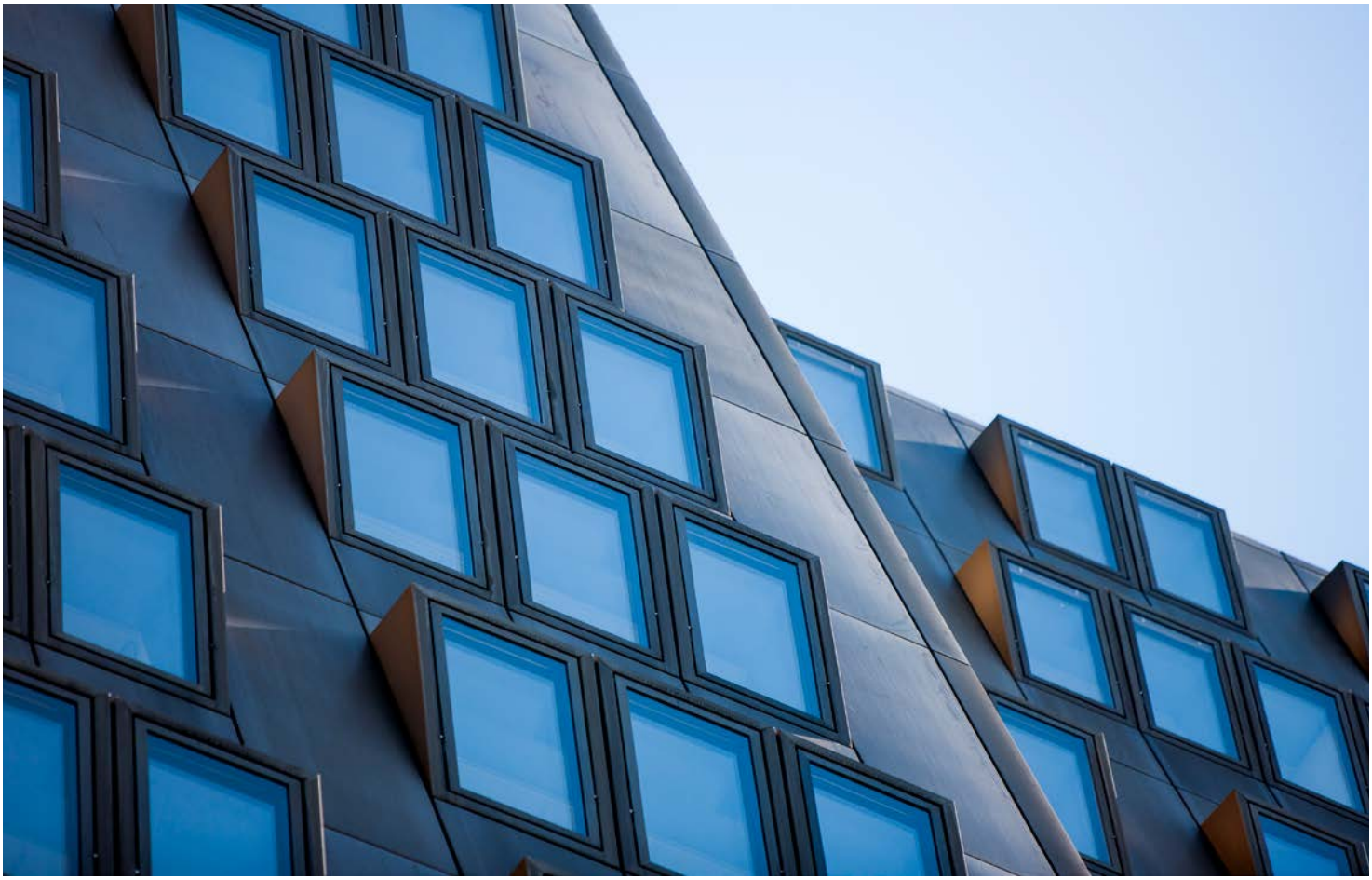
Rechnungshof Österreich

Unabhängig und objektiv für Sie.

Prävention und Bekämpfung von Cyberkriminalität

Reihe BUND 2021/23

Bericht des Rechnungshofes



III–335 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP
Rechnungshof GZ 004.766/010–P3/21

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
1031 Wien, Dampfschiffstraße 2
www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im Juni 2021

AUSKÜNFTE

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

FOTOS

Cover: Rechnungshof/Achim Bieniek

Inhaltsverzeichnis

Abkürzungsverzeichnis 5

Glossar 7

Prüfungsziel 11

Kurzfassung 11

Zentrale Empfehlungen 17

Zahlen und Fakten zur Prüfung 18

Prüfungsablauf und –gegenstand 21

Grundlagen zu Cyberkriminalität 22
- Allgemeines und Definition 22
- Rechtlicher Rahmen 24

Daten(–basis) zu Cyberkriminalität 25
- Statistische Erfassung Cyberkriminalität 25
- Zusammenhang der Daten von Polizei und Justiz 30

Strategie und Wirkungsziele 37
- Strategische Grundlagen 37
- Regierungsprogramme 39
- Strategie im Innenministerium 40
- Strategie im Justizministerium 42
- Wirkungsziele 44

TEIL 1
PRÄVENTION 47

Allgemeines 47

Polizeiinspektionen sowie Bezirks– und Stadtpolizeikommanden 49

Landeskriminalämter 52

Bundeskriminalamt 55

TEIL 2
BEKÄMPFUNG 60

Organisation und Personaleinsatz im Innenministerium 60
- Aufbau und Zuständigkeiten 60
- Bezirks–IT–Ermittlerinnen und –Ermittler 62
- Assistenzbereiche IT–Beweissicherung der Landeskriminalämter 66
- Cybercrime Competence Center im Bundeskriminalamt 72
- Koordinierung der Auskunftsverlangen an Anbieter von Kommunikationsdiensten 84

Aus– und Fortbildung im Innenministerium ____ 86
Ausbildung generell ____ 86
Ausbildung im Bereich Cyberkriminalität ____ 87
Fortbildung ____ 91

Technische Unterstützung im Innenministerium ____ 94
Infrastruktur ____ 94
Infrastruktur der Bezirks–IT–Ermittlerinnen und –Ermittler und der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter ____ 94
Kriminalpolizeiliche Infrastruktur ____ 97
Aktenführung und –übermittlung an die Staatsanwaltschaft ____ 100
Lagebild Cyberkriminalität ____ 101

Organisation und Personaleinsatz im Justizministerium ____ 103
Zusammenwirken Kriminalpolizei und Justiz bei der Verfolgung von Cyberkriminalität ____ 103
Zuständigkeiten für Ermittlungsverfahren im Bereich Cyberkriminalität ____ 104
Organisation der Staatsanwaltschaften in Cyberkriminalität–Ermittlungsverfahren ____ 106

Aus– und Fortbildung Justizministerium ____ 109

Digitale Forensik und Datenanalyse – Innenministerium und Justizministerium ____ 111
Allgemeines ____ 111
Analysesoftware ____ 111
Elektronische Beweismittel, Datenaustausch und –archivierung ____ 114

Resümee ____ 117

Schlussempfehlungen ____ 119

Anhang ____ 126

Tabellenverzeichnis

Tabelle 1:	Kategorisierung von Cyberkriminalität in der Polizeilichen Kriminalstatistik	26
Tabelle 2:	Polizeiliche Anzeigen im Bereich Cyberkriminalität (Polizeiliche Kriminalstatistik)	27
Tabelle 3:	Gerichtliche Verurteilungen wegen Computerkriminalität (Cyberkriminalität im engeren Sinn)	28
Tabelle 4:	Vergleich zwischen polizeilichen Anzeigen und Aktenanfall bei den Staatsanwaltschaften	31
Tabelle 5:	Maßnahmen im Regierungsprogramm 2020–2024 für das Innenministerium im Hinblick auf Cyberkriminalität	39
Tabelle 6:	Maßnahmen im Regierungsprogramm 2020–2024 für das Justizministerium im Hinblick auf Cyberkriminalität	40
Tabelle 7:	Globalbudget: Maßnahme, Kennzahlen und Meilensteine im Wirkungsbereich des Bundeskriminalamts im Hinblick auf Cyberkriminalität	45
Tabelle 8:	Präventionsbedienstete für Cyberkriminalität in den Bezirks– und Stadtpolizeikommanden	50
Tabelle 9:	Präventionsmaßnahmen bei den Bezirks– und Stadtpolizeikommanden im Bereich Cyberkriminalität	50
Tabelle 10:	Ausgebildete Präventionsbedienstete für Cyberkriminalität in den Landeskriminalämtern	53
Tabelle 11:	Präventionsmaßnahmen bei den Landeskriminalämtern im Bereich Cyberkriminalität	53
Tabelle 12:	Bezirks–IT–Ermittlerinnen und –Ermittler in Österreich	62
Tabelle 13:	Aufgaben der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter	67
Tabelle 14:	Grundkonzept des Cybercrime Competence Centers zur Bekämpfung von Cyberkriminalität	74
Tabelle 15:	Personalstand des Cybercrime Competence Centers	80
Tabelle 16:	Zeitliche Entwicklung der Ausbildung Bezirks–IT–Ermittlerinnen und –Ermittler	87
Tabelle 17:	Zeitliche Entwicklung der Ausbildungskonzepte Assistenzbereiche IT–Beweissicherung der Landeskriminalämter und des Cybercrime Competence Centers	89

Abbildungsverzeichnis

Abbildung 1:	Vergleich der polizeilichen Anzeigen und der personenbezogenen Erledigungen durch die Justiz (Cyberkriminalität im engeren Sinn), 2016 bis 2019	33
Abbildung 2:	Bekämpfung von Cyberkriminalität – wesentliche Organisationseinheiten des Innenministeriums und deren Aufgaben	61
Abbildung 3:	Struktur des Cybercrime Competence Centers	72
Abbildung 4:	Zuständigkeitsverteilung für Cyberkriminalität (im engeren Sinn) im Ermittlungsverfahren der Staatsanwaltschaften	105

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BAKS	Büroautomations– und Kommunikationssystem
BGBl.	Bundesgesetzblatt
BMI	Bundesministerium für Inneres
BMJ	Bundesministerium für Justiz
bzw.	beziehungsweise
d.h.	das heißt
EliAs	Elektronische integrierte Assistenz
ERV	Elektronischer Rechtsverkehr
etc.	et cetera
EU	Europäische Union
EUR	Euro
Eurojust	European Union Agency for Criminal Justice Cooperation (Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen)
Europol	Europäisches Polizeiamt
(f)f.	folgend(e)
GmbH	Gesellschaft mit beschränkter Haftung
GP	Gesetzgebungsperiode
Hrsg.	Herausgeber
i.d.(g.)F.	in der (geltenden) Fassung
IKDA	Integrierte Kriminalpolizeiliche Datenanwendung
IKT	Informations– und Kommunikationstechnik
IP	Internetprotokoll
IT	Informationstechnologie
Mio.	Million(en)
Mrd.	Milliarde(n)
PAD	Protokollieren, Anzeigen, Daten
PC	Personal Computer

rd.	rund
RH	Rechnungshof
S.	Seite
SPG	Sicherheitspolizeigesetz
SPOC	Single Point of Contact
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TZ	Textzahl(en)
u.a.	unter anderem
vgl.	vergleiche
VJ	Verfahrensautomation Justiz
WKStA	Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption
Z	Ziffer
z.B.	zum Beispiel

Glossar

Cybermobbing

Der Begriff Cybermobbing bezeichnet das absichtliche und über einen längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen von Personen über digitale Medien (z.B. über soziale Netzwerke oder in Videoportalen) (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

Cybergrooming

Bei Cybergrooming 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. Die Erwachsenen geben sich dabei oft als etwa gleichaltrige Nutzerinnen bzw. Nutzer aus (vgl. www.bundeskriminalamt.at sowie www.saferinternet.at[1]).

Darknet

Große Teile des Internets sind für übliche Suchmaschinen nicht zugänglich. Diese zeigen oft nur Inhalte des offenen Internets (Clearweb) an. Um in das Darknet zu gelangen, benötigt man spezielle Browser. Daten im Darknet werden anonym und verschlüsselt über verschiedene Server geschickt. Das Spektrum an illegalen Aktivitäten im Darknet reicht vom Drogen– und Waffenhandel über Dokumentenfälschung, Geldfälschung, Datenhandel bis hin zur Kinderpornografie und weit darüber hinaus (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

DDoS Attacke

Unter DDoS (Distributed Denial of Service; auf Deutsch: Verweigerung des Dienstes) versteht man einen verteilten Angriff auf einen Computer mit dem erklärten Ziel, die Verfügbarkeit außer Kraft zu setzen (vgl. www.computerlexikon.com).

Digitale Forensik (IT–Forensik)

Spuren auf digitalen Geräten werden bis zur Quelle nachverfolgt und so gesichert, dass sie als Beweismittel in einem Strafverfahren vor Gericht eingesetzt werden können. Die wissenschaftlich–methodischen Grundlagen dafür bilden den Kern der digitalen Forensik. Diese wird überall dort eingesetzt, wo digitale Daten Ziel, Mittel oder Katalysator eines Strafdelikts sind (vgl. Website der Hochschule für angewandte Wissenschaften Albstadt–Sigmaringen in Baden–Württemberg, www.hs-albsig.de bzw. dortige Beschreibung des Masterstudiengangs Digitale Forensik).

[1] alle im Glossar genannten Web–Adressen abgerufen am 26. August 2020

Hacking

Hacking bezeichnet ein unerlaubtes Eindringen in ein fremdes Computersystem. Hacken ist strafbar, wenn jemand Sicherheitsvorkehrungen des Systems verletzt oder überwindet, um sich einen Vermögensvorteil zu verschaffen oder die Betreiberin bzw. den Betreiber des Systems zu schädigen, z.B. durch Auskundschaften von Betriebsgeheimnissen (vgl. www.oesterreich.gv.at).

Kryptowährung

Die Grundidee von Kryptowährungen ist es, dezentrale Währungen zu schaffen, die ohne Zentralbanken und andere Finanzintermediäre – wie Banken, Kreditkartenunternehmen, Zahlungsverkehrsdienstleister – auskommen können.

Kryptowährungen sind digitale (Quasi–)Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem (vgl. Website der Universität Klagenfurt, www.aau.at sowie Gabler Wirtschaftslexikon, wirtschaftslexikon.gabler.de).

Love Scam

Beim sogenannten Love Scam handelt es sich um eine Form des Betrugs. Das spätere Opfer wird in eine Affäre verwickelt und in weiterer Folge unter dem Vorwand einer Notsituation finanziell geschädigt. Die Kontaktaufnahme erfolgt oftmals auf Social Media–Portalen (vgl. www.bundeskriminalamt.at).

OSINT

Open Source Intelligence (OSINT) befasst sich mit der Gewinnung von Informationen, die über offene Quellen frei verfügbar im Internet zu finden sind. Diese Daten werden für weitere Ermittlungen und Analysen herangezogen, um gezielte Erkenntnisse daraus herzuleiten (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

Phishing

Der Begriff Phishing setzt sich aus den englischen Wörtern password und fishing zusammen (auf Deutsch: nach Passwörtern angeln). Es wird dabei versucht, über gefälschte Webseiten, E–Mails oder Kurznachrichten an persönliche Daten zu gelangen. Phishing steht häufig in Zusammenhang mit (zumindest versuchten) Betrugshandlungen und Identitätsmissbrauch (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegelds (auf Englisch: ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung (vgl. Deutsches Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT–Sicherheit in Deutschland 2019).

Sextortion

Der Begriff Sextortion setzt sich aus den englischen Wörtern sex und extortion (auf Deutsch: Erpressung) zusammen und 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 (vgl. www.bundeskriminalamt.at sowie Website der Deutschen Polizeiberatung, www.polizei–beratung.de).

Spam

Spam bezeichnet elektronische, unerwünschte Nachrichten, die massenhaft und ungezielt über verschiedene Kommunikationsdienste verbreitet werden. Teilweise beinhaltet Spam in harmlosen Varianten unerwünschte Werbung. Häufig jedoch enthält Spam auch Schadsoftware im Anhang, Links zu infizierten Webseiten oder wird für Phishing–Angriffe genutzt (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

Trojanisches Pferd (Trojaner)

Als Trojanisches Pferd bezeichnet man ein Computerprogramm oder eine Applikation, das bzw. die als nützliche oder harmlose Anwendung getarnt ist, im Hintergrund aber ohne Wissen der Anwenderin bzw. des Anwenders eine andere, meist schädliche Funktion erfüllt (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

Wallet

Ein Wallet (englisch für Geldbeutel) ist eine virtuelle Geldtasche, in der Benutzerinnen und Benutzer Kryptowährungen „aufbewahren“. Insofern kann ein Wallet mehrere unterschiedliche Kryptowährungen beinhalten. Darüber hinaus gibt es unterschiedliche Arten von Wallets (vgl. Bundesministerium für Inneres, Lagebericht Cyberkriminalität 2018).

WIRKUNGSBEREICH

- Bundesministerium für Inneres
- Bundesministerium für Justiz

Prävention und Bekämpfung von Cyberkriminalität

Prüfungsziel

Der RH überprüfte zwischen November 2019 und Juli 2020 das Thema Cyberkriminalität. Prüfungsziele waren die Beurteilung der Datengrundlagen zu Cyberkriminalität einschließlich der dazu bestehenden Strategien von Innen– und Justizministerium, insbesondere aber die Beurteilung der Prävention und Bekämpfung von Cyberkriminalität in Bezug auf Organisation und Zusammenarbeit von Kriminalpolizei und Justiz sowie Ressourceneinsatz. Der überprüfte Zeitraum umfasste die Jahre 2016 bis 2019. Soweit erforderlich nahm der RH auch auf frühere und aktuellere Entwicklungen Bezug. Wegen der COVID–19–Pandemie musste der RH seine Prüfung von Mitte März bis Mitte Mai 2020 unterbrechen.

Kurzfassung

Ausgangslage und Daten

Cyberkriminalität nimmt seit vielen Jahren kontinuierlich und rasch zu. Die durch Cyberkriminalität verursachten Gefahren und Schäden betreffen Bürgerinnen und Bürger gleichermaßen wie Wirtschaft und staatliche Institutionen. Die Kosten und Schäden durch Cyberkriminalität steigen stetig. Internationale Erhebungen gingen von einem weltweiten Schaden von rd. 600 Mrd. US–Dollar im Jahr 2017 aus. Der Schaden in Österreich dürfte laut Wirtschaftskammer Österreich pro Jahr mehrere 100 Mio. EUR ausmachen. Zu den negativen finanziellen kommen die immateriellen Folgen (Cybermobbing, Verhetzung, Hass im Netz) dazu. (TZ 2, TZ 48)

Insbesondere seit der im Frühjahr 2020 aufgetretenen COVID–19–Pandemie war die klassische Kriminalität in Österreich rückläufig, während Cyberkriminalität (z.B. durch Hackerangriffe, Ausnutzung von technischen Sicherheitslücken) verstärkt anstieg. Das Innenministerium traf in den letzten Jahren zwar Maßnahmen auf den wesentlichen Organisationsebenen und schuf damit die Grundlage für Prävention

und Bekämpfung von Cyberkriminalität. Es bestand aber Verbesserungspotenzial vor allem bei der Prävention, beim Personal und der Organisation. Das Justizministerium befand sich bei der Bekämpfung von Cyberkriminalität noch im Anfangsstadium. Insbesondere bei der Organisation und Aus– bzw. Fortbildung bei Staatsanwaltschaften bestand Aufholbedarf. (TZ 2, TZ 48)

Im Jahr 2019 verdoppelte sich in Österreich die Zahl der Cyberkriminalität–Anzeigen im Vergleich zum Jahr 2016 auf 28.439. Die Gesamtzahl z.B. der Bediensteten der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter stieg im gleichen Zeitraum lediglich von 73 auf 85 Vollzeitäquivalente. Polizei, Staatsanwaltschaften und Gerichte sind bei der Bekämpfung von Cyberkriminalität mit wachsenden Anforderungen konfrontiert; dies betrifft die Anwendung des IT–Strafrechts, die digitale Beweismittelsicherung sowie die Ermittlungstaktik und Kriminaltechnik. Die Aufklärungsquote sank von 2010 bis 2019 von 55,3 % auf 35,8 %. (TZ 2, TZ 23)

Für Cyberkriminalität bestanden keine einheitlichen, zwischen Innen– und Justizministerium abgestimmten Begriffsbestimmungen, was die Bekämpfung von Cyberkriminalität erschwerte. Die Justiz verfügte über keine offiziellen Zahlen zur Tätigkeit der Staatsanwaltschaften im Bereich Cyberkriminalität. Es waren lediglich Zahlen zu gerichtlichen Verurteilungen, die aber auch nur Cyberkriminalität im engeren Sinn (kriminelle Handlungen infolge digitaler Angriffe auf Daten und Computersysteme) umfassten, vorhanden. Mit der Polizeilichen Kriminalstatistik vergleichbare Daten oder Statistiken fehlten. Damit fehlten wesentliche Grundlagen für umfassende Aussagen zu Cyberkriminalität – etwa zum Internetbetrug – und daraus abzuleitende Maßnahmen. (TZ 4)

Eine Gegenüberstellung der Zahl polizeilicher Anzeigen und ermittelter Tatverdächtiger mit Erledigungen der Justiz war auf Basis von Auswertungen der zur Verfahrensunterstützung eingesetzten Applikationen der Justiz lediglich für die der Cyberkriminalität im engeren Sinn zuordenbaren Delikte möglich. Für die Jahre 2016 bis 2019 zeigte sich, dass den rd. 16.900 polizeilichen Anzeigen und rd. 6.700 bei den Staatsanwaltschaften angefallenen Ermittlungsakten mit bekannter Täterschaft rd. 1.000 Verurteilungen (und rd. 550 Diversionen) gegenüberstanden. (TZ 5)

Die von der Justiz zur Unterstützung bei der Führung von Strafverfahren eingesetzten Applikationen waren allerdings nicht oder nur sehr eingeschränkt geeignet, zuverlässige Daten zum Kriminalitätsgeschehen, auch im Hinblick auf Cyberkriminalität, zu gewinnen. Es bestand kein aussagefähiger Zusammenhang zwischen der Polizeilichen Kriminalstatistik und den Zahlen aus den Auswertungen der Justizanwendungen. Es war nicht systematisch nachverfolgbar, wie Staatsanwaltschaften und Gerichte die polizeilichen Anzeigen weiterbehandelten und erledigten. Grundlagen, um die speziell bei Cyberkriminalität große Differenz zwischen der Zahl angezeigter Tatverdächtiger und der Zahl der Anklagen und Verurteilungen aufzuklären,

fehlten. Ein klarer und umfassender Überblick zum Phänomen Cyberkriminalität war damit nicht vorhanden, was die strategische Planung und Ressourcensteuerung erschwerte. (TZ 5)

Strategie

Die strategische Ausrichtung des Innenministeriums in Bezug auf Cyberkriminalität ergab sich aus mehreren nebeneinander gültigen Dokumenten mit unterschiedlichem Detaillierungsgrad und ohne ressortübergreifende Maßnahmen. Die Umsetzung wesentlicher strategischer Ansätze fehlte. Das Innenministerium verfügte auch über keine eigenständige mit dem Justizministerium abgestimmte Cyberkriminalität–Strategie mit Meilensteinen, konkreten Zielen und den dazugehörigen Verantwortlichen. (TZ 9)

Auch das Justizministerium hatte noch keine Strategie zur Bekämpfung und Verfolgung von Cyberkriminalität implementiert oder sich dahingehend mit dem Innenministerium abgestimmt. Für den Bereich „Hass im Netz“ hatte es eine Expertengruppe eingesetzt, um ein Maßnahmenpaket – etwa zu legistischen Anpassungen von Straftatbeständen und Regeln zur Kostentragung – zu erarbeiten. Das Gesetzespaket ging Anfang September 2020 in Begutachtung und wurde am 10. Dezember 2020 vom Nationalrat beschlossen. (TZ 10)

Innenministerium

Prävention

Die Kriminalprävention war auch in Bezug auf Cyberkriminalität wesentlich, da die Deliktszahlen und die damit einhergehenden Schäden in den letzten Jahren – und auch seit der im Frühjahr 2020 aufgetretenen COVID–19–Pandemie – stiegen und sich die Bekämpfung und Aufklärung oftmals schwierig gestalteten. (TZ 12, TZ 13)

Insgesamt war jedoch der Präventionsbereich für Cyberkriminalität im Innenministerium verbesserbar: Auf Ebene der Bezirks– und Stadtpolizeikommanden gab es z.B. bundesweit lediglich 40 % (96 statt 243) der vorgesehenen Präventionsbediensteten für Cyberkriminalität. In den Landeskriminalämtern war kein eigener Präventionsbereich für Cyberkriminalität eingerichtet, obwohl dies aufgrund der zunehmenden Bedeutung von Cyberkriminalität wichtig wäre. Präventionsmaßnahmen betreffend Cyberkriminalität für Erwachsene – im Gegensatz zu jenen für Kinder und Jugendliche – waren noch im Aufbau. So konnte nicht sichergestellt werden, dass potenzielle Opfer, wie etwa Seniorinnen und Senioren, präventiv informiert werden. (TZ 14, TZ 15)

Das Bundeskriminalamt legte in seinen bundesweiten Vorgaben Cyberkriminalität als eigenen Präventionsbereich fest. Die Ausbildung von Präventionsbediensteten für diesen Bereich begann jedoch erst im Jahr 2019 und das entsprechende Curriculum war zur Zeit der Gebarungsüberprüfung noch nicht fertiggestellt. (TZ 16)

Bekämpfung

Nach einem Erlass des Innenministeriums waren in den Bezirks– und Stadtpolizeikommanden sogenannte Bezirks–IT–Ermittlerinnen und –Ermittler als Cyber–Spezialisten einzusetzen. Diese waren Exekutivbedienstete, die eine ergänzende Ausbildung absolviert hatten und zusätzliche Aufgaben übernahmen; organisatorisch waren sie nicht eigens abgebildet. Anfang 2020 gab es bundesweit 293 Bezirks–IT–Ermittlerinnen und –Ermittler. Damit standen im Durchschnitt nur drei Bezirks–IT–Ermittlerinnen und –Ermittler einem Bezirks– oder Stadtpolizeikommando zur Verfügung. (TZ 21)

Den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter kamen unterschiedliche Aufgaben im Bereich Cyberkriminalität zu. Vor allem die forensische Untersuchung und Auswertung technischer Geräte wie auch die fachliche Unterstützung der Bezirks–IT–Ermittlerinnen und –Ermittler sowie der Ermittlungsbereiche in den Landeskriminalämtern waren dabei wesentlich. Es wäre daher eine Organisationsstruktur zweckmäßig, die Flexibilität und somit eine adäquate Reaktionsmöglichkeit auf Entwicklungen im Ermittlungs– oder Forensikbereich ermöglicht. Zudem verfügten nicht alle mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten über die zweckmäßige personelle, technische und räumliche Ausstattung. (TZ 22, TZ 23, TZ 37)

Im Bundeskriminalamt war mit der Organisationseinheit Cybercrime Competence Center eine auf die Bekämpfung von Cyberkriminalität spezialisierte, zentrale Stelle eingerichtet. Das Cybercrime Competence Center legte mit einem Grundkonzept zur Bekämpfung von Cyberkriminalität umfassende Vorschläge hinsichtlich Organisation, Personal sowie Aus– und Fortbildung auf bundesweiter Ebene vor. Obwohl im Bereich Cyberkriminalität die Fallzahlen stark stiegen, reagierte das Innenministerium nicht adäquat. Die Umsetzung des Konzepts war offen. (TZ 26)

Die Personalrekrutierung, –entwicklung und –bindung im Bereich Cyberkriminalität stellte – auch aufgrund der Rahmenbedingungen, wie z.B. formelle Kriterien abseits der fachlichen Eignung, Gehaltsschema des öffentlichen Dienstes, Planstellenbewertungen, langwierige Aufnahmeprozesse, mangelnde Möglichkeiten für Quereinsteigende – eine große Herausforderung dar. Dies im Hinblick auf die hochspezifischen, von einer großen Bandbreite und starken Dynamik geprägten Anforderungen der digitalen Ermittlungsarbeit (digitale Forensik, Datenanalyse und

