltschaften und der gewonnenen Erkenntnisse der Probebetrieb der Kompetenzstellen Cybercrime erlassmäßig bis Ende 2025 verlängert worden sei.

Darüber hinaus seien Anpassungen mit dem Ziel, die Vernetzung justizinterner Stellen mit den Sicherheitsbehörden zu stärken, vorgenommen und sei beim Qualitätszirkel der Teilnehmerkreis um die Generalprokuratur erweitert worden. Die Vernetzungstreffen Cybercrime zum praxisorientierten Austausch seien institutionalisiert worden, außerdem sei die Teilnahme an polizeilichen Vernetzungstreffen sowohl für die Sonderreferentinnen und –referenten als auch für die Koordinatorinnen bzw. Koordinatoren festgelegt worden.

Die Überführung des Probebetriebs in einen Regelbetrieb werde legistischer Maßnahmen bedürfen, wobei diese nach mehreren Evaluierungsschleifen im Rahmen des zweijährigen Probebetriebs festzulegen seien. Im aktuellen Erlass sei zunächst eine Berichtspflicht für Dezember 2024 festgelegt.

Die Verlängerung des Probebetriebs auf zwei Jahre sei notwendig gewesen, da der bundesweite Evaluierungszeitraum von einem Jahr zu kurz gewesen sei, um bereits in den Regelbetrieb überzugehen. Mit Blick auf die dynamischen Komponenten von Cyberkriminalität erscheine es zielführend, über einen längerfristigen Zeitraum die Organisationsstrukturen und administrativen Prozesse zu erproben und weitere Erkenntnisse zu gewinnen, um zielführende und effektive Maßnahmen zu identifizieren, bevor legistische Änderungen in Umsetzung gebracht würden. Weiters verwies das Justizministerium auf die zur Zeit der Stellungnahme bestehende Möglichkeit der Leitung der Staatsanwaltschaften, bestimmte Verfahren an die staatsanwaltschaftlichen Sonderreferentinnen und –referenten zuzuweisen.

Aus– und Fortbildung

15.1 (1) Der RH hatte dem Justizministerium in seinem Vorbericht (TZ 44) empfohlen, ein Aus– und Fortbildungskonzept zu erarbeiten und umzusetzen, das Schulungsangebot auszuweiten und den selbstständigen Wissenserwerb und –transfer zu unterstützen, damit alle mit Cyberkriminalität befassten Bediensteten der Staatsanwaltschaften über das für eine effiziente Fallbearbeitung notwendige technische Grundwissen verfügen. Diesbezüglich wäre verstärkt mit dem Innenministerium zusammenzuarbeiten.

(2) Das Justizministerium hatte im Nachfrageverfahren mitgeteilt, dass es plane, auf Basis des konkreten Bedarfs der befassten Dienststellen ein effizientes und zeitgemäßes Bildungskonzept zu Cyberkriminalität umzusetzen. Neben den bereits bestehenden Fortbildungsmöglichkeiten finde zur Zeit des Nachfrageverfahrens ein reger Austausch zwischen (Ober–)Staatsanwaltschaften, der Vereinigung Österreichischer Staatsanwältinnen und Staatsanwälte sowie den Polizeibehörden statt, um die für die Praxis relevanten Inhalte genau festlegen zu können. In weiterer Folge solle ein speziell für die Erfordernisse der staatsanwaltschaftlichen Praxis zugeschnittenes Curriculum „Cybercrime“ mit Start im Jahr 2023 entwickelt werden.

Weiters seien bereits punktuelle Seminare gestartet worden, beispielsweise „Cybercrime“, „Gewalt und Hass im Netz“ sowie „Vermögensrechtliche Anordnungen – elektronische Beweismittel“. Seit Juli 2021 sei eine an die Bedürfnisse der Justiz angepasste Version der – vom Innenministerium konzipierten – Online–Schulung „Hate Crime – Systematische Ermittlung und Erfassung von vorurteilsmotivierten Straftaten“ für Richterinnen und Richter sowie Staatsanwältinnen und Staatsanwälte verfügbar.