Informationsauswertung) bei der Bekämpfung von steigender Cyberkriminalität. (TZ 30)

Das Innenministerium hatte keine standardisierte Ausbildung für die Assistenzbereiche IT–Beweissicherung der Landeskriminalämter und des Cybercrime Competence Centers umgesetzt. Ein ganzheitliches, über alle Ebenen bedarfsabgestimmtes Ausbildungskonzept fehlte. (TZ 34)

Die Themen IT und Cyberkriminalität waren nur punktuell in einigen Fortbildungsschienen für die Bediensteten unterschiedlicher Organisationseinheiten und Hierarchieebenen berücksichtigt. Diese verfügten zum Teil aber nicht über das für ihre Tätigkeit notwendige IT– bzw. Cyberkriminalität–Basiswissen, obwohl dieses Wissen insbesondere bei den ermittelnden Bediensteten – angesichts der steigenden Bedeutung von Cyberkriminalität für nahezu alle Deliktsbereiche – essenziell war. (TZ 35)

Wesentlichen kriminalpolizeilichen Anforderungen konnte innerhalb der IT–Infrastruktur des Innenministeriums wegen restriktiver Sicherheitseinstellungen nicht entsprochen werden. Dies betraf bei der Bekämpfung von Cyberkriminalität die Speicherung von Ermittlungsdaten, die Auswertung und Analyse elektronischer Beweismittel oder uneingeschränkte Recherchen im Internet. Dadurch entstanden Insellösungen, bei denen eine ausreichende Kontrolle, Wartung und Servicierung durch die zuständigen Stellen des Innenministeriums, eine einheitliche Nutzung von Softwareanwendungen sowie die Datensicherheit nicht immer gewährleistet waren. Das Innenministerium arbeitete am Aufbau einer eigenständigen kriminalpolizeilichen Infrastruktur. (TZ 38)

Justizministerium

Die Staatsanwaltschaften waren im Hinblick auf die besonderen Herausforderungen bei der wirksamen Bekämpfung von Cyberkriminalität organisatorisch und methodisch nicht ausreichend gerüstet. Für die Ermittlungsverfahren galten die allgemeinen, in der Strafprozessordnung festgelegten Zuständigkeitsregeln. Auch innerhalb der Staatsanwaltschaften gab es keine Spezialisierung für Cyberkriminalität. (TZ 43)

Das Thema Cyberkriminalität wurde sowohl in der Ausbildung als auch in der Fortbildung der damit befassten Justizbediensteten nur rudimentär behandelt. Zudem waren technisches und IT–Wissen oder Informationen – etwa zu möglichen Ermittlungsansätzen im Bereich Cyberkriminalität – nicht Inhalt der Ausbildung. Dieses Wissen musste auch nicht verpflichtend durch Fortbildungen erworben werden. Damit war nicht gewährleistet, dass alle Bediensteten über den erforderlichen Wissensstand verfügten. Dies, obwohl vor allem bei Staatsanwaltschaften auch das technische und das IT–Verständnis eine entscheidende Rolle spielten, um in Ermitt-

lungsverfahren alle Möglichkeiten ausschöpfen und sowohl effizient als auch wirksam mit der Kriminalpolizei zusammenarbeiten zu können. (TZ 44)

Digitale Forensik und Datenanalyse – Innenministerium und Justizministerium

Die Sicherung, Aufbereitung und Auswertung von Daten bildeten bei Cyberkriminalität – wie auch in vielen anderen Kriminalitätsbereichen – grundlegende und wichtige Instrumente zur Ermittlung strafrechtlich relevanter Sachverhalte und zur gerichtlichen Verwertung elektronischer Beweismittel. Damit kam einer geeigneten technischen Unterstützung im Bereich der digitalen Forensik wie auch bei der Analyse der daraus gewonnenen Daten steigende Bedeutung zu. (TZ 47)

In der Praxis war der Austausch sichergestellter Daten zwischen Kriminalpolizei und Justiz aber nicht automationsunterstützt. Die Polizeidienststellen übermittelten der Staatsanwaltschaft – insbesondere wegen der bei der Justiz fehlenden Kapazitäten zur Archivierung und mangels gesicherter Übertragungswege – lediglich die wesentlichen aufbereiteten Ergebnisse und Beweismittel in Papierform oder mittels Datenträger. Die Staatsanwaltschaft schloss diese dann dem jeweiligen Ermittlungsakt physisch an. Die Verwahrung und Archivierung der sichergestellten Daten und elektronischen Beweismittel in ihrer Gesamtheit verblieben bei der Polizei. (TZ 47)

Eine gemeinsame Arbeitsgruppe erarbeitete im Jahr 2016 Vorschläge für eine interministerielle Datenaustauschplattform samt umfassender Archivierungslösung für elektronische Beweismittel. Diese Vorschläge wurden vom Innen– und Justizministerium jedoch nicht weiterverfolgt. Damit gab es weiterhin keinen automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten sowie keine zuverlässige und vollständige Dokumentation sämtlicher Bearbeitungsschritte. Eine lückenlose Dokumentation der Bearbeitung elektronischer Beweismittel war aber unerlässlich, um volle Beweiskraft zu sichern. (TZ 47)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

ZENTRALE EMPFEHLUNGEN

- Das Bundesministerium für Inneres und das Bundesministerium für Justiz sollten gemeinsam jene Delikte festlegen, 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)

- Eine zwischen dem Bundesministerium für Inneres und dem Bundesministerium für Justiz abgestimmte Strategie für den Bereich Cyberkriminalität wäre – auch im Hinblick auf das Regierungsprogramm 2020–2024 – zu entwickeln und konsequent zu verfolgen. (TZ 9 und TZ 10)

- Das Bundesministerium für Inneres sollte angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen schaffen, um allen mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Ministeriums die zeitgemäße und zweckmäßige Erfüllung ihrer Aufgaben zu ermöglichen. (TZ 37)

- Das Bundesministerium für Justiz sollte basierend auf internationalen Beispielen und den Erfahrungen besonders betroffener Staatsanwaltschaften organisatorische Rahmenbedingungen für eine spezialisierte Bearbeitung von Ermittlungsverfahren im Bereich Cyberkriminalität festlegen. (TZ 43)

- Damit alle mit Cyberkriminalität befassten Bediensteten der Staatsanwaltschaften über das für eine effiziente Fallbearbeitung notwendige technische Grundwissen verfügen, sollte das Bundesministerium für Justiz ein Aus– und Fortbildungskonzept erarbeiten und umsetzen, das Schulungsangebot ausweiten und den selbstständigen Wissenserwerb und –transfer unterstützen. Diesbezüglich wäre verstärkt mit dem Bundesministerium für Inneres zusammenzuarbeiten. (TZ 44)

Zahlen und Fakten zur Prüfung

Cyberkriminalität					
ausgewählte Rechtsgrundlagen	– Übereinkommen des Europarats 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. – Strafprozessordnung 1975 (StPO), BGBl. 631/1975 i.d.g.F. – Sicherheitspolizeigesetz (SPG), BGBl. 566/1991 i.d.g.F.				
Datenbasis	**2016**	**2017**	**2018**	**2019**	**Veränderung 2016 bis 2019**
	Anzahl				in %
polizeiliche Anzeigen Cyberkriminalität insgesamt (Fälle)	**13.103**	**16.804**	**19.627**	**28.439**	**117**
davon					
im engeren Sinn	*2.630*	*3.546*	*3.070*	*7.622*	*190*
im weiteren Sinn	*10.473*	*13.258*	*16.557*	*20.817*	*99*
davon					
Internetbetrug	*9.672*	*11.761*	*13.328*	*16.831*	*74*
Sonstige Kriminalität im Internet	*801*	*1.497*	*3.229*	*3.986*	*398*
Erledigungen der Staatsanwaltschaften (personenbezogen) zu Cyberkriminalität im engeren Sinn[1]	**1.594**	**1.971**	**2.082**	**2.507**	**57**
davon					
durch Anklage	*297*	*429*	*507*	*699*	*135*
durch Diversion	*67*	*105*	*106*	*114*	*70*
durch Einstellung	*850*	*1.054*	*1.011*	*1.152*	*36*
durch Abbrechung	*380*	*383*	*458*	*542*	*43*
Erledigungen der Gerichte zu Cyberkriminalität im engeren Sinn[1]	**234**	**289**	**361**	**518**	**121**
davon					
Verurteilung	*149*	*213*	*235*	*383*	*157*
Diversion	*51*	*41*	*71*	*85*	*67*
Freispruch	*34*	*35*	*55*	*50*	*47*
Prävention Cyberkriminalität					
Maßnahmen (z.B. Vorträge, Einzelberatungen)	489	734	1.635	2.272	365
beratene Personen	5.169	9.816	29.301	37.988	635

Cyberkriminalität						
Personal zur Bekämpfung von Cyber-kriminalität im Innenministerium	2016	2017	2018	2019	2020	Veränderung 2016 bis 2020
	in Köpfen zum 1. Jänner					in %
Bezirks–IT–Ermittlerinnen und –Ermittler[2]	–	–	–	–	293	–
	in Vollzeitäquivalenten zum 1. Jänner					
Landeskriminalämter (Aufgabenbereich IT–Beweissicherung)	73	78,5	85,8	81	85	16
Bundeskriminalamt (Cybercrime Competence Center)	39,5	41,8	52,5	62,8	63,5	61

[1] Daten zu Cyberkriminalität im weiteren Sinn bei der Justiz nicht auswertbar
[2] Daten nur für den Stichtag 1. Jänner 2020 verfügbar

Quellen: BMI; BMJ; Zusammenstellung: RH

Prüfungsablauf und –gegenstand

1 Der RH führte zwischen November 2019 und Juli 2020 eine Gebarungsüberprüfung zum Thema Cyberkriminalität durch. Prüfungshandlungen setzte er beim Bundesministerium für Inneres (in der Folge: **Innenministerium**), der Landespolizeidirektion und dem Landeskriminalamt Wien, dem Stadtpolizeikommando Ottakring in Wien, dem Bundesministerium für Justiz (in der Folge: **Justizministerium**) und der Staatsanwaltschaft Wien. Bei den Landespolizeidirektionen außer Wien führte der RH Erhebungen mittels Fragebogen durch. Gespräche zum Prüfungsgegenstand fanden beim Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und beim Bundeskanzleramt statt. Der Schwerpunkt der Prüfungshandlungen lag beim Innenministerium.

Ziele der Gebarungsüberprüfung waren die Beurteilung der Datengrundlagen zu Cyberkriminalität einschließlich der dazu bestehenden Strategien von Innen– und Justizministerium, insbesondere aber die Beurteilung der Prävention und Bekämpfung von Cyberkriminalität in Bezug auf Organisation und Zusammenarbeit von Kriminalpolizei und Justiz sowie Ressourceneinsatz.

Der überprüfte Zeitraum umfasste die Jahre 2016 bis 2019. Soweit erforderlich nahm der RH auch auf frühere bzw. aktuellere Entwicklungen Bezug. Infolge der COVID–19–Pandemie unterbrach der RH seine Prüfungshandlungen ab Mitte März 2020 und führte sie Mitte Mai 2020 weiter.

Zu dem im Jänner 2021 übermittelten Prüfungsergebnis nahmen das Justizministerium im März 2021 und das Innenministerium im April 2021 Stellung. Der RH erstattete seine Gegenäußerungen im Juni 2021.

Grundlagen zu Cyberkriminalität

Allgemeines und Definition

2 (1) In den letzten Jahren stieg die Nutzung von digitalen Geräten, der Informationstechnologie (**IT**) und des Internets massiv. Ende Mai 2020 gab es weltweit über 4 Mrd. Internetzugänge[2]. In Österreich hatten 89 % der Haushalte im Jahr 2018 einen Internetzugang, 57 % aller Personen im Alter zwischen 25 und 64 Jahren nutzten beruflich digitale Geräte und 88 % der Unternehmen waren mit einer Website im Internet vertreten.[3]

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 stetig. Internationale Erhebungen gingen von einem weltweiten Schaden von rd. 600 Mrd. US–Dollar im Jahr 2017 aus. Laut Wirtschaftskammer Österreich bedeutete das einen Schaden von mehreren 100 Mio. EUR in Österreich. Für Deutschland kam eine Untersuchung aus dem Jahr 2019 zu dem Ergebnis, dass sich der Schaden durch digitale Angriffe auf rd. 103 Mrd. EUR pro Jahr belaufe.[4]

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[5], Cybergrooming[6]), das Recht auf Schutz der Ehre und der persönlichen Integrität sowie den öffentlichen Frieden (z.B. Cybermobbing, Verleumdung, Verhetzung, „Hass im Netz“).

Im Jahr 2019 stieg in Österreich die Zahl der als Cyberkriminalitätsdelikte bezeichneten Fälle im Vergleich zum Vorjahr um rd. 45 % auf 28.439 angezeigte Delikte. Die Strafverfolgungsbehörden – Polizei, Staatsanwaltschaften und Gerichte – sind bei der Bekämpfung von Cyberkriminalität mit wachsenden Anforderungen im Hinblick auf die Anwendung des IT–Strafrechts, die digitale Beweismittelsicherung sowie die Ermittlungstaktik und Kriminaltechnik (Forensik) konfrontiert. Die Aufklärungsquote

[2] siehe Internet World Stats, World internet usage and population statistics (https://www.internetworldstats.com/stats.htm; abgerufen am 17. Juli 2020)

[3] Statistik Austria, IKT–Einsatz von Haushalten 2018, IKT–Einsatz in Unternehmen 2018

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

[5] 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.

[6] 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.

sank von 2010 bis 2019 von 55,3 % auf 35,8 %[7]. Die Verurteilungszahlen zu Cyberkriminalität sind gering, nähere Zahlen dazu sind unter TZ 4 dargestellt.

(2) Für das Phänomen bzw. den Begriff Cyberkriminalität gibt es keine allgemein gültige Definition. In Lehr– und Fachbüchern und auch im Innen– und Justizministerium – selbst innerhalb der Ressorts – werden unterschiedliche Begriffe wie Cyber–crime, Internetkriminalität, Computerkriminalität, Cyberkriminalität etc. verwendet. Dementsprechend inhomogen sind daher statistische Daten und Angaben (z.B. zu Schäden durch Cyberkriminalität).

Im polizeilichen Bereich ist die Unterscheidung zwischen Cybercrime im engeren Sinn und Cybercrime im weiteren Sinn gebräuchlich:

- Cybercrime im engeren Sinn (Informations– und Kommunikationstechnik (**IKT**) als Angriffsziel) umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der IKT begangen werden. Die Straftaten sind gegen die Netzwerke selbst oder gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet (z.B. Datenbeschädigung, Hacking, DDoS Angriffe).
- Cybercrime im weiteren Sinn (IKT als Tatmittel) umfasst Straftaten, bei denen die IKT als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird (z.B. Betrugsdelikte, Drogenhandel im Darknet, pornografische Darstellungen Minderjähriger im Internet, Cybergrooming oder Cybermobbing).

Der RH verwendet in der Folge grundsätzlich den Begriff Cyberkriminalität im engeren bzw. weiteren Sinn[8].

(3) Im Bereich Cyberkriminalität war auch die europäische und internationale Zusammenarbeit wesentlich. Sowohl das Innen– als auch das Justizministerium arbeiteten auf Basis unterschiedlicher Rechtsgrundlagen mit verschiedenen Akteuren zusammen, z.B. European Union Agency for Criminal Justice Cooperation (**Eurojust**) und European Cybercrime Centre beim Europäischen Polizeiamt (**Europol**). Ein Überblick über die wesentlichen internationalen Kooperationen des Innenministeriums findet sich im Anhang, Tabelle A.

[7] Die Gesamtaufklärungsquote lag im Vergleich dazu im Jahr 2019 bei 52,5 %.

[8] Davon zu unterscheiden sind (laut Definition der Österreichischen Strategie für Cyber Sicherheit)

- Cyber Sicherheit, die den Schutz eines zentralen Rechtsguts mit rechtsstaatlichen Mitteln vor akteursbezogenen, technischen, organisations– und naturbedingten Gefahren, die die Sicherheit des Cyber Space (inklusive Infrastruktur– und Datensicherheit) und die Sicherheit der Nutzerinnen und Nutzer im Cyber Space gefährden, beschreibt und
- Cyber Defence als Summe aller Maßnahmen zur Verteidigung des Cyber Raums mit militärischen und speziell dafür geeigneten Mitteln zur Erreichung militärstrategischer Ziele.

Rechtlicher Rahmen

3 Österreich unterzeichnete im November 2001 die Convention on Cybercrime – „Budapester Konvention" – des Europarats und ratifizierte sie im Jahr 2012[9]. Die Budapester Konvention dient als Leitlinie, um nationale Gesetze zu schaffen, und bietet einen Rahmen für die internationale Zusammenarbeit zwischen den Vertragsstaaten des Übereinkommens. Erfasst sind in erster Linie Handlungen gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computersystemen, Netzwerken und Computerdaten sowie der Missbrauch solcher Systeme und Daten; strafprozessuale Maßnahmen sollen harmonisiert bzw. das Rechtshilfesystem für länderüberschreitende Kooperationen verbessert werden.

Auf Ebene der Europäischen Union (**EU**) folgten weitere Richtlinien und Verordnungen, die Österreich in nationales Recht umsetzte bzw. unmittelbar anwendete. Anpassungen und Änderungen erfolgten in der Strafprozessordnung (**StPO**) und auch im materiellen Strafrecht z.B. durch Verankerung spezifischer Computerdelikte im Strafgesetzbuch (**StGB**). Die dynamische Entwicklung des Phänomens Cyberkriminalität und eine fehlende Definition bzw. schwierige Abgrenzung zeigen sich auch in der Strafgesetzgebung (z.B. zum Bereich „Hass im Netz"; ein Gesetzespaket dazu ging Anfang September 2020 in Begutachtung und wurde am 10. Dezember 2020 vom Nationalrat beschlossen).

Im Bereich Cyberkriminalität waren weiters z.B. das EU–Polizeikooperationsgesetz, das österreichische Auslieferungs– und Rechtshilfegesetz und die ergänzende Verordnung relevant.

[9] Das Übereinkommen über Computerkriminalität trat gemäß Art. 36 Abs. 4 Budapester Konvention für Österreich mit 1. Oktober 2012 in Kraft, BGBl. III 140/2012.

Daten(–basis) zu Cyberkriminalität

Statistische Erfassung Cyberkriminalität

4.1 (1) Öffentlich zugängliche statistische Daten zur Entwicklung von Cyberkriminalität fanden sich in der vom Innenministerium erstellten Polizeilichen Kriminalstatistik und im vom Justizministerium erstellten Sicherheitsbericht.

(2) Die Polizeiliche Kriminalstatistik zeigte Anzahl und Entwicklung der den Sicherheitsbehörden bekannt gewordenen gerichtlich strafbaren Handlungen differenziert nach Delikten und Deliktsgruppen.

Das Innenministerium ordnete in der Polizeilichen Kriminalstatistik einzelne Straftatbestände den zwei Kategorien Cyberkriminalität im engeren Sinn und Cyberkriminalität im weiteren Sinn zu, wobei es letztere zusätzlich in Internetbetrug und Sonstige Kriminalität im Internet trennte.[10] Die unter dem Begriff „Hass im Netz“ zunehmend im öffentlichen Blickfeld stehenden, über soziale Medien begangenen Straftaten der Verhetzung sowie der Aufforderung zu bzw. Gutheißung von mit Strafe bedrohten Handlungen und von terroristischen Straftaten[11] wurden nicht als Cyberkriminalität erfasst.

[10] Delikte im Bereich von Cyberkriminalität im weiteren Sinn galten mit Ausnahme der Kinderpornografie statistisch nur dann als solche, wenn dezidiert das Internet als Tatörtlichkeit erfasst war.

[11] §§ 282, 282a und 283 StGB

Im Detail erfolgte die Zuordnung der Straftaten nach verwirklichten Delikten wie in folgender Tabelle dargestellt:

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 – Cybermobbing (§ 107c StGB)[1] – Widerrechtlicher Zugriff auf ein Computersystem – Hacking (§ 118a StGB), z.B. Eindringen in ein Computersystem durch Überwindung von Passwörtern, gegebenenfalls im Vorfeld Phishing – Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)[1] – Missbräuchliches Abfangen von Daten (§ 119a StGB) – Datenbeschädigung (§ 126a StGB), z.B. Veränderung oder Löschung von Daten beim Eindringen in ein Computersystem – Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB), z.B. durch Computerviren, Trojaner oder DDoS–Attacken – Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB), z.B. Herstellung oder Beschaffung von Schadsoftware – Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB), Betrug an einer Maschine, z.B. unbefugtes Bezahlen mit fremder Bankomatkarte – Datenfälschung (§ 225a StGB)
Cyberkriminalität im weiteren Sinn	Internetbetrug	– Betrug, schwerer Betrug und gewerbsmäßiger Betrug (§§ 146 bis 148 StGB)
	Sonstige Kriminalität im Internet	– Erpressung bzw. schwere Erpressung (§§ 144 und 145 StGB), z.B. durch Ransomware oder Sextortion – Pornografische 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 und 224 StGB) – Urkundenunterdrückung (§ 229 StGB) – Gebrauch fremder Ausweise (§ 231 StGB) – Geldfälschung bzw. Fälschung unbarer Zahlungsmittel (§§ 232 und 241a StGB) – Verleumdung (§ 297 StGB) – Straftaten nach den §§ 3a ff. Verbotsgesetz

StGB = Strafgesetzbuch Quelle: BMI

[1] Delikt ab 2017 der Cyberkriminalität (im engeren Sinn) zugeordnet

Die Zahl der angezeigten Straftaten im Bereich Cyberkriminalität entwickelte sich gemäß der Polizeilichen Kriminalstatistik – aufgeschlüsselt nach Kategorien und innerhalb dieser nach den zahlenmäßig bedeutsamsten Delikten – in den Jahren 2016 bis 2019 wie folgt:

Tabelle 2: Polizeiliche Anzeigen im Bereich Cyberkriminalität (Polizeiliche Kriminalstatistik)

Kategorien und Delikte	2016	2017	2018	2019	Veränderung 2016 bis 2019
	Anzahl				in %
Cyberkriminalität im engeren Sinn	2.630[1]	3.546	3.070	7.622	190
davon					
Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)	*457*	*363*	*403*	*684*	*50*
Datenbeschädigung (§ 126a StGB)	*659*	*1.186*	*415*	*467*	*-29*
Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)	*817*	*1.056*	*1.415*	*5.537*	*578*
Cyberkriminalität im weiteren Sinn	10.473	13.258	16.557	20.817	99
davon					
Internetbetrug	*9.672*	*11.761*	*13.328*	*16.831*	*74*
Sonstige Kriminalität im Internet	*801*	*1.497*	*3.229*	*3.986*	*398*
davon					
Erpressung (§ 144 StGB)	*–*	*474*	*1.599*	*1.874*	*–*
Pornografische Darstellung Minderjähriger (§ 207a StGB)	*681*	*733*	*1.161*	*1.666*	*145*
Summe Cyberkriminalität	13.103[1]	16.804	19.627	28.439	117

StGB = Strafgesetzbuch Quelle: BMI

[1] Ohne §§ 107c und 119 StGB; diese wurden in der Polizeilichen Kriminalstatistik erst ab 2017 als Cyberkriminalität erfasst.

Eine vollständige Aufgliederung nach den einzelnen Delikten findet sich im Anhang, Tabelle B.

(3) Das Justizministerium veröffentlichte im Rahmen seines jährlichen Sicherheitsberichts Statistiken zu den Verurteilungen durch österreichische Gerichte differenziert nach Deliktsgruppen, wobei Computerkriminalität als eine Deliktsgruppe festgelegt war. Grundlage für die Darstellung bildete die von der Bundesanstalt „Statistik Österreich“ (in der Folge: **Statistik Austria**) anhand eines Auszugs aus dem Strafregister erstellte Gerichtliche Kriminalstatistik. Die vom Justizministerium der Computerkriminalität zugeordneten Delikte entsprachen im Wesentlichen der vom Innenministerium in der Polizeilichen Kriminalstatistik verwendeten Definition von Cyberkriminalität im engeren Sinn. Abweichend zu dieser fehlten aber Cybermobbing und die Verletzung des Telekommunikationsgeheimnisses. Eine mit der Polizei

vergleichbare umfassendere Definition für Cyberkriminalität – also auch eine solche „im weiteren Sinn“ – hatte das Justizministerium nicht festgelegt.

Die Zahl der gerichtlichen Verurteilungen wegen Computerkriminalität entwickelte sich wie folgt:[12]

Tabelle 3: Gerichtliche Verurteilungen wegen Computerkriminalität (Cyberkriminalität im engeren Sinn)

Delikt	2016	2017	2018	2019
	Anzahl			
Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)	2	1	2	6
Missbräuchliches Abfangen von Daten (§ 119a StGB)	0	0	0	1
Datenbeschädigung (§ 126a StGB)	5	3	7	8
Störung der Funktionsfähigkeit eines Computers (§ 126b StGB)	1	0	1	0
Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)	3	0	0	0
Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)	117	148	179	321
Datenfälschung (§ 225a StGB)	12	26	27	25
Summe Computerkriminalität	**140**	**178**	**216**	**361**

StGB = Strafgesetzbuch

Quellen: BMJ; Sicherheitsberichte; Statistik Austria

Öffentlich zugängliche Statistiken zu den im Bereich Cyberkriminalität bei den Staatsanwaltschaften geführten Ermittlungsverfahren bzw. bei den Gerichten durchgeführten Hauptverfahren gab es nicht.

4.2 Der RH kritisierte, dass für den Bereich Cyberkriminalität keine einheitlichen, zwischen Innen– und Justizministerium abgestimmten Begriffsbestimmungen bestanden, wodurch aus seiner Sicht eine abgestimmte Vorgehensweise zur Bekämpfung von Cyberkriminalität erschwert wurde. Die Justiz verfügte über keine offiziellen Zahlen zur Tätigkeit der Staatsanwaltschaften im Bereich Cyberkriminalität; es waren lediglich Zahlen zu gerichtlichen Verurteilungen vorhanden, die aber auch nur Cyberkriminalität im engeren Sinn umfassten. Mit der Polizeilichen Kriminalstatistik vergleichbare Daten bzw. Statistiken fehlten. Damit fehlten auch wesentliche Grundlagen für umfassende Aussagen zu Cyberkriminalität, z.B. zum Internetbetrug, und daraus abzuleitende Maßnahmen.

[12] Abweichungen zu der in den „Zahlen und Fakten zur Prüfung“ dieses Berichts dargestellten Gesamtzahl der Verurteilungen sind auf die unterschiedliche Datengrundlage zurückzuführen. Basis der Werte in „Zahlen und Fakten“ sind Auswertungen aus der Verfahrensautomation Justiz. Dort sind z.B. auch die in der offiziellen Verurteilungsstatistik fehlenden Delikte von Cyberkriminalität im engeren Sinn enthalten.

Der RH hielt weiters fest, dass weder das Innen– noch das Justizministerium die unter „Hass im Netz“ subsumierbaren Delikte als Cyberkriminalität erfasst hatte.

Der RH empfahl dem Innenministerium und dem 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) Laut Stellungnahme des Innenministeriums seien die Delikte, die unter den Begriff Cyberkriminalität zu subsumieren sind, durch die Trennung in „Cyberkriminalität im engeren Sinn“ sowie „Cyberkriminalität im weiteren Sinn“ ausreichend klar geregelt. Die statistische Erfassung erfolge dabei über die in regelmäßigen Abständen publizierte Polizeiliche Kriminalstatistik. Zielgerichteterweise weise die Polizeiliche Kriminalstatistik auch Cyberkriminalität im weiteren Sinn aus (z.B. Betrug versus Internetbetrug).

(2) Das Justizministerium führte in seiner Stellungnahme aus, dass die Empfehlung in ihrer Bedeutung zu relativieren sei. So weise die Polizeiliche Kriminalstatistik für 2019 als mengenmäßig größten Teil der Internetkriminalität den Internetbetrug mit 16.831 Anzeigen aus. Dem sei jedoch gegenüberzustellen, dass es 2019 insgesamt 43.887 Betrugsanzeigen gegeben habe. Das Delikt des Betrugs insgesamt zur Cyberkriminalität zu zählen, würde daher ebenso wenig Sinn machen, wie den Anteil an Cyberkriminalität an diesem Delikt einfach zu ignorieren. Es gehe also darum, ob bzw. inwieweit an bestimmte Formen der Cyberkriminalität spezifische Maßnahmen geknüpft werden sollten, wie etwa spezifische Behördenstrukturen, spezifische Präventionskonzepte bis hin zur spezifischen statistischen Erfassung.

Das Regierungsprogramm 2020–2024 weise dem Innenministerium die „Erstellung eines Strategiekonzepts zur verbesserten Bekämpfung von Cybercrime in Österreich“ zu. Die angesprochenen Fragen, und damit auch eine spezifische statistische Erfassung, könnten jedenfalls im Rahmen einer solchen Strategieentwicklung erörtert werden, an der sich das Justizministerium nach Maßgabe der zur Verfügung stehenden Ressourcen gerne beteiligen werde.

4.4 (1) Der RH entgegnete dem Innenministerium, dass dessen Argumentation einer ausreichend klaren Regelung lediglich die Sicht– und Vorgangsweise des Innenministeriums selbst bei der Definition und statistischen Erfassung von Cyberkriminalität im Blick hatte. Er betonte demgegenüber, dass nur auf Basis einer sowohl von der Polizei als auch von der Justiz einheitlich verwendeten Definition vergleichbare Zahlen erhoben und dargestellt werden können.

(2) Gegenüber dem Justizministerium verwies der RH darauf, dass gerade das vom Justizministerium angeführte Beispiel des Internetbetrugs deutlich die unterschiedlichen Zugangsweisen (Begriffsdefinitionen) von Polizei und Justiz aufzeigte, als Folge dessen vergleichbare Daten als Grundlage für wirksame Steuerungsmaßnahmen fehlten.

Der RH erachtete es daher als zielführend, dass sich das Justizministerium bei einer Strategieentwicklung des Innenministeriums zur verbesserten Bekämpfung von Cyberkriminalität maßgeblich einbringt. In diesem Rahmen wäre insbesondere auch eine gemeinsame Definition von Delikten, die unter den Begriff Cyberkriminalität zu subsumieren sind, zu erarbeiten, um vergleichbare Daten und damit eine verbesserte Basis für effiziente und zwischen Polizei und Justiz abgestimmte Steuerungsmaßnahmen zu erhalten. In Bezug auf eine eigene – noch zu erstellende – Strategie des Justizministeriums für den Bereich Cyberkriminalität verwies der RH auf seine Gegenäußerung in TZ 10.

Zusammenhang der Daten von Polizei und Justiz

5.1 (1) Die Staatsanwaltschaften erfassten ihre Ermittlungsakten und die gesetzten Verfahrens– bzw. Erledigungsschritte grundsätzlich in der Applikation Verfahrensautomation Justiz (**VJ**). Polizeiliche Anzeigen ohne bekannte Tatverdächtige sowie weitere Ermittlungsansätze protokollierten und erledigten sie ohne weitere Bearbeitungsschritte elektronisch in einer eigenen Applikation Elektronische integrierte Assistenz (**EliAs**).[13]

Das Justizministerium strebte im Rahmen der strategischen Initiative Justiz 3.0 an, die interne IT zu einer umfassend vollelektronischen Verfahrensabwicklung weiterzuentwickeln. Die bestehenden justizeigenen Applikationen waren nicht geeignet, zuverlässige Zahlen zu generieren.

(2) Der RH ermittelte anhand von Auswertungen der aktuellen Applikationen bundesweite Gesamtzahlen zu den bei den Staatsanwaltschaften angefallenen Ermittlungsakten (bekannte und unbekannte Täterschaft) im Bereich Cyberkriminalität. Er musste sich dabei auf die eindeutig zuordenbaren Delikte von Cyberkriminalität im engeren Sinn beschränken.[14] Ein Zusammenhang zwischen den so ermittelten Zahlen und den Daten der Polizei war nicht herstellbar.

[13] in der Regel erledigt durch Abbrechung, gegebenenfalls auch Einstellung

[14] Zwischen Polizei und Justiz waren nur diese vergleichbar; § 107c StGB war anders als bei der Verurteilungsstatistik hier berücksichtigt.

In der Gegenüberstellung der bei den Staatsanwaltschaften bundesweit angefallenen Ermittlungsakten mit den Anzeigen laut Polizeilicher Kriminalstatistik ergaben sich deutliche zahlenmäßige Abweichungen.

Die Abweichungen insgesamt sowie bezogen auf das deutlich am stärksten betroffene Delikt (Betrügerischer Datenverarbeitungsmissbrauch) sind in nachstehender Tabelle dargestellt (eine detaillierte Gegenüberstellung für alle Delikte findet sich im Anhang, Tabelle C):

Tabelle 4: Vergleich zwischen polizeilichen Anzeigen und Aktenanfall bei den Staatsanwaltschaften

	2016	2017	2018	2019	Veränderung 2016 bis 2019
	Anzahl				in %
Cyberkriminalität im engeren Sinn insgesamt:					
Anzeigen gemäß Polizeilicher Kriminalstatistik	2.630[1]	3.546	3.070	7.622	190
Aktenanfall bei den Staatsanwaltschaften gemäß Verfahrensautomation Justiz	4.035	4.181	4.202	6.373	58
Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB):					
Anzeigen gemäß Polizeilicher Kriminalstatistik	817	1.056	1.415	5.537	578
Aktenanfall bei den Staatsanwaltschaften gemäß Verfahrensautomation Justiz	1.487	1.536	2.117	3.825	157

StGB = Strafgesetzbuch Quellen: Grunddaten BMI und BMJ; Berechnung: RH

[1] Ohne §§ 107c und 119 StGB; diese wurden in der Polizeilichen Kriminalstatistik erst ab 2017 als Cyberkriminalität erfasst.

Eine beispielhafte Einsicht des RH in 80 Ermittlungsakten zu Cyberkriminalitätsdelikten bei der Staatsanwaltschaft Wien zeigte, dass in 32 der 80 Fälle[15] Polizei und Staatsanwaltschaft das Delikt unterschiedlich statistisch erfassten.

So führte in insgesamt 16 der 80 Fälle die Art der Aktenführung bei den Staatsanwaltschaften systemimmanent zu Doppelerfassungen der polizeilichen Anzeigen. Dies betraf jene Konstellationen, bei denen aus folgenden Gründen grundsätzlich ein zusätzlicher Fall angelegt wurde:

- Wechsel in der Bearbeitung zwischen Bezirksanwaltschaft und Staatsanwaltschaft (drei Fälle),
- Bekanntwerden der Täterschaft (z.B. nach Auskünften von Internetprovidern und Betreibern sozialer Medien) in Fällen mit vorerst unbekannter Täterschaft (acht Fälle),
- Abtrennung von Verfahren oder Übertragung an eine andere Staatsanwaltschaft (fünf Fälle).

[15] In zwei Fällen trafen zwei Abweichungsgründe zu.

Darüber hinaus hatte die Staatsanwaltschaft Wien in 13 Fällen die verwirklichten Straftatbestände – insbesondere das Delikt des Betrügerischen Datenverarbeitungsmissbrauchs – abweichend zur Polizei beurteilt.[16]

Fünf Fälle übermittelte die Polizei lediglich zur rechtlichen Beurteilung (sie waren damit in der Polizeilichen Kriminalstatistik nicht als Straftat ausgewiesen), die allerdings bei der Staatsanwaltschaft zu einem Aktenanfall führten.

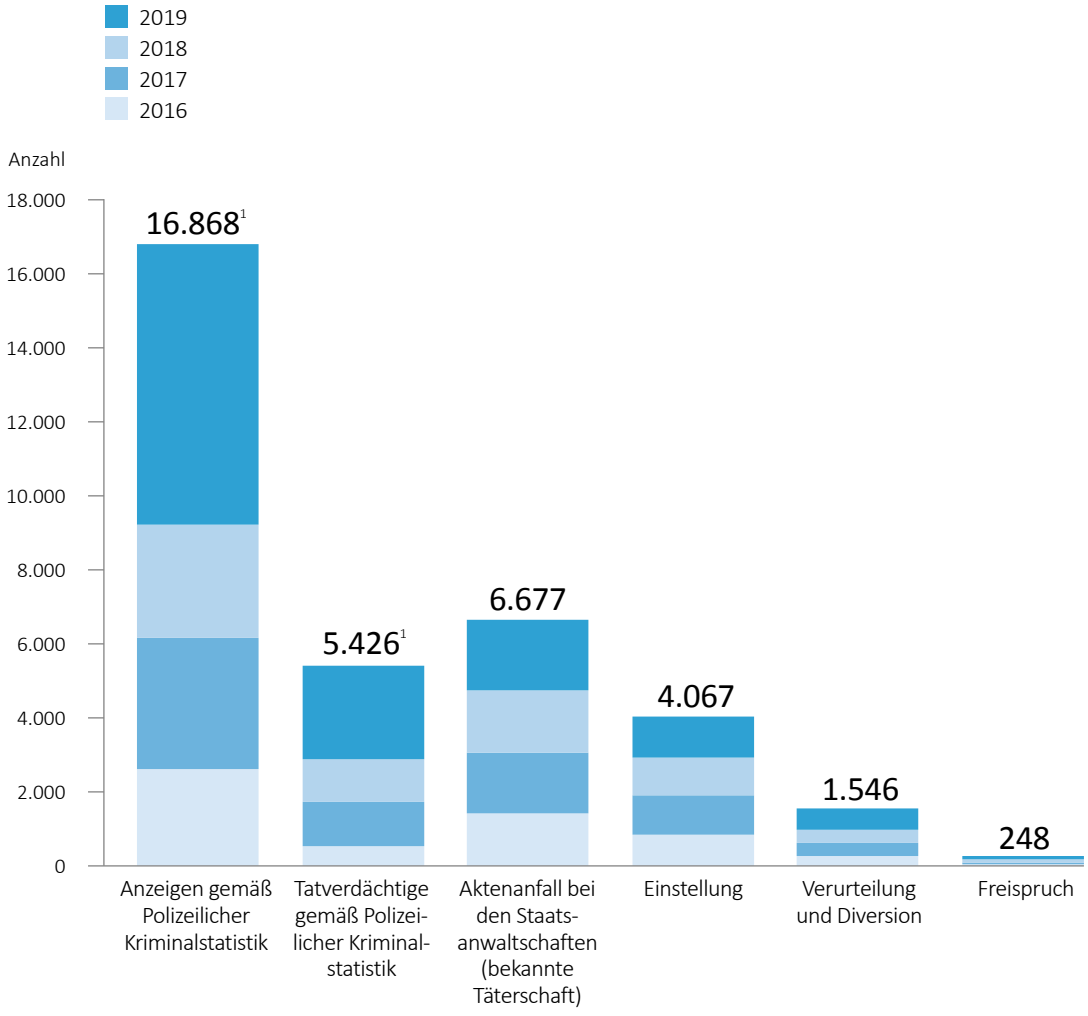
(3) Der RH ermittelte für Cyberkriminalität im engeren Sinn für den Zeitraum 2016 bis 2019 den Aktenanfall (mit bekannter Täterschaft) bei den Staatsanwaltschaften sowie die personenbezogenen Erledigungen[17] durch die Staatsanwaltschaften und Gerichte insgesamt. Er stellte diese der Zahl der Anzeigen und der Tatverdächtigen gemäß Polizeilicher Kriminalstatistik gegenüber (die zahlenmäßige Darstellung inklusive der konkreten Erledigungen durch die Justiz aufgeschlüsselt nach einzelnen Delikten findet sich im Anhang, Tabellen D und E).

[16] Dies betraf insbesondere Fälle der missbräuchlichen Verwendung fremder Bankomatkarten und unberechtigter Bezahlung oder Abhebung unter Nutzung der Near Field Communication (Nahfeldkommunikation)–Technik. Diese waren abweichend oftmals als Diebstahl (§ 127 StGB) bzw. Betrug (§ 146 StGB) qualifiziert worden.

[17] beschränkt auf inhaltliche Erledigungen, d.h. ohne Ausscheidung und sonstige Erledigung

Die folgende Abbildung zeigt das Ergebnis dieser Gegenüberstellung für die Jahre 2016 bis 2019:

Abbildung 1: Vergleich der polizeilichen Anzeigen und der personenbezogenen Erledigungen durch die Justiz (Cyberkriminalität im engeren Sinn), 2016 bis 2019



[1] Jahr 2016 ohne §§ 107c und 119 StGB; diese wurden in der Polizeilichen Kriminalstatistik erst ab 2017 als Cybercrime erfasst.

Quellen: BMI; BMJ; Berechnung und Darstellung: RH

Demnach standen bei Cyberkriminalität im engeren Sinn im Zeitraum 2016 bis 2019 den rd. 16.900 polizeilichen Anzeigen und rd. 6.700 bei den Staatsanwaltschaften angefallenen Ermittlungsakten mit bekannter Täterschaft rd. 1.000 Verurteilungen (und rd. 550 Diversionen) gegenüber.

Eine zusammenfassende Auswertung der personenbezogenen Erledigungen[18] durch Staatsanwaltschaften und Gerichte zeigte, dass der Großteil der Ermittlungsverfahren zu Cyberkriminalität eingestellt wurde. Ausnahmen bestanden vor allem beim Betrügerischen Datenverarbeitungsmissbrauch (vergleichsweise viele Verurteilungen) und bei der Datenfälschung (vergleichsweise viele diversionelle Erledigungen).

(4) Der RH hatte in seinem Bericht „Bundeskriminalamt" (Reihe Bund 2015/14, TZ 24) und der nachfolgenden Follow–up–Überprüfung (Reihe Bund 2018/6, TZ 13) kritisiert, dass keine Verknüpfungen zwischen der Polizeilichen Kriminalstatistik und den Statistiken der Justiz bestanden und daher Aussagen über die Weiterbehandlung der Anzeigen bei der Justiz nicht möglich waren.

Der Rat der EU evaluierte im Jahr 2016[19] die praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität in Österreich. Im Evaluierungsbericht kritisierte er Unterschiede in den Statistiken von Polizei und Justiz und empfahl, an zuverlässigen und umfassenden statistischen Erhebungen bei den an der Bekämpfung von Cyberkriminalität beteiligten Akteuren zu arbeiten.

Das Regierungsprogramm 2020–2024 sah als Maßnahme die Angleichung der polizeilichen und justiziellen Kriminalstatistiken vor.

5.2 Der RH hielt kritisch fest, dass die bei der Justiz zur Unterstützung bei der Führung von Strafverfahren eingesetzten Applikationen nicht bzw. nur sehr eingeschränkt geeignet waren, zuverlässige Daten zum Kriminalitätsgeschehen, vor allem auch im Hinblick auf Cyberkriminalität, zu gewinnen. Er sah in diesem Zusammenhang Verbesserungsmöglichkeiten im Rahmen der vom Justizministerium angestrebten Weiterentwicklung der internen IT hin zu einer umfassenden elektronischen Verfahrensführung.

Der RH kritisierte, dass kein aussagefähiger Zusammenhang zwischen der Polizeilichen Kriminalstatistik und den Zahlen aus den Auswertungen der Justizanwendungen bestand. Es war auch nicht systematisch verfolgbar, wie die polizeilichen Anzeigen bei den Staatsanwaltschaften (und Gerichten) weiterbehandelt bzw. erledigt wurden. Dadurch fehlten Grundlagen, um die speziell im Bereich Cyberkriminalität große Differenz zwischen der Zahl angezeigter Tatverdächtiger und der Zahl der Anklagen bzw. Verurteilungen aufzuklären. So standen bei Cyberkriminalität im engeren Sinn im Zeitraum 2016 bis 2019 den rd. 16.900 polizeilichen Anzeigen und rd. 6.700 bei den Staatsanwaltschaften angefallenen Ermittlungsakten mit bekannter Täterschaft lediglich rd. 1.000 Verurteilungen gegenüber. Ein klarer und umfassender Überblick

[18] Nicht berücksichtigt sind dabei die bei den Staatsanwaltschaften mit Abbrechung, Ausscheidung oder sonstiger Erledigung abgeschlossenen Ermittlungsverfahren.

[19] Bericht vom Mai 2017

zum Phänomen Cyberkriminalität war damit nicht vorhanden, was die strategische Planung und Ressourcensteuerung erschwerte.

Der RH empfahl dem Justizministerium, im Zuge der Weiterentwicklung der internen IT sicherzustellen, dass zuverlässige und aussagekräftige Statistiken zu Anfall und Erledigung von Strafverfahren durch Staatsanwaltschaften und Gerichte generiert werden können; insbesondere sollten auch deliktspezifische Statistiken für den Bereich Cyberkriminalität ermöglicht werden.

Der RH empfahl dem Innenministerium und dem Justizministerium, die polizeilichen und justiziellen Kriminalstatistiken aufeinander abgestimmt weiterzuentwickeln und methodische Angleichungen vorzunehmen.

Er empfahl dem Innenministerium und dem Justizministerium, die Voraussetzungen für eine systematische Nachverfolgung der Erledigung polizeilicher Anzeigen gegen tatverdächtige Personen z.B. auf Basis bereichsspezifischer Personenkennzeichen zu schaffen.

5.3 (1) Das Innenministerium teilte in seiner Stellungnahme mit, dass weiter daran gearbeitet werde, die polizeilichen und justiziellen Kriminalstatistiken anzugleichen. In diesem Zusammenhang weise es auf zu berücksichtigende externe Faktoren hin, z.B. den legistischen Änderungsbedarf oder technische Adaptierungen außerhalb der Sphäre des Innenministeriums.

An der (legistischen) Umsetzung eines umfassenden Systems der bereichsspezifischen Personenkennzeichen werde gearbeitet. Damit sollten sowohl die „Nachverfolgung“ im Bereich der justiziellen Kriminalstatistiken ermöglicht als auch Redundanzen von Personendatensätzen in anderen Rechtsbereichen wie Asyl und Fremdenwesen vermieden werden.

(2) Laut Stellungnahme des Justizministeriums werde, wie bereits vom RH angemerkt, im Rahmen der Digitalisierungsinitiative Justiz 3.0 eine vollelektronische Verfahrensführung und eine – damit einhergehende – Verbesserung der Datenlandschaft angestrebt. Eine wesentliche Hürde seien jedoch auch in Zukunft u.a. die unterschiedlichen Arbeits– und Dokumentationsformen der Polizei und der Staatsanwaltschaften, die sich auch in den Registeranwendungen der Polizei (PAD = Protokollieren, Anzeigen Daten) und der Justiz (VJ) niederschlagen würden. So führe z.B. die weitere Aktualisierung der Fakten im staatsanwaltschaftlichen Ermittlungsverfahren zu vergleichsweise höherem Dokumentations– und Personalaufwand. Infolgedessen habe sich bislang auch die Übernahme der einzelnen Fakten aus der polizeilichen Registeranwendung in die VJ als wenig zielführend herausgestellt. Im Rahmen der als Teil von Justiz 3.0 geplanten Erneuerung der VJ sei aber die registermäßige Erfassung

von Delikten bei Entscheidungen geplant, womit auch eine deutliche Qualitätsverbesserung im Bereich der Statistik erzielt werden könne.

Das bereichsspezifische Personenkennzeichen stehe seit einem Release der VJ im November 2020 in allen Registern (d.h. auch in den Strafregistern) zur Verfügung, es werde – sofern technisch möglich – für die Verfahrensbeteiligten automatisch ermittelt und in der VJ–Datenbank gespeichert. Es seien somit bereits erste technische Schritte im Sinne der Empfehlungen des RH gesetzt worden. Das Konzept des bereichsspezifischen Personenkennzeichens sei erfolgreich in der VJ eingeführt worden, jedoch sehe die Bereichsabgrenzungsverordnung aktuell keine Abbildung für den Strafbereich vor.

5.4 Der RH entgegnete dem Justizministerium, dass unterschiedliche Arbeits– und Dokumentationsformen einem aussagefähigen Zusammenhang zwischen den in den Registeranwendungen enthaltenen statistischen Daten von Polizei und Justiz zum Kriminalitätsgeschehen nicht entgegenstehen sollten. Um einen solchen Zusammenhang herzustellen, wäre jedenfalls die Erfassung grundlegender Daten zum Aktenanfall bei Polizei und Justiz sowie zu den Erledigungen ausreichend abzustimmen. Der RH erachtete es daher als wesentlich, dass das Justizministerium im Rahmen der Digitalisierungsinitiative vorausschauend die Empfehlung des RH zur Weiterentwicklung und methodischen Angleichung der polizeilichen und justiziellen Kriminalstatistiken berücksichtigt.

Der RH sah in der Verwendung bereichsspezifischer Personenkennzeichen eine geeignete Möglichkeit, die Erledigung polizeilicher Anzeigen gegen tatverdächtige Personen durch die Justiz systematisch nachzuverfolgen. Das Justizministerium sollte daher diese auch im Strafbereich einsetzen und im Zusammenwirken von Polizei und Justiz zur Nachverfolgung nutzen.

Strategie und Wirkungsziele

Strategische Grundlagen

6.1 Die EU erließ im Jahr 2013 eine Mitteilung zur „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“. Eine der fünf darin genannten Prioritäten war die drastische Eindämmung von Cyberkriminalität. Ausfluss dieser strategischen Überlegungen war die Gründung des European Cybercrime Centre bei Europol ebenfalls im Jahr 2013 sowie die Empfehlung an alle Mitgliedstaaten, die Budapester Konvention über Computerkriminalität zeitnah zu ratifizieren.

Das European Cybercrime Centre fokussierte sich auf die Bekämpfung von Cyberkriminalität, sexueller Ausbeutung und Kindesmissbrauch im Internet sowie Zahlungsbetrug. Das Innenministerium entsandte zur Mitwirkung einen Cyber Verbindungsbeamten.

Der Evaluierungsbericht des Rates der EU aus 2017 hielt die Lage in Österreich insbesondere in Bezug auf die Tätigkeiten des Innenministeriums für vielversprechend. Er zeigte aber auch Defizite und Verbesserungsmöglichkeiten auf, vor allem bei der Justiz. Zu den fehlenden Maßnahmen siehe TZ 5, TZ 43, TZ 44.

6.2 Der RH anerkannte, dass sich Österreich bzw. das Innenministerium an der Umsetzung der strategischen Zielsetzung der EU zur Bekämpfung von Cyberkriminalität beteiligte.

7.1 Das Bundeskanzleramt hatte gemeinsam mit Verbindungspersonen zum Nationalen Sicherheitsrat und Expertinnen und Experten im Jahr 2013 die Österreichische Strategie für Cyber Sicherheit erarbeitet. Diese sollte ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und der Menschen im virtuellen Raum unter Gewährleistung ihrer Menschenrechte darstellen. Sie leitete sich aus der Österreichischen Sicherheitsstrategie ab und orientierte sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen. Die Österreichische Strategie für Cyber Sicherheit wurde bis zur Zeit der Gebarungsüberprüfung nicht aktualisiert.

Die Strategie normierte Handlungsfelder und Maßnahmen, wobei der Fokus auf Cyber Sicherheit und nicht Cyberkriminalität lag. Für die Koordinierung der operativen Umsetzung war u.a. das Innenministerium verantwortlich. Maßnahmen für die Justiz waren nicht enthalten.

Eine vertiefende ressortübergreifende Auseinandersetzung mit dem Thema Cyberkriminalität oder konkretere Maßnahmen zur Bekämpfung von Cyberkriminalität enthielt die Strategie nicht.

Zur Zeit der Gebarungsüberprüfung überarbeitete das Bundeskanzleramt die Österreichische Strategie für Cyber Sicherheit. Die Veröffentlichung war zeitnah geplant.

7.2 Der RH hielt fest, dass die Österreichische Strategie für Cyber Sicherheit die Sicherheit der Infrastrukturen und Leistungen im Cyber Raum verbessern und Bewusstsein und Vertrauen in der Gesellschaft schaffen sollte. Er bemängelte jedoch, dass mit der aus dem Jahr 2013 stammenden Strategie – gerade im schnelllebigen, sich ständig weiterentwickelnden Internetzeitalter – die notwendige Aktualität nicht mehr gegeben war.

In diesem Zusammenhang hielt er fest, dass das Bundeskanzleramt zur Zeit der Gebarungsüberprüfung die Österreichische Strategie für Cyber Sicherheit überarbeitete.

Regierungsprogramme

8.1 (1) Das Regierungsprogramm 2017–2022 sah bezogen auf Cyberkriminalität im Bereich Inneres insbesondere die Schließung digitaler Sicherheitslücken in Österreich und den Schutz der Bevölkerung vor den neuen Bedrohungen durch die Digitalisierung vor. Es enthielt als Vorhaben den Ausbau des Cybercrime Competence Centers im Bundeskriminalamt zu einer modernen Hightech–Einheit. Für das Justizministerium legte das Regierungsprogramm keine Maßnahmen im Zusammenhang mit Cyberkriminalität fest.

(2) Das Regierungsprogramm 2020–2024 enthielt für den Bereich Inneres im Hinblick auf Cyberkriminalität Maßnahmen z.B. zu Prävention, Organisation, Personal sowie Aus– und Fortbildung. Die nachstehende Tabelle gibt ausgewählte Maßnahmen wieder:

Tabelle 5: Maßnahmen im Regierungsprogramm 2020–2024 für das Innenministerium im Hinblick auf Cyberkriminalität

ausgewählte Maßnahmen
Verbesserung statistischer Aufarbeitung und dabei insbesondere Angleichung der polizeilichen und justiziellen Kriminal– und Rechtspflegestatistiken (TZ 5)
Aktualisierung der Österreichischen Strategie für Cyber Sicherheit (TZ 7)
Erstellung eines Strategiekonzepts zur verbesserten Bekämpfung von Cyberkriminalität in Österreich, z.B. Verbesserung der Bekämpfung von Cyberkriminalität, Verbesserung der Aufklärungsquote, Reduzierung von Cyberkriminalität durch umfassende Prävention (TZ 9, TZ 12)
Ausbau von Präventionsprogrammen (TZ 13 bis TZ 17)
Personaloffensive: 2.300 zusätzliche Planstellen und 2.000 zusätzliche Ausbildungsplanstellen für die Polizei (auch für Spezialisierungen, z.B. Cyberkriminalität, bürgernahe Polizeiarbeit); Entwicklung eines modernen, den sicherheitspolizeilichen Herausforderungen entsprechenden Dienst– und Besoldungssystems (TZ 21, TZ 23, TZ 24, TZ 28 bis TZ 30)
laufende Anpassung der Polizeiausbildung und –fortbildung (Cyberkriminalität und Digitalisierung) (TZ 32 bis TZ 35)
Aus– und Fortbildungsmaßnahmen zur Schaffung von Cyber Cops im Innenministerium, in diesem Zusammenhang Schaffung eines Stipendiensystems für IT–Spezialistinnen und –Spezialisten (Studium) und dadurch langfristige Bindung an das Innenministerium (TZ 32 bis TZ 35)
Stärkung der Zusammenarbeit mit Wissenschaft und Forschung als Grundlage für strategische Entscheidungen, z.B. für Cyber Sicherheit (TZ 7, TZ 9, TZ 18, TZ 39)

Quelle: Regierungsprogramm 2020–2024

Im Bereich der Justiz enthielt das Regierungsprogramm insbesondere folgende Maßnahmen z.B. zu Organisation, Aus– und Fortbildung und den rechtlichen Grundlagen im Hinblick auf Cyberkriminalität:

Tabelle 6: Maßnahmen im Regierungsprogramm 2020–2024 für das Justizministerium im Hinblick auf Cyberkriminalität

ausgewählte Maßnahmen
Verbesserung statistischer Aufarbeitung und dabei insbesondere Angleichung der polizeilichen und justiziellen Kriminal– und Rechtspflegestatistiken (TZ 5)
Stärkung der unabhängigen Ermittlungsarbeit der Staatsanwaltschaften z.B. durch Aufbau von IT– und Wirtschaftsexpertise (TZ 43, TZ 44)
zeitgemäße und erweiterte bzw. präzisierte Straftatbestände zur Bekämpfung aller Arten von Cyberkriminalität samt Prüfung der Erhöhung von Strafrahmen sowie Bündelung staatsanwaltschaftlicher Ermittlungskompetenzen zur Bekämpfung digitaler Verbrechen (TZ 10, TZ 42, TZ 43)
Verfolgung von „Hass im Netz“, Bündelung der Ressourcen im Zusammenhang mit Cyberkriminalität für die Staatsanwaltschaften (Spezialzuständigkeit) samt Schulung für Bedienstete der Justiz in Kooperation mit dem Innenministerium (TZ 10, TZ 43, TZ 44)
ressortübergreifende Nutzung moderner Analysewerkzeuge in Großstrafverfahren, Einsatz von Künstlicher Intelligenz zur Durchsuchung von Beweismitteln (gemeinsam mit der Polizei) (TZ 46)

Quelle: Regierungsprogramm 2020–2024

Das Regierungsprogramm 2020–2024 gab nicht an, mit welchen finanziellen Mitteln und wie die Maßnahmen umzusetzen waren bzw. umgesetzt werden konnten.