(3) (a) Der RH stellte nunmehr fest, dass das Justizministerium seit Jänner 2023 eine Basisschulung Cybercrime für Bezirks– und Staatsanwältinnen bzw. –anwälte anbot. Darin vermittelte es technische und rechtliche Grundlagen zu aktuellen Cyber–Phänomenen. Bis zu 253 Personen aus dem staatsanwaltlichen und bis zu 106 Personen aus dem bezirksanwaltlichen Bereich nahmen bis zur Follow–up–Überprüfung (Oktober 2023) daran teil und somit jeweils mehr als die Hälfte der Zielgruppen. Zudem konnten an dieser Basisschulung ab Oktober 2023 auch Richterinnen und Richter teilnehmen. Das Justizministerium plante außerdem einen Lehrgang für Staatsanwältinnen und Staatsanwälte der Kompetenzstellen Cybercrime. Mit diesem Lehrgang sollten vertiefende rechtliche, internationale und praktische Inhalte geschult werden.

(b) Die von den Interessenvertretungen der Staatsanwältinnen und Staatsanwälte sowie der Richterinnen und Richter angebotenen fachspezifischen Bildungsveranstaltungen koordinierte das Justizministerium mit seinem Schulungsangebot. Damit bot es in den Jahren 2020 bis 2023 insgesamt mehr als 190 Bildungsveranstaltungen mit Bezug zu Cyberkriminalität an.

(c) Das Justizministerium entsandte Vortragende zur Sicherheitsakademie des Innenministeriums, ließ Bedienstete des Innenministeriums an eigenen Schulungen teilnehmen und nahm zur Abstimmung des Ausbildungsangebots an Austauschtreffen der Akademien des Bundes, an Qualitätszirkeln und Vernetzungstreffen teil. Außerdem kooperierten Staatsanwaltschaften bei Ausbildungen auf lokaler Ebene mit Landespolizeidirektionen.

15.2 Das Justizministerium setzte die Empfehlung um. Es bot eine Basisschulung zu Cyberkriminalität für Bezirks– und Staatsanwältinnen bzw. –anwälte an, mit der es zur Zeit der Follow–up–Überprüfung bereits mehr als der Hälfte dieser Zielgruppe Grundwissen zu Cyberkriminalität vermittelt hatte. Darüber hinaus bot es ab Oktober 2023 diese Basisschulung auch Richterinnen und Richtern an, plante einen vertiefenden Lehrgang für Staatsanwältinnen und –anwälte der Kompetenzstellen Cybercrime und koordinierte fachspezifische Bildungsangebote. Nach Ansicht des RH war die vertiefende Ausbildung für Staatsanwältinnen und Staatsanwälte der Kompetenzstellen Cybercrime wesentlich, um notwendiges Spezialwissen für die Aufgabenerfüllung gewährleisten zu können.

Der RH empfahl daher dem Justizministerium, den geplanten, vertiefenden Lehrgang zu Cyberkriminalität zeitnah umzusetzen, um insbesondere Staatsanwältinnen und Staatsanwälten der Kompetenzstellen Cybercrime eine angemessene Fortbildung zu ermöglichen.

15.3 Laut Stellungnahme des Justizministeriums würden das erste und zweite von drei Pflichtmodulen des Lehrgangs Cyberkriminalität bereits im Frühjahr 2024, das dritte Pflichtmodul sowie das Wahlmodul „Großverfahren“ im zweiten Halbjahr 2024 und ein weiteres Wahlmodul „Best Practice“ Ende 2024/Anfang 2025 stattfinden.

Im Rahmen des ersten Moduls würden materiell–rechtliche sowie prozessrechtliche Themen, u.a. unter Einbeziehung aktueller Themen sowie auch unionsrechtlicher und nationaler Aspekte der Sicherstellung von Datenträgern und Daten, das Verfahren vor dem Verfassungsgerichtshof und dem Europäischen Gerichtshof und aktuelle gesetzgeberische Entwicklungen erörtert. Das zweite Pflichtmodul widme sich internationalen Aspekten, z.B. Internationalen Rechtsquellen zum Thema Cyberkriminalität, der Rechtshilfe oder den Herausforderungen der justiziellen Zusammenarbeit. Im dritten Modul werde technisches, forensisches und ermittlungstaktisches Wissen geschult. Eine Präsentation und vertiefende Erläuterung der technischen

Ermittlungsmöglichkeiten in den Räumlichkeiten des Cybercrime Competence Centers seien geplant, ferner werde die künstliche Intelligenz als Tatmittel thematisiert.