8.2 Der RH hielt fest, dass das Regierungsprogramm 2020–2024 eine Vielzahl von Maßnahmen zur Prävention und Bekämpfung von Cyberkriminalität sowohl für das Innen– als auch das Justizministerium festlegte.

Strategie im Innenministerium

9.1 (1) Die Strategie Innere Sicherheit aus dem Jahr 2015 beschäftigte sich zwar mit Cyber Sicherheit, nicht aber mit der Bekämpfung von Cyberkriminalität. In weiterer Folge definierte das Innenministerium z.B. im Strategiepapier „Innen Sicher“ 2018 oder im nachfolgenden strategischen Arbeitsprogramm „Freiheit und Sicherheit“ aus 2019 aber wesentliche Schlüsselherausforderungen zur Verhinderung und Bekämpfung von Cyberkriminalität. Die jeweiligen strategischen Dokumente sollten den Rahmen für die Sicherheitspolitik des Innenministeriums bilden.

Zur Zeit der Gebarungsüberprüfung hatte das Innenministerium keine explizite Cyberkriminalität–Strategie mit Meilensteinen, konkreten Zielen und den dazugehörigen Verantwortlichen ausgearbeitet.

(2) Das Bundeskriminalamt berief sich in den im Zuge der Gebarungsüberprüfung geführten Interviews in Bezug auf die strategische Ausrichtung sowie die dazugehörigen Arbeitsprogramme auf die vom Innenministerium für die Jahre 2017 bis 2020 erstellte Sicherheitsdoktrin. Diese stellte die mittelfristigen strategischen Rahmenbedingungen des Innenministeriums mit Handlungsempfehlungen dar und war mit dem Regierungsprogramm 2020–2024 sowie der Österreichischen Sicherheitsstrategie abgestimmt.[20] Auch in diesem Dokument definierte das Innenministerium Cyberkriminalität als eine der Schlüsselherausforderungen. Die gesetzten Prioritäten in diesem Zusammenhang waren u.a.:

- die umfassende Weiterentwicklung des Cybercrime Competence Centers in Richtung einer modernen Hightech–Crime–Einheit,
- Personalrekrutierung für das Cybercrime Competence Center gegebenenfalls über eine neue IT–Unterstützungsagentur, um schnell und flexibel professionelles Personal in der notwendigen Qualität und Quantität zur Verfügung zu haben,
- Verstärkung der Präventionsarbeit,
- Förderung der internationalen Kooperationen und Vernetzungen.

9.2 Der RH hielt fest, dass sich zwar die strategische Ausrichtung des Innenministeriums in Bezug auf Cyberkriminalität im Lauf der letzten Jahre weiterentwickelt hatte. Allerdings ergab sie sich aus mehreren, nebeneinander gültigen Dokumenten mit unterschiedlichem Detaillierungsgrad, die keine ressortübergreifenden Maßnahmen beinhalteten.

Darüber hinaus kritisierte er, dass das Innenministerium über keine eigenständige Cyberkriminalität–Strategie mit Meilensteinen, konkreten Zielen und den dazugehörigen Verantwortlichen verfügte. Auch fehlte eine Abstimmung mit dem Justizministerium. Insbesondere im Hinblick auf die steigenden Fallzahlen im Bereich Cyberkriminalität und die Umsetzung des Regierungsprogramms 2020–2024 wäre eine solche Strategie notwendig.

Der RH empfahl dem Innenministerium, auch im Hinblick auf das Regierungsprogramm 2020–2024, eine mit dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität zu entwickeln und konsequent zu verfolgen.

9.3 Laut Stellungnahme des Innenministeriums erscheine – in Anbetracht der von disruptiven Technologien und der zunehmenden Digitalisierung von Staat und Wirtschaft geförderten dynamischen Entwicklung von Cyberkriminalität, die zu einem weiteren Anstieg und dem Auftreten neuer Kriminalitätsphänomene in immer kürzeren Intervallen führe – die Schaffung einer mehrjährigen und interministeriell abgestimmten Strategie für Cyberkriminalität kontraproduktiv.

[20] Im Rahmen eines Strategieprozesses legte das Innenministerium in der Folge jährlich die Schwerpunkte in der auf der Sicherheitsdoktrin aufgebauten Teilstrategie fest.

In der in Vorbereitung befindlichen mehrjährigen Ressortstrategie sei daher vorgesehen, in einem entwicklungsoffenen Strategiekonzept die laufende Anpassung der Ermittlungsmethoden und Präventionsansätze bei der Vorbeugung und Bekämpfung von Cyberkriminalität sicherzustellen. Dies entspreche auch dem vom Regierungsprogramm 2020–2024 gewählten Ansatz.

9.4 Der RH entgegnete dem Innenministerium, dass gerade die große Dynamik im Bereich Cyberkriminalität und die in immer kürzeren Abständen auftretenden neuen Phänomene eine darauf abgestimmte Strategie notwendig machen. Er beurteilte eine mehrjährige Ressortstrategie positiv, unabhängig davon war aus seiner Sicht eine ressortübergreifende strategische Abstimmung mit dem Justizministerium zur Prävention und Bekämpfung von Cyberkriminalität jedoch unerlässlich. Der RH hielt seine Empfehlung daher aufrecht.

Strategie im Justizministerium

10.1 Das Justizministerium hatte im überprüften Zeitraum keine Strategie zur Bekämpfung und Verfolgung von Cyberkriminalität implementiert oder sich dahingehend mit dem Innenministerium abgestimmt.

Es stellte zur Zeit der Gebarungsüberprüfung – auch im Hinblick auf die Umsetzung des Regierungsprogramms 2020–2024 – diesbezügliche strategische Überlegungen an. Für den Bereich „Hass im Netz“ hatte das Justizministerium eine Expertengruppe eingesetzt, um ein Maßnahmenpaket – z.B. im Hinblick auf legistische Anpassungen von Straftatbeständen und Regelungen zur Kostentragung in der StPO – zu erarbeiten. Das Gesetzespaket ging Anfang September 2020 in Begutachtung und wurde am 10. Dezember 2020 vom Nationalrat beschlossen. Wesentliche Punkte des Entwurfs waren z.B. die Ausweitung des Tatbestands des § 107c StGB (Cybermobbing), die Erweiterung des Tatbestands des § 283 Abs. 1 Z 2 StGB (Verhetzung) und die Schaffung einer Möglichkeit zur Ausforschung von Täterinnen bzw. Tätern bei Privatanklagedelikten, die im Wege der Telekommunikation oder Verwendung eines Computersystems begangen werden, durch Neuregelung des § 71 StPO.

Die Bundesministerin für Justiz[21] plante auch, eine wissenschaftliche Einrichtung mit der Erstellung einer Studie zu beauftragen, die das kriminalsoziologische Phänomen von Cyberkriminalität sowie allfällige praktische Probleme der Strafverfolgung in diesem Bereich aufarbeiten und darstellen sollte, um in der Folge Maßnahmen setzen zu können. Weitergehende Schritte hatte das Justizministerium noch nicht gesetzt.

[21] Dr.in Alma Zadić, LL.M.

10.2 Der RH hielt kritisch fest, dass das Justizministerium im überprüften Zeitraum noch keine ausreichenden strategischen Überlegungen zu Cyberkriminalität angestellt oder konkrete Maßnahmen zur Umsetzung des Regierungsprogramms 2020–2024 – außer für den Bereich „Hass im Netz" – gesetzt hatte. Insbesondere im Hinblick auf die weitere Umsetzung des Regierungsprogramms erachtete der RH eine mit dem Innenministerium abgestimmte Strategie aber als wesentlich.

Der RH empfahl dem Justizministerium, auch im Hinblick auf das Regierungsprogramm 2020–2024, eine mit dem Innenministerium abgestimmte Strategie für den Bereich Cyberkriminalität zu entwickeln und konsequent zu verfolgen.

10.3 Das Justizministerium führte in seiner Stellungnahme aus, dass das Regierungsprogramm 2020–2024 im Zusammenhang mit der Bekämpfung von Cyberkriminalität dem Justizministerium die „Erarbeitung zeitgemäßer und Erweiterung bzw. Präzisierung vorhandener Straftatbestände zur Bekämpfung aller Arten von Cybercrime sowie Prüfung der Erhöhung der derzeit in Geltung stehenden Strafrahmen" zuweise.

Dieser Aufgabe komme das Justizministerium laufend nach. Zum Beispiel sei mit dem Hass–im–Netz–Bekämpfungsgesetz (BGBI. I 148/2020) der Tatbestand gegen Cybermobbing in § 107c StGB (nunmehr: „Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems") im Sinne dieser Vorgabe ausgeweitet und verschärft worden.

Ein Gesetzesentwurf zur Umsetzung der Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln sei von der zuständigen Fachsektion des Justizministeriums fertiggestellt worden. Dieser müsse insofern als Maßnahme zur Umsetzung des Regierungsprogramms angesehen werden, als – im Sinne der wesentlichen Neuerungen der Richtlinie – nicht mehr nur körperliche unbare Zahlungsmittel, sondern auch nicht körperliche unbare Zahlungsmittel und damit insbesondere auch der Online–Zahlungsverkehr erfasst würden. Der Entwurf sehe u.a. Verschärfungen im Bereich der §§ 148a, 241b und 241f StGB vor.

Demgegenüber weise das Regierungsprogramm 2020–2024 die der Empfehlung entsprechende „Erstellung eines Strategiekonzepts zur verbesserten Bekämpfung von Cybercrime in Österreich" dem Innenministerium zu. Sobald das Innenministerium in diese Richtung aktiv werde, werde sich das Justizministerium selbstverständlich an den diesbezüglichen Arbeiten beteiligen. Das Justizministerium habe das im Übrigen auch bei der Umsetzung der gleichfalls führend an das Innenministerium gerichteten Entschließung des Nationalrats vom 14. Oktober 2020 (104/E XXVII. GP)

betreffend die Entwicklung einer Strategie zur Bekämpfung von politischen, gesellschaftlichen und wirtschaftlichen Risiken durch Deepfakes[22] getan.

10.4 Der RH entgegnete dem Justizministerium, dass nach seiner Ansicht die vom Justizministerium gesetzten – und vom RH im Bericht dargestellten – Maßnahmen zur Bekämpfung und Verfolgung von Cyberkriminalität und zur Umsetzung des Regierungsprogramms 2020–2024 nicht ausreichend waren. Die geplante Beteiligung an einer Strategieentwicklung des Innenministeriums beurteilte der RH positiv. Dennoch erachtete er es vor dem Hintergrund der identifizierten Problemfelder als notwendig – auch ohne explizite Festlegung im Regierungsprogramm –, im Justizministerium aus eigenen Überlegungen eine Strategie für den Bereich Cyberkriminalität zu entwickeln und konsequent zu verfolgen. Der RH hielt seine Empfehlung daher aufrecht.

Wirkungsziele

11.1 (1) Das Innenministerium verfolgte im überprüften Zeitraum u.a. das Wirkungsziel „Kriminalität konsequent und zielgerichtet bekämpfen“. Dieses Wirkungsziel sollte u.a. durch die Stärkung der Cyberkriminalität–Ermittlungen und die Bekämpfung von Cyberkriminalität erreicht werden.

Die nachfolgende Tabelle gibt einen Überblick über jene Maßnahme und die dazugehörigen Kennzahlen bzw. Meilensteine, die in den Jahren 2018 bis 2020 einen Beitrag zur Erreichung des Wirkungsziels im Wirkungsbereich des Bundeskriminalamts auf Untergliederungs– und Globalbudgetebene leisten sollte:

[22] Bei Deepfakes handelt es sich um verschiedene Formen technisch veränderter, d.h. audio–visuell manipulierter Videos, Fotos oder Texte (vgl. Öffentliche Sicherheit 3–4/21, S. 35).

Tabelle 7: Globalbudget: Maßnahme, Kennzahlen und Meilensteine im Wirkungsbereich des Bundeskriminalamts im Hinblick auf Cyberkriminalität

Maßnahme	Kennzahlen	Zielzustand 2018	Istzustand 2018	Zielzustand 2019	Istzustand 2019	Zielzustand 2020
		Anzahl				
Stärkung der Cyberkriminalität–Ermittlungen und Bekämpfung der Internetkriminalität	Delikte pro 100.000 Einwohnerinnen und Einwohnern bei Cyberkriminalität (Durchschnitt drei Jahre; mit Internetbetrug)[1]	≤130	189,2	≤135	246	≤350
		in %				
	Aufklärungsquote bei Cyberkriminalitätsdelikten (Durchschnitt drei Jahre; mit Internetbetrug)[2]	≥38,7	38,1	≥38,9	36,7	≥37
		Meilensteine jeweils zum 31. Dezember				
	Cyberkriminalitätspezialisten[3] in den Regionen	mehr als 90 % der Regionen sind mit Cyberkriminalitätspezialisten[3] ausgestattet	90 % der Regionen sind mit Cyberkriminalitätspezialisten[3] ausgestattet	mehr als 90 % der Regionen sind mit Cyberkriminalitätspezialisten[3] ausgestattet	90 % der Regionen sind mit Cyberkriminalitätspezialisten[3] ausgestattet	–
		Anzahl				
	fallbezogene Ermittlungskooperationen mit anderen Organisationseinheiten bei komplexen IT–Ermittlungsansätzen[4]	–	9	–	–	10
		Anzahl				
	Kriminalprävention im Internetbereich (Präventionsveranstaltungen/–gespräche im Bereich Computer– und Internetkriminalität)[4]	–	–	–	–	≥1.190

[1] Anzahl angezeigter strafbarer Cyberkriminalität–Handlungen * 100.000 / Einwohnerzahl; Durchschnitt der letzten drei Jahre; umfasst sind Cyberkriminalitätsdelikte im engeren Sinn
[2] Anteil der geklärten Fälle an angezeigten Fällen; Durchschnitt der letzten drei Jahre
[3] grundsätzlich Bezirks–IT–Ermittlerinnen und –Ermittler
[4] Kennzahl ab dem Jahr 2020; Organisationseinheiten des Innenministeriums

Quellen: BMI; Bundesvoranschläge 2019 und 2020

Das Innenministerium leitete dieses Wirkungsziel aus der jeweils gültigen Strategie ab und verknüpfte es mit dem Regierungsprogramm 2020–2024 und der Österreichischen Sicherheitsstrategie. Zu erreichende Ziele entwickelte es im Rahmen der jährlichen Planung, maßgeblich dafür waren die strategisch verankerten Arbeitsschwerpunkte.

Um das Wirkungsziel zu erreichen, verteilte das Bundeskriminalamt im Ressourcen–, Ziel– und Leistungsplan Aufträge an die jeweiligen Landespolizeidirektionen. Seit dem Jahr 2018 galt dabei das Phänomen Cyberkriminalität als eines der drei wichtigsten.

Aus Sicht des Bundeskriminalamts waren regional unterschiedliche präventive und repressive Maßnahmen notwendig, um einer Steigerung von Cyberkriminalität entgegenwirken zu können. Es gab daher in bundesländerspezifischen Arbeitsprogrammen Maßnahmen und Kennzahlen vor.

Zu nicht erreichten Kennzahlen und Meilensteinen erarbeitete das Bundeskriminalamt jährliche Abweichungsanalysen bzw. Controlling–Berichte. Laut Auskunft des Bundeskriminalamts bewertete und analysierte es die kriminalpolizeilichen Kennzahlen unterjährig nicht, da unterjährig die Aufklärungsquote nicht aussagekräftig sei und signifikante Deliktsanstiege und korrespondierende Maßnahmen intern im Zuge von Führungskräfte–Treffen besprochen würden.

(2) Das Justizministerium hatte keine Wirkungsziele oder Kennzahlen in Verbindung mit Cyberkriminalität definiert.

(3) Das Innenministerium und das Justizministerium stimmten die Wirkungsziele oder Kennzahlen nicht ab, obwohl in den Jahren 2016 bis 2019 die angezeigten Delikte im Bereich Cyberkriminalität von 13.103 auf 28.439 stiegen.

11.2 Der RH hielt fest, dass das Innenministerium das Wirkungsziel „Kriminalität konsequent und zielgerichtet bekämpfen“ mit seiner strategischen Zielsetzung abgestimmt hatte und somit eine Wirkungszielkaskade vorlag. Darüber hinaus würdigte er die unterschiedlichen Arbeitsprogramme für die Landespolizeidirektionen zur Bekämpfung von Cyberkriminalität positiv.

Der RH hielt kritisch fest, dass das Bundeskriminalamt die Kennzahlen wiederholt nicht erreicht hatte. Darüber hinaus kritisierte er, dass es zwischen dem Innenministerium und dem Justizministerium keine Abstimmung der Wirkungsziele und Kennzahlen im Hinblick auf Cyberkriminalität gab. Dies, obwohl von 2018 auf 2019 die Delikte pro 100.000 Einwohnerinnen und Einwohnern bei Cyberkriminalität von durchschnittlich rd. 190 auf 246 stiegen und im gleichen Zeitraum die Aufklärungsquote von 38,1 % auf 36,7 % sank.

Zur Ausbildung von Bezirks–IT–Ermittlerinnen und –Ermittlern verwies der RH auf seine Feststellungen und Empfehlung in TZ 33.

TEIL 1
PRÄVENTION

Allgemeines

12.1 Die Kriminalprävention dient der Vorbeugung strafbarer Handlungen und ist damit ein wesentlicher Teil der Kriminalitätsbekämpfung. Ihr kommt dabei insbesondere die Aufgabe zu, die Bürgerinnen und Bürger über Möglichkeiten des Selbstschutzes aufzuklären. Kriminalität tritt in vielen verschiedenen Arten auf und wird in Österreich durch die Polizei bekämpft. Aber auch durch entsprechend informierte Bürgerinnen und Bürger gesetzte Präventionsmaßnahmen können einen wesentlichen Beitrag zu mehr Sicherheit leisten.

In § 20 Sicherheitspolizeigesetz (**SPG**) waren die Aufgaben der Polizei zur Aufrechterhaltung der öffentlichen Sicherheit festgelegt. Dazu gehörte auch, präventive Maßnahmen zum vorbeugenden Schutz von Rechtsgütern wie z.B. Leben, Gesundheit und Vermögen zu setzen oder sicherheitspolizeiliche Beratungen durchzuführen. Darüber hinaus hatte die Polizei gemäß § 25 Abs. 2 SPG kriminalpräventive Vorhaben zu fördern, z.B. durch die Zusammenarbeit mit Vereinen und Schulen.

Das Innenministerium leistete auch gemeinsame Präventionsarbeit mit der Privatwirtschaft, Nichtregierungsorganisationen sowie auf internationaler Ebene mit Europol oder Interpol[23].

Das Büro der Vereinten Nationen für Drogen– und Verbrechensbekämpfung hielt in einer eingehenden Untersuchung zu Cyberkriminalität im Jahr 2013 u.a. fest, dass besonders die Sensibilisierung der Bevölkerung durch Kriminalprävention ein geeignetes Mittel zur Bekämpfung von Cyberkriminalität sei und international eine hohe Priorität einnehmen müsse.

Das Innenministerium hatte in seinen strategischen Zielsetzungen die Eindämmung von Cyberkriminalität durch verstärkte Prävention festgehalten und in den jährlichen Arbeitsprogrammen an die Landespolizeidirektionen vorgegeben.

[23] Interpol ist die Kurzbezeichnung für International Criminal Police Organization.

12.2 Der RH hielt fest, dass die Kriminalprävention insbesondere in Bezug auf Cyberkriminalität wesentlich war, da die Deliktszahlen und die damit einhergehenden Schäden in den letzten Jahren stiegen und sich die Bekämpfung und Aufklärung oftmals schwierig gestalteten. Er anerkannte, dass das Innenministerium den Ausbau von präventiven Maßnahmen in seinen Strategiepapieren, Wirkungszielen und Arbeitsprogrammen für die Landespolizeidirektionen verankert hatte und über (internationale) Kooperationen zur Präventionsarbeit verfügte.

Der RH hielt aber kritisch fest, dass das Innenministerium zur Zeit der Gebarungsüberprüfung die geplanten Maßnahmen nicht ausreichend umsetzte.

13.1 Mit der im Frühjahr 2020 aufgetretenen COVID–19–Pandemie veränderte sich auch die Kriminalität in Österreich. So waren z.B. Einbruchsdiebstähle rückläufig, während Cyberkriminalität[24] weiter anstieg. Laut einer parlamentarischen Anfragebeantwortung des Innenministeriums vom Mai 2020 kam es in den Monaten März und April 2020 zu einem Anstieg von 8,3 % bei Cyberkriminalität im weiteren Sinn und von 166,2 % bei Cyberkriminalität im engeren Sinn. Die Schadenshöhe in diesen zwei Monaten betrug rd. 8 Mrd. EUR[25].

Das Innenministerium versuchte, die Bevölkerung möglichst breitenwirksam zu informieren und präventive Maßnahmen zu setzen. So warnte z.B. der Innenminister[26] in Pressekonferenzen vor Internetbetrug, es gab regelmäßige Aussendungen in diversen – auch sozialen – Medien oder auf der Homepage des Innenministeriums, des Bundeskriminalamts und der Landespolizeidirektionen.

Präventive Beratungen wurden während der COVID–19–Pandemie überwiegend per Telefon oder E–Mail durchgeführt. Das Innenministerium setzte weiters verstärkt auf mediale Präsenz und drehte z.B. Kurzvideos zur Veröffentlichung auf Social Media.

13.2 Der RH hielt fest, dass das Innenministerium während der COVID–19–Pandemie die Bevölkerung zu neu aufgetretenen Cyberkriminalität–Phänomenen informierte und präventive Maßnahmen in Pressemitteilungen, Schaltungen auf Social Media oder in den Medien erläuterte. Er wies darauf hin, dass die COVID–19–Pandemie zu verstärkter Cyberkriminalität (z.B. durch Hackerangriffe) führte und erachtete

[24] Kriminelle nutzten die Verunsicherung und angespannte Lage in der Bevölkerung aus und verkauften z.B. nicht einsatzfähige Gesichtsmasken oder wirkungslose Desinfektionsmittel, oder sie entwickelten neue Betrugsmethoden, die vor allem auf Personen im Homeoffice abzielten.

[25] Laut Innenministerium beinhalteten diese Zahlen nur die von Betroffenen bei der Anzeigenlegung gemeldeten Schadensangaben. Die hohe Schadenssumme errechnete sich auch aus angezeigten Forderungen, welche aus dem Milieu der Staatsverweigernden in Erpressungsabsicht gestellt wurden, jedoch nicht zur Auszahlung gelangten. Wesentlich höher lagen nach der Anfragebeantwortung die Dunkelziffern in diesem Bereich, da die Anzahl nicht angezeigter Straftaten verhältnismäßig stark über der Anzahl angezeigter Straftaten lag.

[26] Karl Nehammer, MSc

präventive Gegenmaßnahmen daher als umso dringlicher. Es wäre demnach zweckmäßig, verstärkt und strukturiert Informationswege für Präventionsmaßnahmen (z.B. laufende Online–Veranstaltungen) zu überlegen.

Polizeiinspektionen sowie Bezirks– und Stadtpolizeikommanden

14.1 (1) Auf allen Ebenen des Innenministeriums waren nach den grundsätzlichen Vorgaben des Innenministeriums bzw. des Bundeskriminalamts kriminalpräventive Tätigkeiten wahrzunehmen.

In den Polizeiinspektionen und/oder Bezirks– und Stadtpolizeikommanden waren besonders geschulte Polizeibedienstete – sogenannte Präventionsbedienstete – einzusetzen, die innerhalb ihres örtlichen Zuständigkeitsbereichs kriminalpräventive Aufgaben wahrnahmen. Die Organisation, Koordination und Steuerung dieser Präventionsbediensteten nahmen die Kriminalreferentinnen und –referenten in den Bezirks– und Stadtpolizeikommanden wahr. Diese meldeten den Ausbildungsbedarf jährlich an das Landeskriminalamt, welches in der Folge das Bundeskriminalamt informierte.

Das allgemeine – vom Bundeskriminalamt vorgegebene – Anforderungsprofil für Präventionsbedienstete sah insbesondere vor, dass die Beamtinnen und Beamten die Tätigkeit freiwillig ausüben, Interesse und Bereitschaft dafür mitbringen und online das Grundmodul der Kriminalprävention am Campus der Sicherheitsakademie des Innenministeriums positiv absolvieren.

Im Bereich Cyberkriminalität sollten nach den Vorgaben des Bundeskriminalamts die Präventionsbediensteten private und juristische Personen grundsätzlich und anlassbezogen beraten und schulen, mit Kooperationspartnern (z.B. der Wirtschaftskammer Österreich) in Projekten zusammenarbeiten sowie zielgruppenorientierte Handlungs– und Rechtssicherheit vermitteln. Nicht vorgesehen war z.B., dass Präventionsbedienstete in Computersysteme eingreifen, umfassende Sicherheitskonzepte erstellen oder für die technische Netzwerksicherheit sorgen.

Die vom Bundeskriminalamt erlassenen „Richtlinien für die Aufgaben, Organisation und Vollziehung der Kriminalprävention“ (in der Folge: **Präventionsrichtlinie**) aus dem Jahr 2017 gaben mit Stichtag 31. Dezember 2019 vor, wie viele Präventionsbedienstete bundesweit in den Bezirks– und Stadtpolizeikommanden für Cyberkriminalität zur Verfügung stehen sollten. Die vorgeschriebene Mindestanzahl resultierte aus Meldungen der Landespolizeidirektionen und Bezirks– bzw. Stadt-

polizeikommanden, auf deren Grundlage das Bundeskriminalamt in Abstimmung mit dem Innenministerium die Anzahl festlegte.

Die nachstehende Tabelle zeigt die festgelegte Mindestanzahl und die tatsächlich ausgebildeten Präventionsbediensteten für ganz Österreich zum 31. Dezember 2019:

Tabelle 8: Präventionsbedienstete für Cyberkriminalität in den Bezirks– und Stadtpolizeikommanden

	Burgenland	Kärnten	Niederösterreich	Oberösterreich	Salzburg	Steiermark	Tirol	Vorarlberg	Wien	Summe
	in Köpfen zum 31. Dezember 2019									
festgelegte Mindestanzahl	16	25	62	34	20	29	13	4	40	243
ausgebildet	7	19	12	11	9	18	6	–	14	96
	in %									
Planerfüllung	44	76	19	32	45	62	46	0	35	40

Quelle: BMI

Zur Zeit der Gebarungsüberprüfung war die Mindestanzahl ausgebildeter Präventionsbediensteter für Cyberkriminalität bundesweit in den Bezirks– und Stadtpolizeikommanden nur zu 40 % erreicht, in Vorarlberg gab es keine speziell ausgebildeten Bediensteten.