Zum Lehrgang seien bereits 30 Personen aus den Kompetenz– und Koordinierungsstellen Cybercrime bzw. aus der Gruppe der Cybercrime–Koordinatorinnen und –Koordinatoren der Oberstaatsanwaltschaften für eine Teilnahme in Präsenz zugelassen, die maximale Kapazität sei ausgeschöpft. Weitere 13 Teilnehmerinnen und Teilnehmer seien online zugelassen, u.a. Richterinnen und Richter des Landesgerichts für Strafsachen und des Oberlandesgerichts. Das Innenministerium sei in den Lehrgang eingebunden, auf Einladung werde der Leiter des Cybercrime Competence Centers am ersten Modul des Lehrgangs teilnehmen. Zudem werde ein Beamter des Cybercrime Competence Centers vortragen und ein Tag werde am Standort des Cybercrime Competence Centers stattfinden. Ferner werde den Bediensteten des Cybercrime Competence Centers auch eine Online–Teilnahme ermöglicht. Es hätten auch international tätige Vortragende gewonnen werden können. Eine Vertreterin des US–Department for Justice, jeweils ein Vertreter von Eurojust und Europol sowie ein Vertreter der Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern, würden ihre Fachexpertise beisteuern.

Für Ende 2024 sei eine weitere Basisschulung Cyberkriminalität geplant. An den insgesamt 24 Modulen der abgeschlossenen Basisschulung Cyberkriminalität hätten bereits rd. 2.460 Personen teilgenommen.

Schlussempfehlungen

16 Der RH stellte fest, dass

- das Bundesministerium für Inneres von acht überprüften Empfehlungen eine umsetzte, vier teilweise umsetzte und drei nicht umsetzte,
- das Bundeskriminalamt von vier überprüften Empfehlungen zwei teilweise umsetzte und zwei nicht umsetzte sowie
- das Bundesministerium für Justiz von fünf überprüften Empfehlungen zwei umsetzte, eine teilweise umsetzte und zwei nicht umsetzte.

Umsetzungsgrad der Empfehlungen des Vorberichts Reihe Bund 2021/23					
Vorbericht		Nachfrage-verfahren	Follow–up–Überprüfung		
TZ	Empfehlungsinhalt	Status	TZ	Umsetzungsgrad	
Bundesministerium für Inneres					
9	Eine zwischen dem Innen– und dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität wäre – auch im Hinblick auf das Regierungsprogramm 2020–2024 – zu entwickeln und konsequent zu verfolgen.	nicht umgesetzt	3	teilweise umgesetzt	
4	Gemeinsam mit dem Bundesministerium für Justiz wären jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können.	nicht umgesetzt	4	nicht umgesetzt	
39	Alle mit kriminalpolizeilichen Ermittlungen befassten Organisationseinheiten des Bundeskriminalamts wären umfassend in die zentrale Applikation Protokollieren, Anzeigen, Daten (PAD) einzubinden, um einen vollständig automationsunterstützten Informations– bzw. Aktenaustausch mit den nachgeordneten Polizeidienststellen wie auch mit den Staatsanwaltschaften sicherzustellen.	teilweise umgesetzt	5	teilweise umgesetzt	
47	Es wäre ein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, einer vollständigen Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel einzurichten.	teilweise umgesetzt	6	nicht umgesetzt	
26	Die Organisation – vor allem im Bereich des Cybercrime Competence Centers – und die Prozesse im Bereich der Bekämpfung von Cyberkriminalität wären auf Basis bestehender Konzepte weiterzuentwickeln bzw. der veränderten Kriminalitätslandschaft anzupassen.	teilweise umgesetzt	7	nicht umgesetzt	
30	In Zusammenarbeit mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport wären Rahmenbedingungen im Sinne eines modernen Personalmanagements (Personalrekrutierung, –entwicklung und –bindung) zu schaffen, die es ermöglichen, dass allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung steht.	teilweise umgesetzt	9	umgesetzt	