(2) Das Bundeskriminalamt gab im überprüften Zeitraum in den bundesländerspezifischen Arbeitsprogrammen Zielwerte für die Anzahl der durchzuführenden Präventionsmaßnahmen betreffend Cyberkriminalität vor. Ab dem Jahr 2020 verankerte das Innenministerium eine entsprechende Kennzahl auch in einem Wirkungsziel. Laut Auswertungen aus der Applikation Protokollieren, Anzeigen, Daten (**PAD**) setzten die Präventionsbediensteten bundesweit im Jahr 2019 folgende Anzahl an Präventionsmaßnahmen im Bereich Cyberkriminalität und erreichten damit folgende Anzahl an Personen:

Tabelle 9: Präventionsmaßnahmen bei den Bezirks– und Stadtpolizeikommanden im Bereich Cyberkriminalität

	Burgenland	Kärnten	Niederösterreich	Oberösterreich	Salzburg	Steiermark	Tirol	Vorarlberg	Wien	Summe
	Anzahl im Jahr 2019									
Maßnahmen	200	778	791	926	704	695	351	330	222	4.997
erreichte Personen	5.344	15.904	15.173	25.152	14.855	16.217	7.547	1.897	7.466	109.555

Quelle: BMI

Nachdem die Präventionsmaßnahmen für Erwachsene erst im Aufbau waren, boten die Präventionsbediensteten (außer in Kärnten, der Steiermark und Vorarlberg) mehr Beratungen und Veranstaltungen für Kinder und Jugendliche an als für Erwachsene: Von den 4.997 Beratungen bundesweit waren 3.129 (63 %) an Kinder und Jugendliche gerichtet.

(3) Für die Tätigkeit von Präventionsbediensteten bei Polizeiinspektionen sollte nach der Präventionsrichtlinie grundsätzlich ein Drittel der Monatsdienstzeit im Jahresschnitt – unter Berücksichtigung von temporären Spitzen – zur Verfügung stehen. Auf Ebene der Stadtpolizeikommanden in Wien konnten die Präventionsbediensteten bis zur vollen Monatsdienstzeit für diese Aufgabe spezialisiert verwendet werden.

Laut Information des Landeskriminalamts Wien hatte die Kriminalprävention seit Jahren mit Problemen zu kämpfen. So werde etwa die Präventionsrichtlinie auf Ebene der Stadtpolizeikommanden z.B. aufgrund von Personalmangel und Überbelastung durch laufende Projekte nur ansatzweise umgesetzt. Es gebe wenig Anreiz und Anerkennung für Präventionsbedienstete, was es insbesondere für das Thema Cyberkriminalität schwierig mache, freiwillige Interessentinnen und Interessenten zu finden.

Dem Bundeskriminalamt waren die Probleme bewusst. Es erklärte sie mit der partiell sehr schwierigen Personalsituation in den Polizeiinspektionen und dem Umstand, dass die Prävention nur einen Teil der Tätigkeiten ausmachte. Maßnahmen, um für die Tätigkeit als Präventionsbedienstete mehr Anreize zu schaffen, waren nicht geplant.

14.2 Der RH kritisierte, dass es bundesweit auf Ebene der Bezirks– und Stadtpolizeikommanden lediglich 96 statt der vorgesehenen 243 Präventionsbediensteten für Cyberkriminalität (und in Vorarlberg keine derart geschulten Bediensteten) gab. Damit wurde die vom Bundeskriminalamt – in Abstimmung mit den Bezirks– und Stadtpolizeikommanden – vorgegebene Mindestanzahl um 60 % unterschritten. Darüber hinaus wurde die Präventionsrichtlinie in den Wiener Stadtpolizeikommanden nur ansatzweise umgesetzt.

Der RH bemängelte weiters, dass Präventionsmaßnahmen betreffend Cyberkriminalität für Erwachsene – im Gegensatz zu jenen für Kinder und Jugendliche – noch im Aufbau waren und daher noch nicht in ausreichendem Ausmaß gesetzt wurden. Aus seiner Sicht konnte so nicht sichergestellt werden, dass insbesondere Seniorinnen und Senioren oder potenzielle Opfer von z.B. Sextortion oder Love Scam präventiv informiert wurden.

Der RH empfahl dem Innenministerium, auch im Hinblick auf das entsprechende Wirkungsziel Anreize für Präventionstätigkeiten zu schaffen, um weitere Präventionsbedienstete für Cyberkriminalität zu gewinnen.

Weiters empfahl er dem Bundeskriminalamt, sicherzustellen, dass bedarfsorientierte Präventionsmaßnahmen im Bereich Cyberkriminalität auf Ebene der Bezirks– und Stadtpolizeikommanden verstärkt für die Zielgruppe der über 18–Jährigen gesetzt werden.

14.3 Das Innenministerium teilte in seiner Stellungnahme mit, dass aus seiner Sicht das derzeitige Modell einer Freiwilligenmeldung grundsätzlich als positiver Zugang in Zusammenhang mit Präventionstätigkeiten gesehen werde. Dennoch nehme das Innenministerium im Rahmen der Weiterentwicklung des Kriminaldienstes die Empfehlung des RH zum Anlass, zu prüfen, inwieweit zusätzliche Anreize für die Präventionstätigkeit geschaffen werden könnten.

Im Jahr 2019 hätten bereits 94 Bedienstete eine mehrstufige, zweimonatige Ausbildung für die Zielgruppe der über 18–Jährigen absolviert. Weitere Ausbildungsmaßnahmen würden in Abhängigkeit von der Pandemie–Entwicklung gesetzt. Begleitend dazu würden laufend neue Themen aufbereitet (z.B. eigene Module für Seniorinnen und Senioren) und den Bediensteten zur Verfügung gestellt, um ein zielgruppenorientiertes Arbeiten zu ermöglichen.

Landeskriminalämter

15.1 (1) In den Landeskriminalämtern nahm jeweils der Assistenzbereich Kriminalprävention die präventiven Aufgaben wahr. Diesem oblagen nach den grundsätzlichen Vorgaben des Bundeskriminalamts

- die Durchführung von bedarfsangepassten kriminalpräventiven Maßnahmen durch Einzelberatungen oder Präventionsveranstaltungen,
- Schulungen der nachgeordneten Dienststellen sowie
- die kriminalpräventive Öffentlichkeitsarbeit; letztere in Kooperation mit den in den Bezirks– und Stadtpolizeikommanden verwendeten Präventionsbediensteten und durch Koordinierung dieser Bediensteten.

In keinem Landeskriminalamt war ein eigener Bereich für Cyberkriminalität eingerichtet. Dieser wurde – außer in Vorarlberg – von entsprechend geschulten Präventionsbediensteten abgedeckt; in Wien war ein Bereich Digitale Sicherheit in die Gruppe Eigentumsprävention integriert. Es gab zur Zeit der Gebarungsüberprüfung daher auch keine Planstellen für den Bereich Cyberkriminalität.

Die folgende Tabelle zeigt die ausgebildeten Präventionsbediensteten für Cyberkriminalität zum 31. Dezember 2019:

Tabelle 10: Ausgebildete Präventionsbedienstete für Cyberkriminalität in den Landeskriminalämtern

	Burgenland	Kärnten	Niederösterreich	Oberösterreich	Salzburg	Steiermark	Tirol	Vorarlberg	Wien
	Anzahl in Köpfen zum 31. Dezember 2019								
Präventionsbedienstete	2	1	3	2	1	1	2	–	9

Quelle: BMI

In Vorarlberg führten der Assistenzbereich IT–Beweissicherung und fallweise auch der Ermittlungsbereich Betrug präventive Maßnahmen zu Cyberkriminalität durch, da im Assistenzbereich Kriminalprävention keine diesbezügliche fachliche Kompetenz vorhanden war. Nach Angaben der Landespolizeidirektion Vorarlberg gab es für Prävention Cyberkriminalität weder die Ausbildung noch die Ressourcen.

(2) Die Präventionsbediensteten der Landeskriminalämter führten in ganz Österreich laut den vom Bundeskriminalamt übermittelten Auswertungen im Jahr 2019 folgende Anzahl an Präventionsmaßnahmen im Bereich Cyberkriminalität durch und erreichten damit folgende Anzahl an Personen:

Tabelle 11: Präventionsmaßnahmen bei den Landeskriminalämtern im Bereich Cyberkriminalität

	Burgenland	Kärnten	Niederösterreich	Oberösterreich	Salzburg	Steiermark	Tirol	Vorarlberg	Wien
	Anzahl im Jahr 2019								
Maßnahmen	3	17	93	23	48	130	253	5	108
erreichte Personen	3	477	2.421	679	984	3.216	2.836	50	2.283

Quelle: BMI

(3) Das Landeskriminalamt Wien plante aufgrund steigender Fallzahlen im Bereich Cyberkriminalität, im Assistenzbereich Kriminalprävention eine eigene Gruppe für Cyberkriminalität mit sechs Bediensteten einzurichten. Es arbeitete ein Konzept aus und stellte Ende 2018 den Antrag an die Landespolizeidirektion. Diese Gruppe sollte sich auf Personen über 18 Jahre spezialisieren, da es für diese Zielgruppe noch keine ausreichenden Präventionsmaßnahmen gab.

Zur Zeit der Gebarungsüberprüfung war der Antrag noch nicht genehmigt. Das Landeskriminalamt hatte daher vorerst einen Bereich Digitale Sicherheit in die Gruppe Eigentumsprävention integriert. Im Bereich Digitale Sicherheit standen mit Anfang 2020 vier Bedienstete zur Verfügung.

15.2 Der RH hielt kritisch fest, dass bundesweit in den Landeskriminalämtern kein eigener Präventionsbereich für Cyberkriminalität eingerichtet war. Dies wäre aus Sicht des RH aufgrund der zunehmenden Gefahren von Cyberkriminalität eine notwendige und wichtige Maßnahme, um die Bevölkerung präventiv beraten zu können. Der RH hielt fest, dass das Landeskriminalamt Wien bereits seit dem Jahr 2018 bestrebt war, eine eigene Gruppe für Cyberkriminalität im Assistenzbereich Kriminalprävention einzurichten; zur Zeit der Gebarungsüberprüfung war der Antrag aber noch nicht genehmigt.

Der RH empfahl dem Innenministerium, in den Assistenzbereichen Kriminalprävention der Landeskriminalämter den Bereich Cyberkriminalität – z.B. durch die Einrichtung von eigenen, auf die Prävention von Cyberkriminalität spezialisierten Gruppen – stärker zu verankern.

Der RH kritisierte, dass es in der Landespolizeidirektion Vorarlberg – weder auf Ebene der Bezirkspolizeikommanden noch beim Landeskriminalamt – speziell geschulte Präventionsbedienstete für Cyberkriminalität gab. Präventive Maßnahmen zu Cyberkriminalität führten nur der Assistenzbereich IT–Beweissicherung und der Ermittlungsbereich Betrug durch. Dies widersprach aus Sicht des RH auch der Intention des Bundeskriminalamts, eine stabile Basis an einheitlich und gut ausgebildeten Präventionsbediensteten zu gewährleisten.

Der RH empfahl dem Innenministerium, dafür zu sorgen, dass in der Landespolizeidirektion Vorarlberg ausreichend Präventionsbedienstete mit Expertise für Cyberkriminalität zur Verfügung stehen.

15.3 Laut Stellungnahme des Innenministeriums sei die Einrichtung einer eigenen, auf Cyberkriminalität spezialisierten Gruppe in den Assistenzbereichen Kriminalprävention der Landeskriminalämter nicht notwendig, da in jedem Landeskriminalamt entsprechend ausgebildete Bedienstete zur Verfügung stünden, die auch als Ausbildende für den Bereich Computer– und Internetkriminalität, und somit als Verantwortliche, fachlich befähigt seien. Durch eine enge Zusammenarbeit mit dem Assistenzbereich IT–Beweissicherung in jedem Landeskriminalamt könne ein ergänzendes und umfassendes Spektrum abgedeckt werden. Davon profitiere die Präventionstätigkeit zusätzlich und dadurch könne Präventionstätigkeit im Sinn eines gesamtheitlichen Ansatzes geleistet werden.

Bis Dezember 2019 seien drei Exekutivbedienstete der Landespolizeidirektion Vorarlberg ausgebildet worden. Die für 2020 vorgesehenen Ausbildungen von sieben Exekutivbediensteten hätten aufgrund der COVID–19–Pandemie verschoben werden müssen.

15.4 Der RH entgegnete dem Innenministerium, dass die Stärkung von Präventionstätigkeiten durch die Einrichtung von eigenen auf Cyberkriminalität spezialisierten Gruppen in den Landeskriminalämtern – wie vom Landeskriminalamt Wien angestrebt – eine von mehreren Möglichkeiten war, um diese komplexe Materie entsprechend zu verankern. Aufgrund der zunehmenden Gefahren von Cyberkriminalität war es entscheidend, wirksame und nachhaltige Präventionsarbeit zu leisten. Die Einrichtung von eigenen Gruppen würde aus Sicht des RH eine enge Zusammenarbeit mit dem Assistenzbereich IT–Beweissicherung nicht behindern, sondern sogar erleichtern.

Bundeskriminalamt

16.1 Im Bundeskriminalamt war in der Abteilung Kriminalstrategie und zentrale Administration das Büro Kriminalprävention und Opferhilfe u.a. für Angelegenheiten der bundesweiten Kriminalprävention eingerichtet. Dieses gab bundesweit die fachlichen Inhalte und einheitliche Standards für die praktische Umsetzung der Präventionstätigkeit vor. Das Bundeskriminalamt stellte auch Folder und anderes Informationsmaterial zur Verfügung, zudem mussten Präventionsprojekte zur Sicherstellung einheitlicher Qualitätsstandards von ihm genehmigt werden.

In der 2017 erlassenen Präventionsrichtlinie des Bundeskriminalamts[27] war – neben Bereichen wie Eigentumsschutz und Sexualdeliktsprävention – erstmals Cyberkriminalität als eigener Präventionsbereich festgelegt. Zielgruppe sollten Erwachsene sein.

Dem Büro Kriminalprävention und Opferhilfe oblag es, die Ausbildungsmodule für die Präventionsbediensteten zu planen und durchzuführen[28]. So sollten die fachlichen Standards und Inhalte der Ausbildung in Curricula festgelegt werden. Zur Zeit der Gebarungsüberprüfung lag für den Bereich Cyberkriminalität noch kein Curriculum vor. Das Bundeskriminalamt konnte diesbezüglich auch keinen Zeithorizont nennen. Es hatte – nach eigenen Angaben aufgrund fehlender Ressourcen – erst im Jahr 2019 mit Ausbildungen für diesen Bereich begonnen; diese waren speziell für die Prävention von Erwachsenen konzipiert. Bis Ende 2019 hatte das Bundeskriminalamt fünf zentrale Ausbildungslehrgänge durchgeführt.

16.2 Der RH hielt positiv fest, dass das Bundeskriminalamt in seiner Präventionsrichtlinie Cyberkriminalität als eigenen Präventionsbereich festgelegt hatte. Er kritisierte

[27] Vor dem Erlass der Präventionsrichtlinie durch das Bundeskriminalamt im Jahr 2017 war im überprüften Zeitraum eine Richtlinie der Generaldirektion für die öffentliche Sicherheit aus dem Jahr 2005 gültig. Diese enthielt keine Vorgaben zum Umgang mit Cyberkriminalität.

[28] gegebenenfalls in Kooperation mit der Sicherheitsakademie des Innenministeriums

jedoch, dass es mit den Ausbildungen der Präventionsbediensteten erst im Jahr 2019 begonnen und das Curriculum noch nicht fertiggestellt hatte.

Der RH empfahl dem Bundeskriminalamt, das Curriculum mit fachlichen Standards und Inhalten der Präventions–Ausbildung für Cyberkriminalität fertigzustellen, dessen Anwendung sicherzustellen und in der Folge die Ausbildung der Präventionsbediensteten fortzuführen.

16.3 Das Innenministerium teilte in seiner Stellungnahme mit, diese Empfehlung aufzugreifen und im Rahmen einer zur Zeit der Stellungnahme laufenden Evaluierung zu berücksichtigen.

17.1 (1) Das Bundeskriminalamt kooperierte zur Durchführung von Präventionsveranstaltungen laufend z.B. mit der Wirtschaftskammer Österreich, der Arbeiterkammer, dem Seniorenbund, dem Kuratorium Sicheres Österreich oder im Rahmen des Projekts „Gemeinsam Sicher“ mit Zivilschutzverbänden. Insbesondere für Kinder und Jugendliche gab es spezielle Präventionsprojekte, z.B. Click & Check oder Cyber Kids.

(2) Im Jahr 2020 plante das Bundeskriminalamt Auszahlungen für Präventionsmaterial, z.B. Folder oder Give–aways, in Höhe von rd. 100.000 EUR und weitere 4,70 Mio. EUR für Gewaltschutzzentren bzw. Interventionsstellen. Darüber hinaus betrafen Förderungen des Bundeskriminalamts nach eigenen Angaben zu einem großen Teil den Bereich Kriminalprävention, diesbezüglich rechnete es mit Auszahlungen von 1,20 Mio. EUR. Präventionsveranstaltungen bot das Innenministerium generell kostenlos an.

(3) Die Abteilungen des Bundeskriminalamts oder auch die Landeskriminalämter setzten das Büro Kriminalprävention und Opferhilfe über neue Cyberkriminalität–Phänomene in Kenntnis, sodass dieses gezielt Präventionsinformationen generieren und z.B. im Internet oder in Printmedien veröffentlichen konnte.

(4) Das Bundeskriminalamt erstellte in den Jahren 2015 bis 2018 jeweils einen sogenannten Präventionsbericht. Diese Berichte richteten sich nicht nur an das Innenministerium selbst, sondern auch an die Bevölkerung und sollten einen Überblick über Entwicklungen, (neue) Phänomene und gesetzte Schwerpunkte liefern. Ab dem Jahr 2019 plante das Bundeskriminalamt, diese Berichterstattung neu aufzusetzen, z.B. in Form einer Veranstaltung Mitte 2020, bei der die Landespolizeidirektionen ihre Projekte präsentieren könnten. So sollte den Präventionsbediensteten eine Plattform geboten, die Akzeptanz der Führungskräfte für Präventionstätigkeiten gehoben sowie die Bevölkerung informiert werden. Aufgrund der COVID–19–Pandemie verschob das Bundeskriminalamt diese Pläne vorläufig.

17.2 Der RH hielt positiv fest, dass das Bundeskriminalamt mit zahlreichen Institutionen kooperierte, um gezielt präventive Maßnahmen setzen zu können. Er hielt auch fest, dass das Innenministerium eine Vielzahl von Sensibilisierungsprogrammen zu Cyberkriminalität kostenlos anbot.

Allerdings bemängelte er, dass das Bundeskriminalamt seit dem Präventionsbericht 2018 keine vergleichbaren Informationen erstellt und veröffentlicht hatte. Aus Sicht des RH könnten Maßnahmen wie der Präventionsbericht dazu genutzt werden, die Bevölkerung über Präventionsangebote zu informieren bzw. auch vor neuen Phänomenen zu warnen. Zudem könnte damit Anerkennung für die Präventionsbediensteten ausgedrückt und könnten gegebenenfalls Anreize geschaffen werden, zukünftig als Präventionsbedienstete tätig zu sein.

Der RH empfahl dem Bundeskriminalamt, regelmäßig – etwa in Form eines Präventionsberichts – einen Überblick über (neue) Phänomene und gesetzte Präventionstätigkeiten bzw. –projekte zu veröffentlichen. Dies sollte insbesondere für den Bereich Cyberkriminalität das Bewusstsein in der Bevölkerung erhöhen und eine Plattform für die Arbeit der Präventionsbediensteten bieten.

17.3 Das Innenministerium teilte in seiner Stellungnahme mit, dass auf der Homepage des Bundeskriminalamts regelmäßig zu den verschiedenen Bereichen der Kriminalprävention berichtet und auf das Tätigkeitsfeld bzw. Projekte der Kriminalprävention hingewiesen werde. Durch die Zusammenarbeit der Fachabteilungen des Bundeskriminalamts würden mit Pressemitteilungen und Social–Media–Beiträgen aktuelle Phänomene erklärt und präventive Maßnahmen vorgestellt.

Zudem veröffentliche das Cybercrime Competence Center jährlich den Cybercrime–Report, welcher über die Entwicklung und die Herausforderungen im Bereich Cyberkriminalität Aufschluss gebe.

17.4 Der RH bewertete die zahlreichen vom Bundeskriminalamt zum Thema Cyberkriminalität zur Verfügung gestellten Informationen für die Bevölkerung positiv. Dennoch war es aus Sicht des RH – auch aus Steuerungsgründen – notwendig, einen Gesamtüberblick über (neue) Phänomene und Präventionstätigkeiten bzw. –projekte zu haben und diesen zu veröffentlichen.

18.1 Das Bundeskriminalamt war auch dafür zuständig, Trends in der Kriminalitätsentwicklung frühzeitig zu erkennen, um schon im Vorfeld wirksame Strategien dagegen zu etablieren. Es übernahm außerdem Forschungsagenden in kriminalpolizeilichen Angelegenheiten, um neue Kriminalitätsphänomene richtig erkennen und darauf abgestimmte Lösungen erarbeiten zu können.

Literatur[29], Forschung und auch das Bundeskriminalamt gingen davon aus, dass gerade im Bereich Cyberkriminalität ein erhöhtes Dunkelfeld vorlag. Dunkelfeld in der Kriminalität umfasst generell all jene Delikte, die tatsächlich verübt wurden, aber den Strafverfolgungsbehörden nicht zur Kenntnis gelangten und in der Folge nicht in der Kriminalstatistik erfasst wurden.[30] So ergab etwa die Studie eines deutschen Landeskriminalamts aus dem Jahr 2018 bei computerbezogener Kriminalität ein Dunkelfeld von 90 %.

Das Bundeskriminalamt führte selbst keine Dunkelfeldforschung[31] durch und hatte auch keine Kooperationen mit Wissenschaft und Forschung bzw. anderen Institutionen abgeschlossen. Das Bundeskriminalamt in Deutschland oder z.B. auch das Landeskriminalamt Schleswig–Holstein[32] hatten im Gegensatz dazu bereits mehrere Forschungsprojekte bzw. –berichte im Zusammenhang mit Cyberkriminalität zur Dunkelfeldforschung veröffentlicht.

18.2 Der RH hielt kritisch fest, dass das Bundeskriminalamt weder selbst noch in Kooperation mit Wissenschaft und Forschung Dunkelfeldforschung zu Cyberkriminalität durchführte. Nach Ansicht des RH würde eine solche Rückschlüsse auf das tatsächliche Kriminalitätsaufkommen bieten, die Aussagekraft der Polizeilichen Kriminalstatistik erhöhen und insgesamt ein umfassenderes Bild von Umfang und Struktur von Cyberkriminalität und entstandenen Schäden ermöglichen. Darauf basierend könnten gezieltere Präventionsmaßnahmen gesetzt und Strategien zur Bekämpfung von Cyberkriminalität erarbeitet werden.

Der RH empfahl dem Innenministerium, Kooperationen zur Dunkelfeldforschung mit Wissenschaft und Forschung einzurichten, um ein umfassenderes Bild von Umfang und Struktur von Cyberkriminalität sowie dem tatsächlichen Kriminalitätsaufkommen zu erhalten.

18.3 Laut Stellungnahme des Innenministeriums werde es dieser Empfehlung folgen. Im Jahr 2017 seien organisatorische Maßnahmen im Cybercrime Competence Center gesetzt worden, um sich auf wissenschaftlicher Ebene mit der Entwicklung von Cyberkriminalität auseinanderzusetzen. Mittlerweile sei ein Referat an diversen Forschungsgruppen beteiligt, die sich mit der Entwicklung von Software auseinandersetzten, um die Cyberkriminalität–Ermittlungen – aber auch forensische Prozesse in der IT – zu verbessern. Für die Dunkelfeldforschung gebe es weiters Gespräche

[29] *Rüdiger/Bayerl* (Hrsg.), Cyberkriminologie – Kriminologie für das digitale Zeitalter

[30] *Schneider*, 2.1 Kriminalitätsmessung: Kriminalstatistik und Dunkelfeldforschung, in *Schneider* (Hrsg.), Internationales Handbuch der Kriminologie, Band 1: Grundlagen der Kriminologie (2017) S. 289–333

[31] Ziel der Dunkelfeldforschung ist es, Erkenntnisse über das Gesamtaufkommen bestimmter Straftaten einschließlich des Dunkelfelds zu gewinnen.

[32] *Dreißigacker/Riesner*, Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamts Schleswig–Holstein 2015 und 2017. Forschungsbericht 139 (2018)

mit Vertreterinnen und Vertretern der Donau–Universität Krems, die bereits Studien zu diesem Thema erstellt hätten.

Für 2021 werde in Zusammenarbeit mit renommierten wissenschaftlichen Forschungseinrichtungen die Anwendbarkeit von Methoden der künstlichen Intelligenz anhand mehrerer Pilotthemen (u.a. Dunkelfeldforschung zum Thema Hate Crime) getestet. Diese Methoden sollten geprüft, in die Linienarbeit implementiert und mit notwendigen Anpassungen auch für andere Themen (Cyberkriminalität) verwendet werden können.

19.1 Durch Prävention verhinderte Straftaten waren schwierig nachzuweisen und es gab kaum Instrumente, um die Wirkung bei den Beratenen zu messen. Um dennoch beurteilen zu können, ob die gesetzten Maßnahmen effektiv waren, startete das Bundeskriminalamt im Jahr 2019 ein Projekt mit dem Institut für Höhere Studien zur Wirkungs– und Erfolgsmessung. Es sollten dabei Teilnehmende an Präventionsveranstaltungen zu Cyberkriminalität unmittelbar nach der Teilnahme u.a. zur Qualität der Veranstaltung und einige Zeit nach der Veranstaltung zu allfällig geänderten Einstellungs– und Verhaltensmustern bzw. dem individuellen Sicherheitsgefühl befragt werden.

Zur Zeit der Gebarungsüberprüfung lagen noch keine Erkenntnisse aus dem Projekt vor. Aufgrund der COVID–19–Pandemie konnte das Bundeskriminalamt auch keinen Zeitplan vorlegen, da noch nicht absehbar war, bis wann präventive Veranstaltungen und Beratungen wieder durchgeführt werden konnten.

19.2 Der RH hielt es für zweckmäßig, 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 Gebarungsüberprüfung noch keine Erkenntnisse vor.

Der RH empfahl dem Bundeskriminalamt, das Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität weiterzuverfolgen, die Ergebnisse in der Folge zu verwerten und umzusetzen.

19.3 Laut Stellungnahme des Innenministeriums sei die Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität ein essenzieller Faktor, um Erkenntnisse, insbesondere im Hinblick auf die Qualität der Zielgruppen– und Bedarfsorientierung, zu gewinnen. Weitere Kennzahlen könnten sich, insbesondere nach Abschluss verschiedener Projekte, entwickeln. Das vom RH angesprochene konkrete Projekt zur Wirkungs– und Erfolgsmessung sei bereits abgeschlossen. Die Ergebnisse der Experteninterviews zeigten ein umfassendes Bild und würden teilweise bereits in die Ausbildung und Maßnahmen der Kriminalprävention eingebaut.

TEIL 2
BEKÄMPFUNG

Organisation und Personaleinsatz im Innenministerium

Aufbau und Zuständigkeiten

20 Die folgende Abbildung gibt einen Überblick über die Zuständigkeiten und die Aufgaben der wesentlichen mit Cyberkriminalität befassten Organisationseinheiten des Innenministeriums[33]. Auf allen dargestellten Organisationsebenen fanden Ermittlungen zur Bekämpfung von Cyberkriminalität statt und wurden Assistenzdienste geleistet:

[33] Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, die in den Bundesländern für Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen sowie das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung konnten im Rahmen ihrer Zuständigkeit ebenfalls mit Cyberkriminalität befasst sein.

Abbildung 2: Bekämpfung von Cyberkriminalität – wesentliche Organisationseinheiten des Innenministeriums und deren Aufgaben

Organisationsebenen	Organisationseinheiten	Zuständigkeiten und Aufgaben
Bezirks– und Stadtpolizeikommanden	**Polizeiinspektionen** **Kriminalreferate**	Anzeigen durch die Bevölkerung erfolgten in der Regel bei Polizeiinspektionen[1]. Diese bearbeiteten jene Angelegenheiten selbst, für die sie keine fachliche oder personelle Unterstützung benötigten. Bei komplexen kriminalpolizeilichen Amtshandlungen erhielten sie Unterstützung von den bei den Bezirks– und Stadtpolizeikommanden eingerichteten Kriminalreferaten. Speziell in Zusammenhang mit Cyberkriminalität konnten Bedienstete der Polizeiinspektionen Bezirks–IT–Ermittlerinnen und –Ermittler (TZ 21) hinzuziehen oder Assistenzdienstleistungen der Landeskriminalämter in Anspruch nehmen.
Landeskriminalämter	**Ermittlungsbereiche** (EB) **Assistenzbereiche** (AB)	In von den Landespolizeidirektionen definierten Fällen waren die Landeskriminalämter zuständig, z.B. bei überregionalem Medieninteresse, hoher technischer Komplexität, Ermittlungen gegen kriminelle Verbindungen, Sittlichkeitsdelikten oder bei Betrugsdelikten ab bestimmten Schadenssummen. In einzelnen Ermittlungsbereichen der Landeskriminalämter erfolgten auch Ermittlungen zu Cyberkriminalität im weiteren Sinn. Eigene Ermittlungsbereiche für Cyberkriminalität gab es nicht. Für Ermittlungen zu Cyberkriminalität im engeren Sinn waren die Assistenzbereiche IT–Beweissicherung zuständig. (TZ 23)
Bundeskriminalamt	**Abteilungen**	Das Bundeskriminalamt, das die Fachaufsicht über die nachgeordneten Dienststellen innehatte, konnte Fälle jederzeit an sich ziehen. Dies insbesondere, wenn eine spezielle Ausbildung oder Infrastruktur erforderlich war oder mehrere Bundesländer betroffen waren (z.B. bei Massenphänomenen). Einzelne Abteilungen des Bundeskriminalamts ermittelten auch zu Cyberkriminalität im weiteren Sinn. (TZ 27) Für Ermittlungen zu Cyberkriminalität im engeren Sinn war das in der Abteilung Kriminalpolizeiliche Assistenzdienste eingerichtete Cybercrime Competence Center zuständig. (TZ 26)

[1] Anzeigen konnten aber auch bei Landeskriminalämtern oder beim Bundeskriminalamt eingebracht werden.

Quelle: BMI; Darstellung: RH

Bezirks–IT–Ermittlerinnen und –Ermittler

21.1 (1) Nach einem Erlass des Innenministeriums[34] waren auf Ebene der Bezirks– und Stadtpolizeikommanden sogenannte Bezirks–IT–Ermittlerinnen und –Ermittler einzusetzen. Diese waren Exekutivbedienstete, die eine ergänzende Ausbildung absolviert hatten und zusätzliche Aufgaben übernahmen; organisatorisch waren sie nicht eigens abgebildet.

Eine Stärkung dieser sogenannten Cyber Spezialistinnen und Spezialisten war sowohl im Regierungsprogramm 2020–2024 als auch in den Wirkungszielen des Innenministeriums vorgesehen.

Nach Angaben des Bundeskriminalamts gab es mit 1. Jänner 2020 bundesweit 293 Bezirks–IT–Ermittlerinnen und –Ermittler. Diese Zahlen deckten sich nicht mit den Angaben anderer überprüfter Stellen, z.B. gab die Landespolizeidirektion Wien per Ende Mai 2020 50 Bezirks–IT–Ermittlerinnen und –Ermittler an statt der 61 vom Bundeskriminalamt gemeldeten. Das Bundeskriminalamt und die Landespolizeidirektionen konnten nur für das Jahr 2020 Zahlen nennen, da eine laufende einheitliche Erfassung fehlte.

Aufgeschlüsselt nach den Landespolizeidirektionen ergab sich folgendes Bild:

Tabelle 12: Bezirks–IT–Ermittlerinnen und –Ermittler in Österreich

	Burgen-land	Kärnten	Nieder-österreich	Ober-österreich	Salzburg	Steier-mark	Tirol	Vorarl-berg	Wien	Summe
	Anzahl zum 1. Jänner 2020									
Bezirks–IT–Ermittlerinnen und –Ermittler	14	20	57	38	28	38	25	12	61	293

Quelle: BMI

Bezogen auf die zur Zeit der Gebarungsüberprüfung bestehenden 103 Bezirks– und Stadtpolizeikommanden standen diesen im Durchschnitt rund drei Bezirks–IT–Ermittlerinnen und –Ermittler zur Verfügung.

Das Cybercrime Competence Center erachtete es in seinem im August 2019 finalisierten Grundkonzept zur Bekämpfung von Cyberkriminalität (TZ 26) als notwendig, die Stellung und Bedeutung der Bezirks–IT–Ermittlerinnen und –Ermittler aufzuwerten, sie dem Kriminaldienst zuzuordnen und eigens bewertete Planstellen zu schaffen.

[34] Erlass der Generaldirektion für die öffentliche Sicherheit zu „Exekutiv– und Einsatzangelegenheiten; Kriminaldienst Assistenzbereich IT–Beweissicherung in den Landeskriminalämtern und IT–Ermittlerinnen und –Ermittler in den Bezirken“ aus dem Jahr 2019

Zudem sollte – aufgrund der steigenden Anzahl an Anzeigen zu Cyberkriminalitätsdelikten – ein Mindeststand von durchschnittlich fünf Bezirks–IT–Ermittlerinnen bzw. –Ermittlern pro Bezirk nicht unterschritten werden. Konkrete, der Berechnung der zukünftigen Soll–Personalstände zugrunde liegende Kriterien oder Annahmen waren nicht vorhanden.

Es gab keine Vorgaben des Innenministeriums zur Verteilung der Bezirks–IT–Ermittlerinnen und –Ermittler. Die Landespolizeidirektionen Burgenland, Kärnten, Steiermark und Oberösterreich beabsichtigten, mindestens zwei Bezirks–IT–Ermittlerinnen und –Ermittler pro Bezirk einzusetzen, in Wien war zumindest eine bzw. einer pro Polizeiinspektion geplant. Ansonsten richtete sich der Einsatz nach Arbeitsanfall, Größe der Bezirke bzw. Interesse an der Tätigkeit.

Die Landespolizeidirektionen Tirol und Vorarlberg schätzten die bestehende Anzahl an Bezirks–IT–Ermittlerinnen und –Ermittlern als ausreichend ein. Alle anderen Landespolizeidirektionen erachteten es aufgrund der Entwicklungen von Cyberkriminalität als zweckmäßig, diesen Bereich auszubauen.

(2) Die Interne Revision der Landespolizeidirektion Wien prüfte im Jahr 2017 den Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien im Hinblick auf Cyberkriminalität. Zu den Bezirks–IT–Ermittlerinnen und –Ermittlern hielt der Abschlussbericht insbesondere fest, dass diese eine tragende Rolle bei der Bekämpfung von Cyberkriminalität einnahmen. Es sei auch geplant, die Zahl von 32 Personen im Februar 2018 mittelfristig auf 80 Personen aufzustocken. Die Landespolizeidirektion konnte zur Zeit der Gebarungsüberprüfung keinen Zeithorizont für die Umsetzung nennen. Die Interne Revision regte an, Bedienstete, welche bereits Qualifikationen in IKT und Digitalisierung aufwiesen, über die Personalabteilung ausfindig zu machen und einzusetzen. Ende Mai 2020 waren laut Angaben der Landespolizeidirektion 50 Bezirks–IT–Ermittlerinnen und –Ermittler tätig.

21.2 Der RH hielt fest, dass es Anfang 2020 bundesweit 293 Bezirks–IT–Ermittlerinnen und –Ermittler gab. Damit standen einem Bezirks– bzw. Stadtpolizeikommando im Durchschnitt rund drei Bezirks–IT–Ermittlerinnen und –Ermittler zur Verfügung. Der RH erachtete es als erforderlich, aufgrund steigender Zahlen bei Cyberkriminalität und vor dem Hintergrund der Zielsetzungen im Regierungsprogramm 2020–2024 sowie der Wirkungsziele des Innenministeriums, die organisatorische Eingliederung der Bezirks–IT–Ermittlerinnen und –Ermittler zu evaluieren und darauf aufbauend den künftig notwendigen Bedarf festzulegen. Dazu könnten z.B. das Grundkonzept des Cybercrime Competence Centers (dieses sah fünf Bezirks–IT–Ermittlerinnen und –Ermittler pro Bezirk vor) oder Anregungen der Internen Revision der Landespolizeidirektion Wien genutzt werden.

Der RH hielt kritisch fest, dass das Bundeskriminalamt und die Landespolizeidirektionen die Anzahl der Bezirks–IT–Ermittlerinnen und –Ermittler lediglich zum Stichtag 1. Jänner 2020 zur Verfügung stellen konnten; allerdings erachtete der RH die Werte aufgrund widersprüchlicher Angaben als nicht ausreichend valide. Fehlende Vorgaben bzw. Bemessungsgrundlagen zur Aufteilung der Bezirks–IT–Ermittlerinnen und –Ermittler standen aus Sicht des RH einer transparenten und nachvollziehbaren Verteilung sowie Steuerung entgegen.

Der RH hielt weiters fest, dass in Wien zwar seit dem Jahr 2018 geplant war, die Zahl der Bezirks–IT–Ermittlerinnen und –Ermittler auf 80 Personen zu erhöhen, mit Ende Mai 2020 aber erst 50 vorhanden waren.

Er empfahl dem Innenministerium, die organisatorische Stellung der Bezirks–IT–Ermittlerinnen und –Ermittler zu evaluieren und darauf aufbauend den künftig notwendigen Bedarf festzulegen.

21.3 Laut Stellungnahme des Innenministeriums habe es die Notwendigkeit einer personellen Stärkung auf Ebene der Bezirks–IT–Ermittlerinnen und –Ermittler erkannt und sei dies in einem Strategiepapier des Bundeskriminalamts bereits 2018 zum Ausdruck gebracht worden. Im Rahmen einer Evaluierung sei nun ein Projekt initiiert worden, das dieses Vorhaben und seine Umsetzung vorsehe.

22.1 (1) Die Bezirks–IT–Ermittlerinnen und –Ermittler sollten nach den Vorgaben des Innenministeriums

- Cyberkriminalitätsdelikte im engeren Sinn bearbeiten,
- die Ermittlungen bei sonstigen Cyberkriminalitätsdelikten (Cyberkriminalität im weiteren Sinn) unterstützen (z.B. Teilnahme an Hausdurchsuchungen)
- sowie – je nach Möglichkeit ihrer Ausbildung bzw. Ausrüstung – Datensicherungen und Auswertungen (z.B. von einzelnen Beweisdateien wie Fotos oder Videos von Computern oder Speicherkarten aus Mobiltelefonen) unter der Fachaufsicht des im Landeskriminalamt angesiedelten Assistenzbereichs IT–Beweissicherung durchführen.

Die Landespolizeidirektionen gaben gegenüber dem RH durchwegs an, dass die Tätigkeiten der Bezirks–IT–Ermittlerinnen und –Ermittler dem Erlass des Innenministeriums entsprachen, wobei diese in Oberösterreich und Salzburg noch in eigenen Dienstanweisungen präzisiert wurden.

Die Landespolizeidirektion Wien und die Bezirks–IT–Ermittler im Stadtpolizeikommando Ottakring bestätigten, dass die Bezirks–IT–Ermittlerinnen und –Ermittler sämtliche Ermittlungen im Zusammenhang mit IT bzw. Cyberkriminalität selbst führten und auch einfache Sicherungen durchführten. Auswertungen konnte nur der Assistenzbereich IT–Beweissicherung beim Landeskriminalamt erstellen, da die

Bezirks–IT–Ermittlerinnen und –Ermittler einerseits nicht über die erforderliche technische Infrastruktur verfügten und andererseits nach eigenen Angaben dafür auch nicht ausgebildet waren.

Abweichend davon gab der Assistenzbereich IT–Beweissicherung im Landeskriminalamt Wien an, dass die Bezirks–IT–Ermittlerinnen und –Ermittler entgegen den Vorgaben keine Datensicherungen und Auswertungen, sondern nur Ermittlungen zu Cyberkriminalität im weiteren Sinn durchführten und das anfallende Tagesgeschäft erledigten. Bei Cyberkriminalität im engeren Sinn ermittle ausschließlich der Assistenzbereich selbst.

(2) Die Dienstaufsicht über die Bezirks–IT–Ermittlerinnen und –Ermittler übte in ganz Österreich die jeweilige Dienststelle aus. Gemäß den Regelungen des Innenministeriums sollte – aufgrund der fehlenden fachlichen Expertise in den Bezirks– und Stadtpolizeikommanden – der Assistenzbereich IT–Beweissicherung Untersuchungsberichte und sonstige Schriftstücke genehmigen und somit die Fachaufsicht übernehmen.

Alle Landespolizeidirektionen – mit Ausnahme von Wien – bestätigten, dass die Fachaufsicht der jeweilige Assistenzbereich IT–Beweissicherung tatsächlich wahrnahm.

Die Landespolizeidirektion Wien hatte abweichend davon in einer eigenen Dienstanweisung keine Fachaufsicht des Assistenzbereichs IT–Beweissicherung vorgesehen. Nach Angaben des Landeskriminalamts Wien würden dessen Ressourcen dazu nicht ausreichen. Zudem erscheine eine Fachaufsicht nicht zweckmäßig, da die Bezirks–IT–Ermittlerinnen und –Ermittler keine Ermittlungen zu Cyberkriminalität im engeren Sinn sowie keine Datensicherungen und Auswertungen durchführten. Die Fachaufsicht in Wien verblieb somit beim jeweiligen Kommando der Polizeiinspektionen, der Leitung des Kriminalreferats oder den Leitungen der Ermittlungsbereiche. Eine entsprechende IT–Ausbildung hatten diese in der Regel nicht.

22.2 Der RH hielt fest, dass die Vorgaben des Innenministeriums zu den Bezirks–IT–Ermittlerinnen und –Ermittlern in den Landespolizeidirektionen grundsätzlich umgesetzt wurden. Für Wien zeigte sich allerdings ein unklares Bild bzw. gab es unterschiedliche Aussagen und Wahrnehmungen.

Der RH stellte in diesem Zusammenhang fest, dass in Wien ausschließlich der Assistenzbereich IT–Beweissicherung im Landeskriminalamt Ermittlungen zu Cyberkriminalität im engeren Sinn, Auswertungen sowie zu einem großen Teil Datensicherungen durchführte. Es war nicht auszuschließen, dass diese Vorgehensweise für Wien nur daraus resultierte, dass die Bezirks–IT–Ermittlerinnen und –Ermittler nicht entsprechend ausgebildet waren bzw. die technischen Ressourcen fehlten. Die Übernahme von Tätigkeiten der Bezirks–IT–Ermittlerinnen und –Ermittler verschärfte die angespannte Situation im Assistenzbereich IT–Beweissicherung aus Sicht des RH zusätzlich.

Der RH hielt darüber hinaus fest, dass entsprechend einer Dienstanweisung der Landespolizeidirektion Wien der Assistenzbereich IT–Beweissicherung im Landeskriminalamt Wien nicht – wie vom Innenministerium vorgesehen – die Fachaufsicht über die Bezirks–IT–Ermittlerinnen und –Ermittler wahrnahm. Somit war aus Sicht des RH nicht sichergestellt, dass es für die Bezirks–IT–Ermittlerinnen und –Ermittler in Wien eine qualitätssichernde Fachaufsicht gab.

Der RH verwies auf seine Empfehlung in TZ 37, angemessene Rahmenbedingungen für die Erfüllung der übertragenen Aufgaben zu schaffen.

Der RH empfahl dem Innenministerium, in Wien zur Qualitätssicherung eine geeignete Fachaufsicht über die Bezirks–IT–Ermittlerinnen und –Ermittler sowie entsprechende Ressourcen dafür sicherzustellen.

22.3 Das Innenministerium teilte in seiner Stellungnahme mit, diese Empfehlung aufzugreifen und im Rahmen einer geplanten Evaluierung des Kriminaldienstes zu berücksichtigen.

Assistenzbereiche IT–Beweissicherung der Landeskriminalämter

Organisation und Aufgaben

23.1 (1) Bei den Landeskriminalämtern gab es keine eigenen Ermittlungsbereiche für Cyberkriminalität. So nahmen die Bediensteten der Assistenzbereiche IT–Beweissicherung neben Assistenzleistungen auch Ermittlungsaufgaben wahr. Die Gesamtzahl der Bediensteten der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter stieg von 73 Vollzeitäquivalenten am 1. Jänner 2016 auf 85 Vollzeitäquivalente am 1. Jänner 2020. Im gleichen Zeitraum stieg die Anzahl der angezeigten Straftaten im Bereich Cyberkriminalität gemäß Polizeilicher Kriminalstatistik in Österreich von rd. 13.100 auf rd. 28.400, davon im Bereich Cyberkriminalität im engeren Sinn von rd. 2.600 auf rd. 7.600 (siehe Anhang, Tabelle B).

Gemäß Vorgabe des Innenministeriums[35] fielen den in den Landeskriminalämtern eingerichteten Assistenzbereichen IT–Beweissicherung die folgenden Aufgaben zu:

Tabelle 13: Aufgaben der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter

Aufgabenbereich	Beispiele
Assistenzdienst	forensisch korrekte Beweismittelsicherstellung, Transport, Verwahrung, Sicherung, Untersuchung und Datenbereitstellung von IT–Medien technische Unterstützung anderer Ermittlungseinheiten bei Ermittlungen im Internet insbesondere zu Cyberkriminalität im weiteren Sinn, in Zusammenhang mit Kryptowährungen oder Social Media zentrale Stelle für forensische Sicherung, Untersuchung und Auswertung von mobilen Geräten (TZ 37)
Ermittlung	Ermittlungen zu Cyberkriminalität im engeren Sinn, darunter auch zu betrügerischem Datenverarbeitungsmissbrauch
Schulung	Vermittlung von Kenntnissen aus dem eigenen Aufgabenbereich für die Bediensteten der Landeskriminalämter und der nachgeordneten Dienststellen, soweit für deren Aufgabenwahrnehmung erforderlich Praxisausbildungen in Form von Schulungszuteilungen und jährliche Weiterbildung der Bezirks–IT–Ermittlerinnen und –Ermittler in Absprache mit dem Innenministerium; dies umfasste auch die zweimonatige praktische Dienstzuteilung im Zuge der Bezirks–IT–Ermittler–Ausbildung (TZ 33)
übergreifend	Fachaufsicht über die Bezirks–IT–Ermittlerinnen und –Ermittler (TZ 22) Meldung bisher unbekannter Phänomene und neuer Massendelikte an das Bundeskriminalamt

Quelle: BMI

Laut den Landespolizeidirektionen entsprachen die Tätigkeiten der Assistenzbereiche IT–Beweissicherung grundsätzlich den Vorgaben. Die Landespolizeidirektion Niederösterreich gab an, dass der Assistenzbereich IT–Beweissicherung des Landeskriminalamts – unabhängig von etwaigen Organisationsvorschriften – in der Praxis zusätzlich in die Bereiche Netzwerkkriminalität, mobile Forensik, IT–Forensik, IT–Prävention, Schulungen und Expertise gegliedert war.

Die Landespolizeidirektion Wien[36] schränkte die vom Innenministerium vorgegebenen Aufgaben des Assistenzbereichs IT–Beweissicherung insofern ein, als Ermittlungen zum betrügerischen Datenverarbeitungsmissbrauch nur dann in dessen Zuständigkeit fielen, sofern eine tatsächliche Daten– bzw. Programmmanipulation vorlag. Abweichungen in der praktischen Umsetzung der Vorgaben bestanden in Wien außerdem in Zusammenhang mit der Übernahme der Schulungsaufgaben und im Bereich der Fachaufsicht über die Bezirks–IT–Ermittlerinnen und –Ermittler.

[35] Erlass der Generaldirektion für die öffentliche Sicherheit zu „Exekutiv– und Einsatzangelegenheiten; Kriminaldienst Assistenzbereich IT–Beweissicherung in den Landeskriminalämtern und IT–Ermittlerinnen und –Ermittler in den Bezirken“ aus dem Jahr 2019

[36] vgl. Dienstanweisung aus 2019 des Büros Grundsatz– und Rechtsangelegenheiten der Landespolizeidirektion Wien betreffend StGB; Computer– und Netzwerkkriminalität

Die Landespolizeidirektion Wien beantragte im Juni 2016 beim Innenministerium für den Assistenzbereich IT–Beweissicherung eine formelle organisatorische Aufgliederung in drei Gruppen: IT–Beweissicherung, Computer– und Internetkriminalität und mobile Forensik. Damit einhergehend sei die Bewertung von drei Arbeitsplätzen anzupassen. Zur Zeit der Gebarungsüberprüfung hatte der Assistenzbereich die Aufgliederung praktisch bereits vorgenommen, eine Entscheidung des Innenministeriums war allerdings noch ausständig.

(2) Die Interne Revision der Landespolizeidirektion Wien verwies in ihrem Abschlussbericht vom August 2018 darauf, dass auch die formelle Organisationsstruktur des Assistenzbereichs IT–Beweissicherung den Entwicklungen im Bereich Cyberkriminalität Rechnung tragen sollte. Dabei erachtete sie es als sinnvoll, diesem bei der künftigen organisatorischen Gestaltung eine gewisse Flexibilität zu ermöglichen, um adäquat auf Entwicklungen im Ermittlungs– oder Forensikbereich (z.B. in Zusammenhang mit Internet of Things[37] oder car forensics[38]) reagieren zu können.

23.2 Der RH hielt fest, dass den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter sowohl Ermittlungs– als auch Assistenz– und Schulungsaufgaben zukamen. Insbesondere die forensische Untersuchung und Auswertung technischer Geräte sowie die fachliche Unterstützung der Bezirks–IT–Ermittlerinnen und –Ermittler sowie der Ermittlungsbereiche erachtete der RH dabei als essenziell für die effektive Bekämpfung von Cyberkriminalität.

Der RH merkte an, dass der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien nicht alle Aufgaben den Vorgaben des Innenministeriums entsprechend wahrnahm.

Der RH hielt weiters fest, dass die Landeskriminalämter Niederösterreich und Wien in der Praxis die Organisationsstruktur der Assistenzbereiche IT–Beweissicherung – unabhängig von den Vorgaben des Innenministeriums – angepasst hatten. Er verwies darauf, dass die Landespolizeidirektion Wien bereits im Jahr 2016 einen Antrag auch auf formelle Anpassung der Organisationsstruktur – und auf eine damit verbundene Neubewertung von drei Arbeitsplätzen – gestellt hatte. Vor diesem Hintergrund kritisierte der RH, dass zur Zeit der Gebarungsüberprüfung noch keine Entscheidung des Innenministeriums dazu vorlag. Der RH erachtete es als sinnvoll, den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter aller Bundesländer bei der Gestaltung der Organisationsstruktur Flexibilität und somit eine

[37] Internet of Things bezeichnet die Vernetzung von Gegenständen mit dem bzw. über das Internet, damit diese Geräte selbstständig kommunizieren und verschiedene Aufgaben für die Nutzerin und den Nutzer erledigen (vgl. Bundeskriminalamt, Cybercrime Jahresbericht 2016).

[38] Forensische Auswertung von Fahrzeugdaten. Kraftfahrzeuge speichern beim Betrieb Daten und senden sie oft an die Hersteller. Diese Daten ermöglichen es der Polizei, eine Straftat oder den Hergang eines Unfalls aufzuklären (vgl. Bundeskriminalamt, https://www.bundeskriminalamt.at/news.aspx?id=786171624745546152624D3D, zuletzt abgerufen am 31. August 2020).

adäquate Reaktionsmöglichkeit auf Entwicklungen im Ermittlungs– oder Forensikbereich zu ermöglichen.

Er empfahl daher dem Innenministerium, die Vorgaben an die Organisationsstruktur der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter den praktischen Notwendigkeiten anzupassen, sodass bei der Umsetzung auch laufende Entwicklungen im Ermittlungs– oder Forensikbereich flexibel berücksichtigt werden können.

23.3 Das Innenministerium teilte in seiner Stellungnahme mit, diese Empfehlung aufzugreifen und im Rahmen einer geplanten Evaluierung des Kriminaldienstes zu berücksichtigen.

Personalsituation im Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien

24.1 (1) Der Assistenzbereich IT–Beweissicherung dokumentierte in jährlichen Tätigkeitsberichten die wesentlichen Leistungen nach Art und Anzahl. Er beurteilte auch die Personalsituation und berichtete über etwaige diesbezügliche Schwierigkeiten.

Am 1. Jänner 2016 beschäftigte der Assistenzbereich IT–Beweissicherung in Wien 17 Bedienstete. Bis 1. Jänner 2020 stieg der Personalstand auf 21 Personen, elf davon waren von Polizeiinspektionen dienstzugeteilt. Im gleichen Zeitraum stieg die Anzahl der angezeigten Straftaten im Bereich Cyberkriminalität gemäß Polizeilicher Kriminalstatistik in Wien von rd. 4.300 auf rd. 10.900. Ab dem Jahr 2019 waren im Zuge des Projekts zur Neuinstallierung von IT–Ermittlerinnen und –Ermittlern in den Außenstellen des Landeskriminalamts Wien (TZ 26) zehn zusätzliche Personen für diesen Assistenzbereich tätig.

(2) Mehrere Initiativen und ein Abschlussbericht der Internen Revision hatten eine Verbesserung der Personalsituation zum Inhalt:

Wie in TZ 23 beschrieben, richtete die Landespolizeidirektion Wien im Juni 2016 ein Schreiben an das Innenministerium, in dem es u.a. eine Anpassung der Dienststellenstruktur und Neubewertung von drei Planstellen im Bereich des Assistenzbereichs IT–Beweissicherung beantragte.

Die Interne Revision der Landespolizeidirektion Wien hielt in ihrem Abschlussbericht vom August 2018 fest, dass die personelle Ausstattung des Assistenzbereichs IT–Beweissicherung des Landeskriminalamts Wien nicht die aktuellen Entwicklungen im Bereich Cyberkriminalität widerspiegle. Sie empfahl, den Personalstand zu erhöhen, wies aber darauf hin, dass für eine beträchtliche personelle Erweiterung die zugewiesenen Räumlichkeiten nicht ausreichen würden.

Mit Schreiben vom Oktober 2019 machte das Landeskriminalamt Wien die Landespolizeidirektion Wien auf die Problembereiche Raumbedarf, Infrastruktur und Personalsituation aufmerksam. Es wies außerdem darauf hin, dass der Assistenzbereich seine Ermittlungsaufgaben insbesondere zu Cyberkriminalität im engeren Sinn aufgrund der genannten Problemfelder nicht mehr lückenlos übernehmen und die anfallenden Untersuchungsanträge und Schulungsverpflichtungen nicht mehr ausreichend erfüllen könnte.

Bis zum Ende der Gebarungsüberprüfung kam es im Assistenzbereich IT–Beweissicherung zu keinen den Anträgen und Empfehlungen entsprechenden Anpassungen.

24.2 Der RH hielt fest, dass der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien in jährlichen Tätigkeitsberichten die Personalsituation sowie den Assistenzbereich betreffende Entwicklungen im Bereich Cyberkriminalität und die erbrachten Leistungen zahlenmäßig dokumentierte. Er stellte weiters fest, dass die Leitung des Assistenzbereichs bzw. des Landeskriminalamts wiederholt (letztmalig im Jahr 2019) begründete Anträge zur Verbesserung u.a. der Personalsituation an die Landespolizeidirektion bzw. das Innenministerium richtete, um die übertragenen Aufgaben vollständig wahrnehmen zu können. Darüber hinaus erachtete auch die Interne Revision der Landespolizeidirektion Wien in ihrem Bericht aus dem Jahr 2018 mehr Personal für notwendig.