Umsetzungsgrad der Empfehlungen des Vorberichts Reihe Bund 2021/23					
Vorbericht		Nachfrage-verfahren	Follow–up–Überprüfung		
TZ	Empfehlungsinhalt	Status	TZ	Umsetzungsgrad	
37	Angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen wären zu schaffen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Ministeriums die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen.	nicht umgesetzt	10	teilweise umgesetzt	
35	Es wäre sicherzustellen, dass alle ermittelnden Bediensteten über das für ihre Tätigkeit notwendige Basiswissen in den Bereichen IT und Cyberkriminalität verfügen; diese Themen wären daher verstärkt in der Fortbildung zu berücksichtigen.	teilweise umgesetzt	11	teilweise umgesetzt	
Bundeskriminalamt					
27	Die Organisation und Zuständigkeiten innerhalb des Bundeskriminalamts für die Bearbeitung von Cyberkriminalität wären im Hinblick auf die gestiegene Bedeutung technischer Ermittlungsansätze und Expertise unter Berücksichtigung eines Ausbildungs– und Personalkonzepts zu verbessern und eindeutig festzulegen.	zugesagt	7	nicht umgesetzt	
28	Zur Bemessung des Personaleinsatzes im Cybercrime Competence Center wären – unter Bedachtnahme auch auf zukünftige Aufgaben und Organisationsstrukturen – Kriterien zu entwickeln, die Annahmen zu dokumentieren und laufend zu evaluieren.	nicht umgesetzt	8	teilweise umgesetzt	
16	Das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität wäre fertigzustellen, dessen Anwendung sicherzustellen und in der Folge die Ausbildung der Präventionsbediensteten fortzuführen.	zugesagt	12	nicht umgesetzt	
19	Das Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität wäre weiterzuverfolgen, die Ergebnisse wären in der Folge zu verwerten und umzusetzen.	nicht umgesetzt	13	teilweise umgesetzt	
Bundesministerium für Justiz					
10	Eine zwischen dem Innen– und dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität wäre – auch im Hinblick auf das Regierungsprogramm 2020–2024 – zu entwickeln und konsequent zu verfolgen.	nicht umgesetzt	3	teilweise umgesetzt	
4	Gemeinsam mit dem Bundesministerium für Inneres wären jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können.	nicht umgesetzt	4	nicht umgesetzt	
47	Es wäre ein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, einer vollständigen Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel einzurichten.	teilweise umgesetzt	6	nicht umgesetzt	
43	Basierend auf internationalen Beispielen und den Erfahrungen besonders betroffener Staatsanwaltschaften wären organisatorische Rahmenbedingungen für eine spezialisierte Bearbeitung von Ermittlungsverfahren im Bereich Cyberkriminalität festzulegen.	teilweise umgesetzt	14	umgesetzt	

Umsetzungsgrad der Empfehlungen des Vorberichts Reihe Bund 2021/23					
Vorbericht		Nachfrage-verfahren	Follow–up–Überprüfung		
TZ	Empfehlungsinhalt	Status	TZ	Umsetzungsgrad	
44	Damit alle mit Cyberkriminalität befassten Bediensteten der Staatsanwaltschaften über das für eine effiziente Fallbearbeitung notwendige technische Grundwissen verfügen, wäre ein Aus– und Fortbildungskonzept zu erarbeiten und umzusetzen, das Schulungsangebot auszuweiten und der selbstständige Wissenserwerb und –transfer zu unterstützen. Diesbezüglich wäre verstärkt mit dem Bundesministerium für Inneres zusammenzuarbeiten.	teilweise umgesetzt	15	umgesetzt	

Anknüpfend an den Vorbericht hob der RH folgende Empfehlungen hervor:

Bundesministerium für Inneres; Bundesministerium für Justiz

(1) Eine zwischen dem Bundesministerium für Inneres und dem Bundesministerium für Justiz abgestimmte Strategie für den Bereich Cyberkriminalität wäre zu entwickeln und konsequent zu verfolgen. (TZ 3)

(2) Gemeinsam wären jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können. (TZ 4)

(3) Ein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, vollständiger Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel wäre einzurichten. (TZ 6)