Nach Ansicht des RH lagen ausreichende Grundlagen und objektive Gründe für die Ansuchen vor und waren die vom Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien zur Aufgabenerfüllung als erforderlich erachteten Änderungen im Personalbereich nachvollziehbar. Der RH verwies daher auf seine Empfehlung in TZ 37, angemessene Rahmenbedingungen für die Erfüllung der übertragenen Aufgaben zu schaffen.

Probebetrieb IT–Ermittlerinnen und –Ermittler in Außenstellen des Landeskriminalamts Wien

25.1 Da die Fallzahlen im Bereich Cyberkriminalität stetig anstiegen und insbesondere in den Außenstellen des Landeskriminalamts Wien Bedarf an Assistenzdienstleistungen in Verbindung mit Cyberkriminalität bestand, startete das Landeskriminalamt mit Beginn des Jahres 2019 einen Probebetrieb mit sogenannten IT–Ermittlerinnen und –Ermittlern.

Mit Februar 2019 setzte es zwei Mitarbeiter in der Außenstelle Zentrum–Ost ein, deren Aufgabe es war, die dortigen Ermittlungsbereiche durch technische Assistenzleistungen bei Cyberkriminalität–Sachverhalten zu unterstützen. Eigene Ermittlungen führten sie nicht durch.

Der Probebetrieb war nach internen Evaluierungen erfolgreich. In der Folge dehnte das Landeskriminalamt den Probebetrieb mit September 2019 auf die Außenstellen Süd und West aus und setzte ab Dezember 2019 auch in den Außenstellen Mitte und Nord je zwei IT–Ermittlerinnen und –Ermittler ein.

Die insgesamt zehn IT–Ermittlerinnen und –Ermittler verfügten über eine eigene technische Ausstattung und damit auch über Personal Computer (**PC**), die nicht mit dem geschlossenen Netzwerk des Innenministeriums verbunden waren und somit einen freien Internetzugang zu Recherchezwecken – z.B. für sogenannte „Open Source Intelligence“ (**OSINT**)–Recherchen – ermöglichten. Zuvor war es für die Ermittlungsbereiche in den Außenstellen durch die ausschließliche Nutzung von Geräten, die in das Büroautomations– und Kommunikationssystem (**BAKS**) eingebunden waren, nicht möglich, Daten auszuwerten bzw. zu sichten.

Zur Zeit der Gebarungsüberprüfung war der Probebetrieb noch nicht in die Linie übergeführt. Die IT–Ermittlerinnen und –Ermittler besetzten noch Poolplanstellen des Ermittlungsdienstes bzw. des Assistenzdienstes der jeweiligen Außenstellen, drei waren den Außenstellen dienstzugewiesen und hatten Planstellen in Stadtpolizeikommanden. Sie unterstanden der Dienst– und Fachaufsicht der Leitungen der Außenstellen sowie der Fachaufsicht des Leiters des Assistenzbereichs IT–Beweissicherung.

25.2 Der RH würdigte den Probebetrieb mit IT–Ermittlerinnen und –Ermittlern des Assistenzbereichs IT–Beweissicherung in den Außenstellen des Landeskriminalamts Wien positiv. Dieser ermöglichte eine technische Unterstützung für vertiefte Ermittlungen in Verbindung mit Cyberkriminalitätsdelikten und erlaubte die raschere Bearbeitung von sichergestellten Beweismitteln. Der RH hielt jedoch kritisch fest, dass die Landespolizeidirektion Wien trotz der positiven Erfahrungen aus dem Probebetrieb diesen noch nicht in den Regelbetrieb übernommen hatte. Die IT–Ermittlerinnen und –Ermittler besetzten Planstellen der Außenstellen bzw. von Stadtpolizeikommanden und nicht des Assistenzbereichs IT–Beweissicherung, obwohl sie dessen Fachaufsicht unterlagen und Tätigkeiten dieses Assistenzbereichs erledigten.

Der RH empfahl dem 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 und die Planstellen dem Assistenzbereich IT–Beweissicherung zugeordnet werden.

25.3 Das Innenministerium teilte in seiner Stellungnahme mit, dass die Ausdehnung des Probebetriebs beim Landeskriminalamt Wien aktuell geprüft und erforderlichenfalls auf die übrigen Außenstellen des Landeskriminalamts ausgedehnt werde.

Die Planstellen der IT–Ermittlerinnen und –Ermittler würden darüber hinaus aus Flexibilitätsgründen aus dem jeweiligen Mitarbeiterpool den Assistenzbereichen intern zugeteilt und bedarfsorientiert verwendet.

25.4 Der RH entgegnete dem Innenministerium, dass der Probebetrieb zu den IT–Ermittlerinnen und –Ermittlern bereits zur Zeit der Gebarungsüberprüfung auf alle Außenstellen des Landeskriminalamts Wien ausgedehnt war und diese Bediensteten noch Poolplanstellen besetzten, obwohl sie Tätigkeiten des Assistenzbereichs IT–Beweissicherung erledigten und dessen Fachaufsicht unterlagen. Aus Sicht des RH und nach Angaben des Landeskriminalamts Wien hatte sich der Einsatz von IT–Ermittlerinnen und –Ermittlern in allen Außenstellen des Landeskriminalamts Wien bereits bewährt und bedurfte keiner weiteren Evaluierung. Der RH hielt daher seine Empfehlung aufrecht.

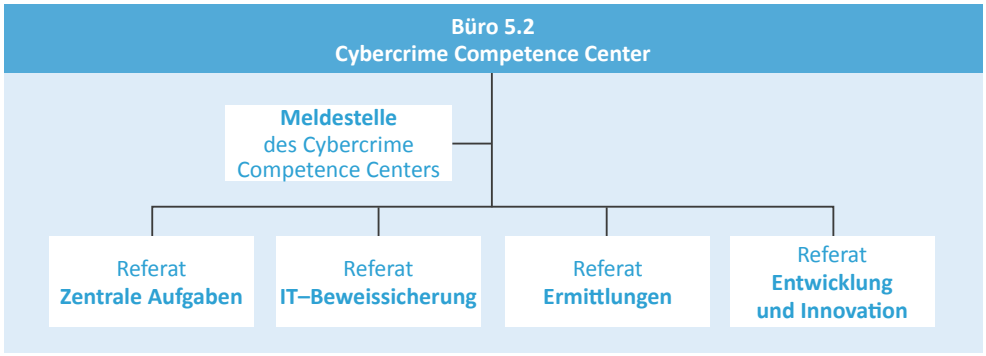
Cybercrime Competence Center im Bundeskriminalamt

Organisation und Zuständigkeit des Cybercrime Competence Centers

26.1 (1) Als zentrale Stelle zur Bekämpfung von Cyberkriminalität etablierte das Innenministerium im Jahr 2012 im Bundeskriminalamt das Cybercrime Competence Center.

Die Struktur des in der Abteilung Kriminalpolizeiliche Assistenzdienste eingerichteten Cybercrime Competence Centers stellte sich zur Zeit der Gebarungsüberprüfung wie folgt dar:

Abbildung 3: Struktur des Cybercrime Competence Centers



Quelle: BMI; Darstellung: RH

Gemäß Grundsatzerlass aus 2017 umfassten die Aufgaben des Cybercrime Competence Centers vor allem:

- elektronische Beweismittelsicherung und –auswertung (IT–Forensik und mobile Forensik),
- Ermittlungen zu Cyberkriminalität im engeren Sinn,
- Ermittlungen zu Cyberkriminalität im weiteren Sinn, sofern zugleich zumindest ein Tatbestand von Cyberkriminalität im engeren Sinn vorlag und die zweckdienlichen Ermittlungsansätze überwiegend IT–technischer Natur waren,
- Koordinierung der Bekämpfung von Cyberkriminalität,
- Fachaufsicht über den Assistenzbereich IT–Beweissicherung in den Landeskriminalämtern und
- Koordinierung und Kontaktaufnahme mit ausländischen Behörden.

Die ebenfalls im Cybercrime Competence Center angesiedelte Meldestelle war 24 Stunden am Tag und sieben Tage die Woche erreichbar.[39] Sie fungierte für Cyberkriminalität–Angelegenheiten als nationale und internationale Kontaktstelle für Europol und Interpol. Zudem stand sie bundesweit generell der Bevölkerung als Ansprechstelle für Fragen zu Cyberkriminalität sowie nachgeordneten Dienststellen für Anfragen im Zusammenhang mit der Sicherung von Beweismitteln zur Verfügung. Sollte im Zuge von Amtshandlungen technische Unterstützung oder eine Assistenzdienstleistung erforderlich werden und diese von Bezirks–IT–Ermittlerinnen und –Ermittlern oder in den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter nicht verfügbar sein, konnte über die Meldestelle um fachkundige Unterstützung angefragt werden. Die Meldestelle war zudem Schnittstelle zum Bereich Cyber Security im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung.

(2) Das Cybercrime Competence Center hatte – aufbauend auf einem bereits vorhandenen Entwurf – im August 2019 ein Grundkonzept zur Bekämpfung von Cyberkriminalität finalisiert. Ziel war es, dieses ergänzend zur Österreichischen Strategie für Cyber Sicherheit zu entwickeln. Damit sollten Cyberkriminalität–Ermittlungen sowie die elektronische Beweismittelsicherung in Österreich an den aktuellen Stand der Entwicklung angepasst und internationalen Bestrebungen in diesem Bereich gefolgt werden. Als Grundlage dienten vorangegangene Projekte wie DIGINT[40], internationale Beispiele (Deutschland, Norwegen und Belgien) sowie Erfahrungswerte der betroffenen Organisationseinheiten. Das Grundkonzept umfasste das Cybercrime Competence Center selbst sowie die Assistenzbereiche IT–Beweissicherung in den Landeskriminalämtern und die Bezirks–IT–Ermittlerinnen und –Ermittler. Der Bundesminister für Inneres sicherte Anfang Mai 2020 dem Cybercrime Competence Center

[39] Für den Betrieb der Meldestelle war ein Journaldienst eingerichtet, um die durchgehende Erreichbarkeit zu gewährleisten.

[40] Machbarkeitskonzept des Innenministeriums für die Bereiche Digitalisierung und Internetkriminalität

zusätzliche Arbeitsplätze zu. Abgesehen davon war zur Zeit der Gebarungsüberprüfung die Umsetzung offen.

Inhalte des Grundkonzepts betrafen Organisation, Personal, Aus– und Fortbildung sowie die Zusammenarbeit auf unterschiedlichen Ebenen. Die wesentlichen Maßnahmen sind in folgender Tabelle dargestellt:

Tabelle 14: Grundkonzept des Cybercrime Competence Centers zur Bekämpfung von Cyberkriminalität

Bereich	vorgeschlagene Maßnahmen (Auswahl)
Organisation	im Cybercrime Competence Center: Einrichtung von zwei bis drei Außenstellen in den Bundesländern, um das vorhandene Fachwissen auch in anderen Teilen des Landes zur Verfügung stellen zu können Einrichtung von mobilen Unterstützungseinheiten, die vor Ort die nötigen forensischen Sicherungsmaßnahmen durchführen könnten, damit auch weitere technische Ermittlungsschritte rechtzeitig gesetzt werden könnten (durchgehende Rufbereitschaft) Schaffung von spezialisierten Ermittlungseinheiten als „Untereinheiten“, da der Bereich der Cyberkriminalität–Ermittlungen eine immer höhere Spezialisierung erfordert Einrichtung einer Koordinierungsstelle, um den verschiedenen, im Bereich des Darknets sowie der Kryptowährungen ermittelnden Abteilungen innerhalb des Bundeskriminalamts einen Überblick zu bieten und die jeweiligen Ermittlungstätigkeiten aufeinander abstimmen zu können Einführung einer zusätzlichen Kategorisierung von Cyberkriminalität – Complex Cybercrime –, um künftig Ermittlungszuständigkeiten besser abgrenzen zu können; Definition von Complex Cybercrime als klassische Delikte, für deren Aufklärung spezielle technische Expertise nötig wäre bzw. bei denen Ermittlungsansätze vor allem im digitalen Raum zu suchen wären
	in den Landeskriminalämtern: Aufgliederung der bei den Landeskriminalämtern angesiedelten Assistenzbereiche IT–Beweissicherung – nach dem Vorbild des Cybercrime Competence Centers – in zwei Bereiche (elektronische Beweismittelsicherung, Cyberkriminalität–Ermittlungsarbeiten)
Personal	Rekrutierung von mehr qualifiziertem Personal sowie generell bundesweite Anhebung der Personalstände in diesem Bereich; Aufwertung der Stellung der Bezirks–IT–Ermittlerinnen und –Ermittler, u.a. durch Schaffung eigens bewerteter Planstellen (TZ 21)
Aus– und Fortbildung	Umsetzung des Ausbildungskonzepts für Cybercrime Competence Center und Assistenzbereiche IT–Beweissicherung; Etablierung von Cyberkriminalität als fixem Bestandteil der Polizeigrundausbildung und von Fortbildungen (TZ 34)

Quelle: Bundeskriminalamt

26.2 Der RH hielt fest, dass das Innenministerium im Bundeskriminalamt mit dem Cybercrime Competence Center eine auf die Bekämpfung von Cyberkriminalität spezialisierte Organisationseinheit eingerichtet hatte. Das Cybercrime Competence Center hatte aufbauend auf einem Entwurf mit dem Grundkonzept zur Bekämpfung von

Cyberkriminalität auch umfassende Vorschläge hinsichtlich Organisation, Personal sowie Aus– und Fortbildung sowohl im Bundeskriminalamt selbst als auch auf bundesweiter Ebene vorgelegt. Der RH kritisierte, dass – obwohl im Bereich Cyberkriminalität die Fallzahlen stark stiegen – das Innenministerium nicht adäquat reagierte und die Umsetzung des Grundkonzepts zur Zeit der Gebarungsüberprüfung noch offen war.

Der RH empfahl dem Innenministerium, 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.

26.3 Laut Stellungnahme des Innenministeriums werde es die Empfehlung aufgreifen. Neben einer entsprechenden Personaldotierung seien auch organisatorische Anpassungen im Bereich des Cybercrime Competence Centers geplant, um speziell auf neue Technologien oder Modi Operandi eingehen zu können. Besondere Schwerpunkte lägen dabei einerseits auf operativen Aufgaben, z.B. der Kooperativen Fallbearbeitung, mobilen Unterstützungseinheiten oder spezialisierten Ermittlungseinheiten, und andererseits auf „unterstützenden“ Aufgaben, z.B. elektronische Beweismittelsicherung, Multimediaforensik oder dem Digitalen Beweismittelmanagement.

Zuständigkeiten innerhalb des Bundeskriminalamts

27.1 (1) Die Zuständigkeiten innerhalb des Bundeskriminalamts waren durch die Geschäftseinteilung festgelegt. Im Hinblick auf Cyberkriminalität war zusätzlich der Grundsatzerlass zum Cybercrime Competence Center wesentlich.

Grundsätzlich lagen die operativen Ermittlungskompetenzen bei Cyberkriminalität im weiteren Sinn bei der jeweiligen Abteilung im Bundeskriminalamt. Eine originäre Ermittlungskompetenz des Cybercrime Competence Centers bestand nur für Cyberkriminalität im engeren Sinn. Für Cyberkriminalität im weiteren Sinn war diese gegeben, wenn zugleich zumindest ein Tatbestand von Cyberkriminalität im engeren Sinn vorlag und die zweckdienlichen Ermittlungsansätze überwiegend IT–technischer Natur waren. Zudem war das Cybercrime Competence Center für IT–Beweissicherung (Forensik) als Assistenzdienstleister zuständig.

(2) Das Cybercrime Competence Center arbeitete im Bereich Cyberkriminalität hauptsächlich mit der Abteilung Ermittlungen, Organisierte und Allgemeine Kriminalität und der Abteilung Wirtschaftskriminalität zusammen. Berührungspunkte bestanden z.B. beim Handel mit Waffen oder Suchtmitteln über das Darknet, bei der Verwendung von Kryptowährungen, im Rahmen der Bekämpfung von Kinderpornografie und des Kindesmissbrauchs, der Bearbeitung und Zusammenführung von

Tathandlungen in Zusammenhang mit Erpressungsmails oder im Bereich der Wirtschaftskriminalität.

In den vergangenen Jahren hatten sich viele Deliktsbereiche verstärkt in den Cyber Raum verlagert. Dabei waren die operativ ermittlungszuständigen Abteilungen wiederholt mit Fällen konfrontiert, für die spezielle technische Expertise notwendig war. In bestimmten Fällen war die Unterstützung durch Personal für digitale Forensik und mit technischem Spezialwissen als Assistenzdienstleistung bzw. mittels kooperativer Fallbearbeitung (z.B. bei Hausdurchsuchungen und forensischer Datenauswertung) erforderlich. Die Ermittlungszuständigkeit verblieb allerdings bei der Abteilung selbst. Für das Cybercrime Competence Center stand für eine effektive Fallbearbeitung oftmals die technische Ermittlungskompetenz im Vordergrund.

Das Cybercrime Competence Center und die Abteilungen Ermittlungen, Organisierte und Allgemeine Kriminalität sowie Wirtschaftskriminalität gaben an, dass grundsätzlich die Zuständigkeiten klar seien und die Zusammenarbeit gut funktioniere. Dennoch war in der Vergangenheit die operative Ermittlungszuständigkeit innerhalb des Bundeskriminalamts in Fällen, bei denen sowohl klassische Ermittlungsansätze als auch umfassende technische Ermittlungsansätze zu berücksichtigen waren, fallweise Gegenstand von Diskussionen, die letztlich die Leitung des Bundeskriminalamts entschied. Um solche Fälle künftig rascher und effektiver bearbeiten zu können, schlug das Cybercrime Competence Center in seinem Grundkonzept u.a. eine verstärkte kooperative Fallbearbeitung durch im Cybercrime Competence Center eingerichtete Ermittlungsgruppen sowie eine neue Kategorisierung „Complex Cybercrime“ vor.

(3) In der Abteilung Wirtschaftskriminalität war seit Dezember 2018 die Kompetenzstelle virtuelle Währungen und Kryptowährungen als Teil des Kompetenzzentrums Wirtschaftskriminalität eingerichtet. Definierte Aufgaben waren u.a. die Bündelung von Expertenwissen und Bereitstellung von rechtlicher und fachlicher Expertise, Durchführung von Schulungen, Erstellen eines Lagebilds und Erkennen von Trends sowie Support bei Ermittlungen. Außerdem sollte sie als Schnittstelle zu internen sowie externen (Forschungseinrichtungen, Ministerien etc.) Bedarfsträgern fungieren.

Für die Sicherstellung von Kryptowährungen sowie bei Ermittlungen in Zusammenhang mit Kryptowährungen waren technisches Expertenwissen und kriminalistisches Fachwissen erforderlich. Das Cybercrime Competence Center hatte einen Erlass zur Sicherstellung sowie ein diesbezügliches Nachschlagewerk für den Journaldienst im Cybercrime Competence Center erstellt. Es führte auch selbst Ermittlungen z.B. zu Smart Contracts (umgangssprachlich für Verträge oder Programmierungen in der Blockchain) durch.

Die Zuständigkeiten des Cybercrime Competence Centers und der Abteilung Wirtschaftskriminalität waren vor allem bei Ermittlungen nicht konkret definiert bzw. ausreichend voneinander abgegrenzt, womit wiederum über die Zuständigkeiten anlassbezogen entschieden werden musste.

27.2 Der RH hielt fest, dass die Zuständigkeit für Cyberkriminalität im Bundeskriminalamt grundsätzlich festgelegt war. In den vergangenen Jahren hatten sich klassische Delikte allerdings zusehends in den Cyber Raum verlagert und hatte sich die Bekämpfung von Cyberkriminalität zu einer Querschnittsmaterie entwickelt. 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.

Darüber hinaus war für den RH nicht nachvollziehbar, warum sowohl im Cybercrime Competence Center als auch in der Abteilung Wirtschaftskriminalität (in Form einer Kompetenzstelle) Zuständigkeiten für virtuelle Währungen und Kryptowährungen bestanden. Es fehlten auch eine klare Aufgabenfestlegung und –abgrenzung. Dadurch entstanden Kompetenzüberschneidungen bzw. Doppelgleisigkeiten.

Der RH empfahl dem Bundeskriminalamt, 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.

27.3 Laut Stellungnahme des Innenministeriums werde es diese Empfehlung aufgreifen und im Rahmen der geplanten Umsetzung eines umfassenden Personal– und Einsatzkonzepts berücksichtigen. Es werde auch eine klare Aufgabenfestlegung und –abgrenzung zwischen der Abteilung Wirtschaftskriminalität und dem Cybercrime Competence Center erarbeiten. Eine direkte Unterstützung im Aufgabenbereich der Abteilung Wirtschaftskriminalität sei erforderlich, um die stark steigende Zahl an Geldflussermittlungen bei Wirtschafts– und Betrugsdelikten sowie beim Asset Recovery Office und bei der Austrian Financial Intelligence Unit effizient zu bewältigen.

Grundlagen für die Personalbemessung

28.1 Das Bundeskriminalamt legte den Soll–Personalstand (Planstellen) und die Arbeitsplatzbewertungen – als Basis für die Verhandlungen mit dem Bundeskanzleramt bzw. dem Bundesministerium für öffentlichen Dienst und Sport[41] – im Zuge interner Evaluierungen fest, in welche auch das Cybercrime Competence Center eingebunden war. Die den Bediensteten zustehenden Bezüge waren von den Arbeitsplatzbewertungen bzw. der mit der Planstelle verknüpften Einstufung abhängig und richteten sich folglich nach dem Gehaltsschema des öffentlichen Dienstes. Für Bedienstete des Cybercrime Competence Centers waren die fachlichen Voraussetzungen aus Arbeitsplatzbeschreibungen ersichtlich und in Interessentensuchen weiter konkretisiert.

Das Cybercrime Competence Center legte in seinem Grundkonzept zur Bekämpfung von Cyberkriminalität einen zukünftigen Soll–Personalstand mit 160 Personen fest. Das Personal sollte zentral im Bundeskriminalamt sowie in zwei bis drei einzurichtenden Außenstellen tätig werden. Die 160 Personen würden einem Zuwachs von rd. 100 Bediensteten gegenüber dem Jahr 2019 entsprechen. Es sah den steigenden Personalbedarf insbesondere in den im Grundkonzept vorgesehenen zusätzlichen Ermittlungsaufgaben, im höheren Zeitaufwand für die Extraktion und Aufbereitung von Daten – bedingt durch die immer größer werdenden Datenmengen und zunehmenden Verschlüsselungsmöglichkeiten – sowie in der steigenden Anzahl auszuwertender Datenträger und Geräte begründet. Im Grundkonzept war kein Zeithorizont für den Personalzuwachs angegeben.

Das Cybercrime Competence Center erfasste die Gesamtzahlen der von ihm bearbeiteten Akten und ausgewerteten Asservaten (Verwahrstücken), wie z.B. Mobiltelefone. Dabei zeigte sich, dass insbesondere die Anzahl jener Akten, bei denen Assistenzdienste geleistet wurden, von 530 im Jahr 2016 auf 1.510[42] im Jahr 2019 anstieg. Dem im Grundkonzept festgelegten Soll–Personalstand legte das Cybercrime Competence Center jedoch nur teilweise konkrete Annahmen oder Kriterien zugrunde.

28.2 Der RH erachtete einen personellen Mehrbedarf des Cybercrime Competence Centers aufgrund der im Grundkonzept zur Bekämpfung von Cyberkriminalität vorgesehenen zusätzlichen Ermittlungsaufgaben und der steigenden Fallzahlen – insbesondere im Bereich der Assistenzdienstleistungen – als nachvollziehbar. Er vermisste jedoch Kriterien bzw. konkrete Annahmen – z.B. die weitere Entwicklung der Fallzahlen, die Bearbeitungsdauern oder die technische Entwicklung betreffend –, die als objektive Grundlage für einen zukünftigen Personalbedarf von 160 Personen dienten. Dadurch

[41] seit Jänner 2020: Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport

[42] Wert per 1. Dezember 2019

war nur bedingt feststellbar, welcher Personalstand beim Cybercrime Competence Center gegenwärtig und zukünftig angemessen war und ob die tatsächlichen Entwicklungen den getroffenen Annahmen entsprachen. Der RH hielt in diesem Zusammenhang fest, dass im Grundkonzept kein Zeithorizont für den personellen Mehrbedarf angegeben war.

Der RH empfahl daher dem Bundeskriminalamt, 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.

28.3 Das Innenministerium merkte in seiner Stellungnahme an, dass im Rahmen der geplanten organisatorischen Änderungen in den nächsten Jahren zusätzliche Bedienstete zur Abdeckung des zu erwartenden Personal–Mehrbedarfs aufgenommen werden würden.

Für den geplanten Mehrbedarf sei auf evidenzbasierte Erfahrungswerte zurückgegriffen worden, da gerade im Bereich der Bekämpfung von Cyberkriminalität – aufgrund dynamischer Entwicklungen und der stetigen technischen Weiterentwicklungen – die zukünftig auf das Cybercrime Competence Center zukommenden Aufgaben noch nicht konkret abschätzbar seien. Selbstverständlich werde auch weiterhin geprüft, ob die tatsächlichen Entwicklungen den getroffenen Annahmen entsprochen hätten, und werde erforderlichenfalls die Personalplanung geändert.

28.4 Der RH hielt fest, dass die vom Innenministerium in seiner Stellungnahme genannten evidenzbasierten Erfahrungswerte zur Zeit der Gebarungsüberprüfung nicht dokumentiert waren bzw. konkrete Annahmen als objektive Grundlage für die Bestimmung des zukünftigen Personalbedarfs fehlten. Dadurch war nur bedingt feststellbar, welcher Personalstand beim Cybercrime Competence Center gegenwärtig und zukünftig angemessen war. Er hielt daher seine Empfehlung aufrecht.

Entwicklung Personalstand

29.1 Der Personalstand des Cybercrime Competence Centers im überprüften Zeitraum ist aus der folgenden Tabelle ersichtlich:

Tabelle 15: Personalstand des Cybercrime Competence Centers

	2016	2017	2018	2019	2020	Veränderung 2016 bis 2020
	Anzahl zum 1. Jänner					in %
eingerichtete Planstellen	49	49	58	57	62	27
besetzte Planstellen	33	38	39	43	52	58
Vollzeitäquivalente[1]	39,50	41,75	52,50	62,75	63,50	61

[1] Differenz zu besetzten Planstellen aufgrund von Dienstzuteilungen und Personen, die über einen Personaldienstleister zur Verfügung standen

Quelle: Bundeskriminalamt

Der Personalstand des Cybercrime Competence Centers (in Vollzeitäquivalenten) stieg zwischen Jänner 2016 und Jänner 2020 um 61 %. Die Kosten für die Bediensteten – inklusive jener, die über einen Personaldienstleister zur Verfügung gestellt wurden – stiegen von 2,95 Mio. EUR im Jahr 2016 auf 4,79 Mio. EUR im Jahr 2019 und somit um 62 %.

In Zusammenhang mit dem Personalstand des Cybercrime Competence Centers hatte der RH in seinem Bericht „Bundeskriminalamt“ (Reihe Bund 2015/14, TZ 19) kritisiert, dass 55 % der vom Bundeskriminalamt für erforderlich erachteten Planstellen unbesetzt waren. Zur Zeit der nachfolgenden Follow–up–Überprüfung (Reihe Bund 2018/6, TZ 11) hatte der Fehlbestand 31 % betragen und es hatte weiter Probleme bei der Rekrutierung von geeignetem Personal gegeben.

Am 1. Jänner 2020 waren im Cybercrime Competence Center 52 der 62 (84 %) Planstellen besetzt. Bei den unbesetzten Planstellen handelte es sich vor allem um jene der Verwendungsgruppe A1 (Bedienstete mit Hochschulbildung). Im Gegenzug waren ihm am 1. Jänner 2020 zehn Personen der Verwendungsgruppe E2b (Exekutivbedienstete mit abgeschlossener Polizeigrundausbildung) dienstzugeteilt und drei Personen über einen Personaldienstleister zur Verfügung gestellt. Inklusive dieser Beschäftigten überstieg der Personalstand in Köpfen am 1. Jänner 2020 die Anzahl der genehmigten Planstellen.