Bundesministerium für Inneres

(4) Alle mit kriminalpolizeilichen Ermittlungen befassten Organisationseinheiten des Bundeskriminalamts wären umfassend in die zentrale Applikation Protokollieren, Anzeigen, Daten (PAD) einzubinden, um Doppelgleisigkeiten zu vermeiden, die Praktikabilität sicherzustellen und einen vollständig automationsunterstützten Informations– bzw. Aktenaustausch mit den nachgeordneten Polizeidienststellen wie auch mit den Staatsanwaltschaften sicherzustellen. (TZ 5)

(5) Das Projekt zur Schaffung einer IKT–Lösung für besondere kriminalpolizeiliche Ermittlungen wäre zu konkretisieren und sukzessive umzusetzen, um damit eine stabile IKT–Grundlage für die Kriminaldienstreform 2.0 gewährleisten zu können. (TZ 6)

(6) Die Organisation – vor allem im Bereich des Cybercrime Competence Centers – und die Prozesse im Bereich der Bekämpfung von Cyberkriminalität wären auf Basis bestehender Konzepte weiterzuentwickeln bzw. der veränderten Kriminalitätslandschaft anzupassen. (TZ 7)

(7) Die „Richtverwendungen für IT–Sonderverträge des Bundes“ wären in Abstimmung mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport regelmäßig auf ihre Aktualität zu überprüfen. Die Richtverwendungen sollten jedenfalls geeignete Rahmenbedingungen schaffen, um den mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten geeignetes Personal mit den nötigen technischen bzw. IT–Kenntnissen bedarfsgerecht zur Verfügung zu stellen. (TZ 9)

(8) Es wären – insbesondere im Bereich des Landeskriminalamts Wien – angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen zu schaffen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Bundesministeriums für Inneres die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen. (TZ 10)

(9) Die Schritte zur Stärkung der Prävention und Bekämpfung von Cyberkriminalität wären sukzessive umzusetzen, die gesetzten Maßnahmen regelmäßig auf ihre Zielerreichung zu überprüfen und gegebenenfalls anzupassen sowie strategische Überlegungen zum Personalbedarf miteinfließen zu lassen. (TZ 10)

(10) Die im Zuge der Kriminaldienstreform 2.0 geplanten Cybercrime–Training–Center wären zeitnah einzurichten, um allen ermittelnden Bediensteten die für ihre Tätigkeit notwendigen Basisfähigkeiten in den Bereichen IT und Cyberkriminalität vermitteln zu können. (TZ 11)

Bundeskriminalamt

(11) Die Änderung der Organisation und der Zuständigkeiten für die Bearbeitung von Cyberkriminalität wäre im Hinblick auf die gestiegene Bedeutung technischer Ermittlungsansätze und Expertise unter Berücksichtigung des bereits erstellten Personalkonzepts und in Abstimmung mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport zeitnah umzusetzen. (TZ 7)

(12) Kriterien zur Bemessung des Personaleinsatzes im Cybercrime Competence Center wären – unter Bedachtnahme auch auf zukünftige Aufgaben und Organisationsstrukturen – zu entwickeln, die Annahmen zu dokumentieren und laufend zu evaluieren. (TZ 8)

(13) Es wäre das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität fertigzustellen, seine Anwendung sicherzustellen und in der Folge die Ausbildung der Präventionsbediensteten entsprechend fortzuführen. (TZ 12)

(14) Der in der Präventionsstrategie „Sicheres Internet“ des Bundesministeriums für Inneres vorgesehene Maßnahmenplan sowie die konkreten darauf aufbauenden Maßnahmen wären zu erarbeiten; eine Wirkungs– und Erfolgsmessung wäre wissenschaftlich begleitet zu entwickeln und einzusetzen. (TZ 13)

Bundesministerium für Justiz

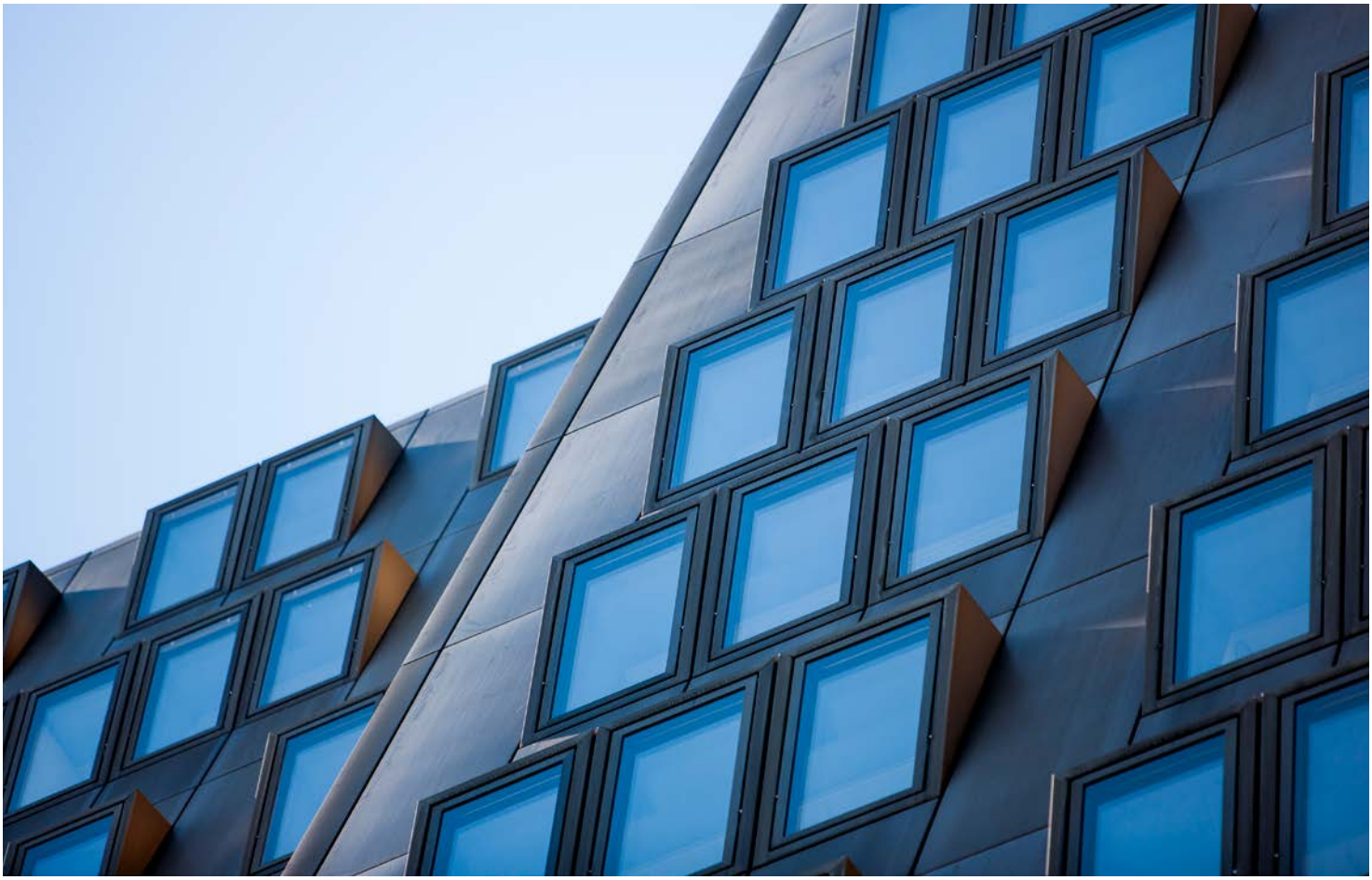
(15) Der Probebetrieb der Kompetenzstellen Cybercrime bei den Staatsanwaltschaften wäre fortzusetzen, zu evaluieren und nach allfällig notwendigen Anpassungen in den Regelbetrieb überzuleiten. (TZ 14)

(16) Der geplante, vertiefende Lehrgang zu Cyberkriminalität wäre zeitnah umzusetzen, um insbesondere Staatsanwältinnen und Staatsanwälten der Kompetenzstellen Cybercrime eine angemessene Fortbildung zu ermöglichen. (TZ 15)

Rechnungshof Österreich

Wien, im Juni 2024
Die Präsidentin:

Dr. Margit Kraker



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-10-23T17:58:44+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	