29.2 Der RH merkte an, dass der Personalstand des Cybercrime Competence Centers zwischen Jänner 2016 und Jänner 2020 um 61 % anstieg und erachtete dies aufgrund der Entwicklung der Fallzahlen als nachvollziehbar.

Der RH hielt fest, dass der Anteil der besetzten Planstellen gegenüber den in früheren RH–Berichten dargelegten Fehlbeständen gestiegen war. Er verwies jedoch auf seine Feststellungen in TZ 30, wonach weiterhin Probleme bei der Rekrutierung von geeignetem Personal bestanden.

Personalrekrutierung

30.1 (1) Sowohl das Innenministerium als auch das Cybercrime Competence Center sahen die Akquise von qualifiziertem Personal als eine zentrale Herausforderung in der Bekämpfung von Cyberkriminalität. Das Cybercrime Competence Center setzte Maßnahmen des Employer Brandings und der Personalgewinnung z.B. durch Teilnahme an Berufsinformationsveranstaltungen, durch Vorträge in Schulen und im Zuge von Aus– und Fortbildungsveranstaltungen. Konkrete Personalsuchen erfolgten über die Jobbörse des Bundes, das Intranet des Innenministeriums oder über informelle Wege.

Im Cybercrime Competence Center waren Planstellen für unterschiedliche Verwendungsgruppen (z.B. E2a, A1 und A2) eingerichtet. Allerdings konnte aufgrund der bestehenden Rahmenbedingungen bei der Ausbildung (zur Ausbildung generell siehe TZ 32) und formellen Anforderungen u.a. im Innenministerium zum Teil bereits vorhandenes und fachlich geeignetes Personal nicht oder nur im Rahmen von Dienstzuteilungen eingesetzt werden.

(2) Fachkräfte, die z.B. als Quereinsteigende aus privatwirtschaftlichen Unternehmen zum Cybercrime Competence Center wechselten, durften – ohne die gesamte Exekutivausbildung unter gleichzeitiger niedriger Einstufung nachzuholen – keine kriminalpolizeilichen Ermittlungen leiten oder an dem kriminalpolizeilichen Exekutivdienst vorbehaltenen Amtshandlungen mitwirken. Die Ermittlungstätigkeit war aber neben forensischen oder Aus– und Fortbildungstätigkeiten nur eine von vielen Aufgaben.

Laut Auskunft des Cybercrime Competence Centers war es zudem problematisch, geeignetes und alle Voraussetzungen erfüllendes Personal (Technikerinnen und Techniker mit akademischem Abschluss) im Rahmen des Gehaltsschemas des öffentlichen Dienstes zu rekrutieren.

(3) Um dringend benötigte Personen rascher, als dies im regulären Aufnahmeprozess für Bundesbedienstete möglich wäre, aufnehmen bzw. ihnen eine Aufnahmezusage geben zu können, griff das Cybercrime Competence Center auch auf sogenanntes Payrolling zurück. Dabei schloss ein Personaldienstleister einen Dienstvertrag mit der ausgewählten Person, um diese anschließend im Zuge einer Arbeitskräfteüberlassung für das Cybercrime Competence Center diesem zuzuweisen.

Dadurch war es auch möglich, Expertinnen und Experten ein höheres Entgelt als gemäß dem Gehaltsschema des öffentlichen Dienstes zu zahlen.

Durch derartige Personalbereitstellungsmodelle über Dritte hatte der Personalplan des Bundes seine Steuerungsfunktion verloren. Folglich war die Transparenz hinsichtlich des Personalaufwands verringert (siehe Bericht „Justizbetreuungsagentur", Reihe Bund 2014/7, TZ 32).

(4) Das Regierungsprogramm 2020–2024 beinhaltete unter dem Punkt „Gute Rahmenbedingungen für eine moderne Polizei" u.a. die Entwicklung eines modernen, den sicherheitspolizeilichen Herausforderungen entsprechenden Dienst– und Besoldungssystems.

30.2 Der RH hielt fest, dass die Personalrekrutierung im Bereich Cyberkriminalität – auch aufgrund der Rahmenbedingungen, wie z.B. formelle Kriterien abseits der fachlichen Eignung, Gehaltsschema des öffentlichen Dienstes, Planstellenbewertungen, langwierige Aufnahmeprozesse, mangelnde Möglichkeiten für Quereinsteigende – eine große Herausforderung darstellte. Er anerkannte, dass sich das Cybercrime Competence Center bei unterschiedlichen Gelegenheiten (z.B. bei Berufsinformationsveranstaltungen, in Schulen oder bei Vorträgen) auch als potenzieller Arbeitgeber präsentierte.

Für den RH war in diesem Zusammenhang grundsätzlich auch nachvollziehbar, dass das Cybercrime Competence Center versuchte, das benötigte Personal auch mittels Payrolling zu gewinnen. Er wies jedoch darauf hin, dass durch diese Vorgehensweise der Personalplan des Bundes seine Steuerungsfunktion verliert und dass der Ausweis der überlassenen Arbeitskräfte im Sachaufwand zu geringerer Transparenz hinsichtlich des Personalaufwands führt.

Der RH merkte an, dass seiner Ansicht nach die Berufsbilder im Cybercrime Competence Center nur bedingt mit jenen anderer Organisationseinheiten des Innenministeriums vergleichbar bzw. dass sie mit anderen Schwerpunkten versehen waren. Er wies darauf hin, dass das Regierungsprogramm 2020–2024 unter dem Punkt „Gute Rahmenbedingungen für eine moderne Polizei" mehrere Maßnahmen anführte, u.a. auch die Entwicklung eines modernen, den sicherheitspolizeilichen Herausforderungen entsprechenden Dienst– und Besoldungssystems.

Der RH empfahl daher dem Innenministerium, in Zusammenarbeit mit dem zuständigen Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport 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.

30.3 Das Innenministerium wies in seiner Stellungnahme darauf hin, dass die Notwendigkeit evident sei, Rahmenbedingungen im Sinne eines modernen Personalmanagements zu schaffen, um das Innenministerium zukünftig als attraktiven Arbeitgeber auch für technische oder IT–Berufe zu positionieren. Das Innenministerium sei an einem interministeriell ausgelegten Projekt des Bundesministeriums für Kunst, Kultur, öffentlichen Dienst und Sport beteiligt, mit dem Ziel der Schaffung neuer Richtlinien im Bereich der Arbeitsplätze des Sondervertragsschemas Automatisierte Datenverarbeitung, einer damit verbundenen Modernisierung der zur Auswahl stehenden Rollen an IT–Arbeitsplätzen und somit einer gezielteren Ausrichtung auf die Anforderungen des Marktes.

Zur Erschließung des Marktes für geeignete und bereits in einem frühen Stadium der Anwerbung interessierte Bewerberinnen und Bewerber arbeite das Innenministerium auf der Ebene der strategischen Personalentwicklung an einem Maßnahmenbündel, das u.a. auch auf Kooperationen mit universitären Einrichtungen und technisch ausgerichteten Schulen abziele sowie über die Bewertung der betreffenden Arbeitsplätze hinaus attraktive Rahmenbedingungen für die Rekrutierung und auch Retention schaffe.

Bereits seit 2019 würden Arbeiten zwischen dem Innenministerium und dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport laufen, die insbesondere die zur Kriminalitätsbekämpfung erforderlichen Kompetenzen in den Bereichen IT, Cyberkriminalität etc. – und somit nicht nur Kompetenzen in den klassischen Segmenten – berücksichtigten.

30.4 Der RH nahm davon Kenntnis, dass das Innenministerium bereits seit 2019 mit dem Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport zusammenarbeitete, um ein Maßnahmenbündel zu schaffen, das das Innenministerium zukünftig als attraktiven Arbeitgeber auch für technische oder IT–Berufe positionieren sollte. Rahmenbedingungen für ein modernes Personalmanagement zu schaffen, stellte aus Sicht des RH jedoch – insbesondere angesichts laufend steigender Zahlen im Bereich Cyberkriminalität – eine dringliche Maßnahme dar. Er bekräftigte daher seine Empfehlung und wies darauf hin, dass die diesbezüglichen Arbeiten zeitnah zu Ergebnissen führen und die Empfehlung des RH entsprechend umgesetzt werden sollte. Er unterstrich in diesem Zusammenhang auch die zentrale Rolle geeigneten Personals bei der Bekämpfung von Cyberkriminalität.

Koordinierung der Auskunftsverlangen an Anbieter von Kommunikationsdiensten

31.1 (1) Wesentliches Element zur Aufklärung von Cyberkriminalität–Straftaten waren Auskünfte von Internetprovidern und Betreibern von sozialen Medien im In– und Ausland. Eine Ausforschung der zumeist anonymen Täterinnen und Täter z.B. mittels Zuordnung von Internetprotokoll (**IP**)–Adressen zu realen Personen war meist nur möglich, wenn der jeweilige Provider oder Forenbetreiber mitwirkte. Für österreichische Anbieter galten die Auskunftspflichten nach der StPO. Mit dem vom Justizministerium Anfang September 2020 zur Begutachtung ausgesendeten Gesetzesentwurf zum Bereich „Hass im Netz" soll laut Entwurf eine Ausweitung bzw. ausdrückliche Einbeziehung sonstiger Dienste der Informationsgesellschaft in die Auskunftspflicht erfolgen.

(2) Alle Polizeidienststellen führten im Zuge von kriminalpolizeilichen Ermittlungen derartige Ausforschungen durch bzw. regten nach Maßgabe der StPO deren Anordnung über die zuständige Staatsanwaltschaft an. Die Polizeidienststellen holten die Auskünfte unmittelbar bei den Betreibern oder über die Justiz im Wege internationaler Rechtshilfe (direkt mittels europäischer Ermittlungsanordnung innerhalb der EU oder über die zentrale Stelle im Justizministerium) ein.

Insbesondere ausländische Betreiber von Online–Diensten stellten an die Auskunftserteilung spezifische Anforderungen etwa hinsichtlich formaler Vorgaben für die Anfrage, beizustellender Dokumente bzw. Informationen oder hinsichtlich der Antwortwege (z.B. E–Mail, Online–Portal, Fax). In diesem Zusammenhang betrieb Europol das Projekt SIRIUS, das den Strafverfolgungsbehörden eine Plattform zum Austausch von Erfahrungen zur Verfügung stellte und Hilfestellungen leistete.

(3) Zur Zeit der Gebarungsüberprüfung führten Innen– und Justizministerium Gespräche zur Einrichtung eines „Single Point of Contact" (**SPOC**) für die einheitliche Übermittlung einschlägiger staatsanwaltschaftlicher Anordnungen an in– und ausländische Betreiber von sozialen Medien sowie Internetprovider. Generell begrüßten die Staatsanwaltschaften die Einrichtung eines SPOC ausdrücklich als Erleichterung und Steigerung der Erfolgsaussichten für Auskünfte.

Im Mai 2020 beauftragte die Leitung des Bundeskriminalamts ein Projekt „Zentrale Ansprechstelle Social Media und Provider" im Bundeskriminalamt. Der Start des Echtbetriebs war für Anfang 2021, das Projektende nach durchgeführter Evaluierung für Anfang 2022 vorgesehen.

31.2 Der RH hielt fest, dass die zur Aufklärung von Cyberkriminalität–Straftaten oftmals erforderliche Einholung von Auskünften bei Betreibern sozialer Medien und Internetprovidern durch unterschiedliche formale und inhaltliche Anforderungen erschwert war. Nach Ansicht des RH war es allerdings nicht zweckmäßig bzw. gar nicht möglich, umfassendes Know–how zu diesen unterschiedlichen Vorgaben bei allen befassten Dienststellen von Polizei und Justiz flächendeckend aufzubauen. Der RH beurteilte daher das Vorhaben von Innen– und Justizministerium, eine zentrale Koordinierungsstelle im Hinblick auf eine effektive und effiziente Arbeitsweise einzurichten, positiv. Durch eine anforderungsgerechte und raschere Übermittlung könnten die Erfolgsaussichten gesteigert und Auskunftsverlangen daher vermehrt eingesetzt werden. Weiters sollte dies ermöglichen, grundlegende Probleme mit einzelnen Betreibern rasch zu identifizieren und in der Folge zu beheben.

Der RH wies weiters darauf hin, dass mit der im Rahmen des Gesetzespakets zum Bereich „Hass im Netz“ geplanten ausdrücklichen Einbeziehung sonstiger Dienste der Informationsgesellschaft in die Auskunftspflicht nach der StPO die Anforderungen bei der Einholung von Auskünften weiter zunehmen werden.

Der RH empfahl dem Innenministerium, 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.

31.3 Laut Stellungnahme des Innenministeriums sei eine solche Koordinierungsstelle mit entsprechendem Know–how im Cybercrime Competence Center vorgesehen. Abstimmungen zu den rechtlichen Rahmenbedingungen fänden derzeit statt.

Aus– und Fortbildung im Innenministerium

Ausbildung generell

32 Den Einstieg in den (uniformierten) Dienst bei der Polizei bildete – nach erfolgreich absolviertem Aufnahmeverfahren – die zweijährige Polizeigrundausbildung. Nach deren Abschluss waren die Bediensteten in die Verwendungsgruppe E2b eingestuft und z.B. in Polizeiinspektionen eingesetzt. Für ein Tätigwerden als Bezirks–IT–Ermittlerin oder –Ermittler war eine ergänzende Ausbildung vorgesehen (TZ 33). Um in die mittlere Führungsebene des Polizeidienstes (Verwendungsgruppe E2a) aufsteigen und z.B. eine Polizeidienststelle führen oder im Kriminaldienst bei den Landeskriminalämtern oder dem Bundeskriminalamt tätig werden zu können, musste eine mindestens dreijährige Praxis nach Ernennung in die Verwendungsgruppe E2b nachgewiesen werden. Zusätzlich waren – nach erfolgreicher Auswahlprüfung – die sechsmonatige Grundausbildung für dienstführende Beamtinnen und Beamte und gegebenenfalls ein Zusatzmodul für den Kriminaldienst zu absolvieren.

Die Bediensteten des Cybercrime Competence Centers und der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter fungierten in den beschriebenen Ausbildungsschienen als Vortragende zu IT– oder Cyberkriminalität–Themen. Für ihre eigene Ausbildung lagen zwar Konzepte und Ergebnisse aus Projekten vor, die jedoch (noch) nicht umgesetzt wurden. Ein über alle Ebenen bedarfsabgestimmtes Konzept zur Vermittlung von IT– und Cyberkriminalität–Wissen existierte im Innenministerium nicht (TZ 34).

Ausbildung im Bereich Cyberkriminalität

33.1 (1) Die folgende Tabelle zeigt die zeitliche Entwicklung der Ausbildung der Bezirks–IT–Ermittlerinnen und –Ermittler:

Tabelle 16: Zeitliche Entwicklung der Ausbildung Bezirks–IT–Ermittlerinnen und –Ermittler

Zeitraum	Ereignis (Auswahl)
2012 bis 2014	Bezirks–IT–Ermittlerinnen und –Ermittler wurden in Form einer einwöchigen Ausbildung geschult und mussten eine zweimonatige Praxis bei den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter absolvieren. 276 Bezirks–IT–Ermittlerinnen und –Ermittler wurden nach diesem Schema ausgebildet.
2013 bis 2014	Das Cybercrime Competence Center erarbeitete ein Ausbildungskonzept Cybercrime Competence Center NEU im Auftrag der Leitung des Bundeskriminalamts. Es verwies dabei auf den fehlenden österreichweiten Mindestausbildungsstandard für den Fachbereich IKT.
2015	Das Innenministerium erachtete die Ausbildung der Bezirks–IT–Ermittlerinnen und –Ermittler in der geplanten Form als nicht finanzierbar. Es erteilte einer Arbeitsgruppe der Sicherheitsakademie den Auftrag, gemeinsam mit relevanten Fach– und Organisationseinheiten ein alternatives Ausbildungskonzept, insbesondere für die Bediensteten auf den Polizeiinspektionen und in den Bezirken, zu erarbeiten.
2016	Das Innenministerium erteilte den Auftrag, das Ausbildungskonzept umzusetzen.
2018	Die neue Bezirks–IT–Ermittler–Ausbildung ging in den Regelbetrieb über.

Quelle: Bundeskriminalamt

Im definierten Aufgabenprofil fanden sich u.a. die Vorbereitung und Durchführung von Beweismittelsicherungen im Bereich elektronischer Beweismittel und Auswertetätigkeiten. Die Bezirks–IT–Ermittlerinnen und –Ermittler sollten auch Kenntnis besitzen, wie sie Cyberkriminalitätsdelikte gesetzeskonform ermitteln und welche Ermittlungsmaßnahmen gesetzt werden konnten.

Die seit 2018 neue Ausbildung umfasste zum einen E–Learning–Module zu rechtlichen und Präventionsthemen sowie Präsenzschulungen im Bundeskriminalamt zu Themen wie Darknet, Kryptowährungen, IT–Ermittlungen, Forensik, Analyse oder Auswertungen. Zum anderen war im Bereich der forensischen Datensicherung bzw. Datenauswertung ein zweimonatiges Praktikum bei den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter zu absolvieren. Laut Erlass galt die Bezirks–IT–Ermittler–Ausbildung erst als abgeschlossen, wenn alle drei Ausbildungssäulen absolviert wurden.

Die in der Anfangsphase einwöchig geschulten Bezirks–IT–Ermittlerinnen und –Ermittler sollten eine ergänzende dreiwöchige Schulung durchlaufen, um ihr Wissen zu vertiefen.

(2) In mindestens zwei Schulungen pro Jahr sollten pro Kurs maximal 15 Personen geschult werden. In den Jahren 2018 und 2019 wurden in sieben Bezirks–IT–Ermittler–Schulungen in Summe 102 Personen ausgebildet. Aus vom RH geführten Interviews ging hervor, dass Teilnehmende das Einstiegsniveau der Ausbildung teilweise als zu hoch beurteilten. Darüber hinaus hatten im Jänner 2020 je nach Bundesland zwischen 51 % (Wien) und 86 % (Niederösterreich) der Bezirks–IT–Ermittlerinnen und –Ermittler die vorgesehene Grundausbildung noch nicht absolviert.

Während Bezirks–IT–Ermittlerinnen und –Ermittler in Kärnten dem Assistenzbereich IT–Beweissicherung im Zuge der Ausbildung – abweichend von den Vorgaben – drei Monate zugewiesen wurden, gab der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien an, dass er lediglich für eine bis zu zweiwöchige praktische Ausbildung zur Verfügung stand. Er verwies in diesem Zusammenhang auf die von den anderen Bundesländern abweichenden Tätigkeiten der Bezirks–IT–Ermittlerinnen und –Ermittler in Wien (TZ 23).

33.2 Der RH hielt kritisch fest, dass zwischen 2014 und 2018 für die Bezirks–IT–Ermittlerinnen und –Ermittler kein Mindestausbildungsstandard festgelegt und folglich kein einheitlicher Ausbildungsstand gegeben war. Er hielt fest, dass das Innenministerium erst ab dem Jahr 2018 eine standardisierte Ausbildung im Regelbetrieb umsetzte. Der RH kritisierte, dass im Jänner 2020 bundesweit zwischen 51 % und 86 % der Bezirks–IT–Ermittlerinnen und –Ermittler die für ihre Tätigkeit notwendige Ausbildung noch nicht absolviert hatten.

Der RH hielt fest, dass der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien lediglich für kürzere Praktika zur Verfügung stand, als dies in dem für alle Bundesländer geltenden Ausbildungsprogramm für Bezirks–IT–Ermittlerinnen und –Ermittler vorgesehen war. Nach Ansicht des RH wäre es jedoch im Sinne einer einheitlichen Ausbildung und im Hinblick auf mögliche Personalwechsel zwischen Bundesländern sinnvoll, wenn alle als Bezirks–IT–Ermittlerinnen und –Ermittler eingesetzten Personen die vorgesehenen Ausbildungssäulen – auch das Praktikum – in vollem Umfang durchlaufen.

Der RH empfahl daher dem Innenministerium, das Ausbildungsprogramm der Bezirks–IT–Ermittlerinnen und –Ermittler einheitlich umzusetzen und damit ein entsprechendes Qualitätsniveau sicherzustellen.

33.3 Laut Stellungnahme des Innenministeriums werde das einheitlich definierte Ausbildungsmodell für Bezirks–IT–Ermittlerinnen und –Ermittler seit 2018 umgesetzt und geschult, wobei bedarfsadäquate Anpassungen vorgesehen seien.

33.4 Der RH entgegnete, dass das Innenministerium zwar ab 2018 prinzipiell eine standardisierte Ausbildung der Bezirks–IT–Ermittlerinnen und –Ermittler im Regelbetrieb umsetzte, jedoch der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien lediglich für kürzere Praktika zur Verfügung stand, als dies in dem für alle Bundesländer geltenden Ausbildungsprogramm vorgesehen und im Sinne einer einheitlichen Ausbildung sinnvoll war.

34.1 (1) Die folgende Tabelle zeigt die zeitliche Entwicklung der Konzepterstellung für die Ausbildung der Bediensteten der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter und des Cybercrime Competence Centers:

Tabelle 17: Zeitliche Entwicklung der Ausbildungskonzepte Assistenzbereiche IT–Beweissicherung der Landeskriminalämter und des Cybercrime Competence Centers

Zeitraum	Ereignis (Auswahl)
2015	Eine Arbeitsgruppe der Sicherheitsakademie empfahl, die Ausbildung der Bediensteten des Cybercrime Competence Centers und der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter in einem eigenen Projekt (weiter) zu entwickeln.
2016	Das Cybercrime Competence Center führte in einem Bericht zum Status quo an, dass noch immer kein einheitlicher Ausbildungsmindeststandard im Bereich IT–Forensik und Cyberkriminalitätsbekämpfung vorhanden war. Dies führe zu „spürbar negativen Auswirkungen auf die Mitarbeitermotivation im Einsatz befindlicher IKT–Fachkräfte“ und „mangelndem Interesse für eine Laufbahn im Fachbereich Cyberkriminalitätsbekämpfung“.
2017 bis 2019	Das Cybercrime Competence Center erarbeitete ein Konzept zur Ausbildung für die eigenen Bediensteten und jene der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter. Dieses sah einen modularen Aufbau vor und beinhaltete als Grundausbildung für alle Bediensteten vorgesehene Module, solche für Quereinsteigende, für Fortgeschrittene sowie Expertinnen und Experten. Das Konzept sah drei Möglichkeiten einer Umsetzung vor und beurteilte sie hinsichtlich ihrer Vor– und Nachteile.

Quelle: Bundeskriminalamt

(2) Das Cybercrime Competence Center bevorzugte die Umsetzung in Form eines Ausbildungscampus im Innenministerium. Bei diesem sollten Fachlehrende und Administratoren auf Planstellen oder via Payrolling beschäftigt, die benötigte Infrastruktur erworben und die Schulungen in den eigenen Räumlichkeiten abgehalten werden. Die Gesamtkosten für fünf Jahre würden nach Berechnungen des Cybercrime Competence Centers – je nach konkreter Ausgestaltung – zwischen 7 Mio. EUR und 9 Mio. EUR liegen. Davon entfielen zwischen 47 % und 62 % auf Personalkosten. Es ging z.B. bei jeweils nur einem gleichzeitig stattfindenden Lehrgang von insgesamt sechs benötigten vollzeitbeschäftigten Lehrpersonen aus. Dieser Bedarf ergab sich aus der Überlegung, inhaltlich drei unterschiedliche Betriebssysteme abdecken zu können und in allen drei Bereichen gegen Ausfall des Lehrpersonals abgesichert zu sein. Zur Zeit der Gebarungsüberprüfung lag noch keine Entscheidung des Innenministeriums vor. Die Bediensteten der Assistenzbereiche IT–Beweissicherung der Landeskriminal-

ämter und des Cybercrime Competence Centers wurden daher weiterhin individuell in Form einzelner interner und externer Schulungen ausgebildet.

(3) Grundsätzlich durften nur Exekutivbedienstete kriminalpolizeiliche Ermittlungen leiten. Das Cybercrime Competence Center verfolgte daher in erster Linie den Ansatz, vorhandene Exekutivbedienstete im Bereich der IT bzw. im technischen Bereich zusätzlich auszubilden. In einigen Bundesländern Deutschlands war es z.B. für Absolventinnen und Absolventen einschlägiger Studiengänge mit Berufserfahrung möglich, nach einer zumindest einjährigen polizeispezifischen Ausbildung in die gehobene kriminalpolizeiliche Dienstlaufbahn – die Sonderlaufbahn Cyberkriminalist – einzusteigen.

Das Innenministerium dachte im Rahmen des Projekts DIGINT die Möglichkeit an, bereits technisch ausgebildetes Personal bzw. externe Fachkräfte mit verkürzter Polizeiausbildung einzusetzen. Das Cybercrime Competence Center und der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien sahen darin eine Ergänzung bzw. Alternative im Ausbildungsbereich und einen Beitrag zur Personalgewinnung.

In der Grundausbildung für dienstführende Beamtinnen und Beamte und in der Fachausbildung Kriminaldienst fanden sich Lehrveranstaltungen zum Thema Cyberkriminalität im Umfang von jeweils einem Tag. Das DIGINT–Projektteam erachtete es als notwendig, Grundlagenwissen bereits in der Polizeigrundausbildung zu vermitteln.

Das Cybercrime Competence Center stellte ab dem Jahr 2020 gemeinsam mit der Sicherheitsakademie Überlegungen an, bundesweite Mindeststandards zu digitalen Ermittlungen und digitaler Forensik in der Polizeigrundausbildung einzuführen.

34.2 Der RH kritisierte, dass das Innenministerium zur Zeit der Gebarungsüberprüfung noch keine standardisierte Ausbildung für die Assistenzbereiche IT–Beweissicherung der Landeskriminalämter und das Cybercrime Competence Center umgesetzt hatte.

In Zusammenhang mit dem vom Cybercrime Competence Center geplanten Ausbildungskonzept merkte der RH an, dass für ihn der angenommene Bedarf von sechs vollzeitbeschäftigten Fachlehrenden – und in weiterer Folge die veranschlagten (Personal–)Kosten, die mit bis zu 62 % der Gesamtkosten beziffert wurden – nicht nachvollziehbar war. Der RH wies darauf hin, dass es für fundierte Entscheidungen essenziell ist, die Gesamtkosten vorab möglichst exakt zu kennen.

Der RH hielt fest, dass im Innenministerium zur Ausbildung im Bereich Cyberkriminalitätsbekämpfung verschiedene Konzepte und Projektberichte vorlagen und das Thema z.B. auch in der Grundausbildung für dienstführende Beamtinnen und Beamte und in der Fachausbildung Kriminaldienst berücksichtigt wurde. Er kritisierte, dass

kein ganzheitliches, über alle Ebenen bedarfsabgestimmtes Ausbildungskonzept existierte.

Der RH hielt weiters fest, dass das Innenministerium Überlegungen zu alternativen Einstiegsmöglichkeiten und Berufsbildern bei den mit Cyberkriminalität befassten Organisationseinheiten anstellte. Er wies darauf hin, dass z.B. in Deutschland Systeme etabliert waren, die auch Quereinsteigenden aus privatwirtschaftlichen Unternehmen den Einstieg in die gehobene kriminalpolizeiliche Dienstlaufbahn ermöglichten, ohne die gesamte Ausbildung und Laufbahn im Exekutivbereich nachholen zu müssen.

Der RH empfahl daher dem Innenministerium, ein ganzheitliches, über alle Ausbildungsebenen bedarfsabgestimmtes Ausbildungskonzept für den Bereich Cyberkriminalität zu entwickeln und zeitnah umzusetzen; dabei wären getroffene Annahmen und finanzielle Auswirkungen angedachter Maßnahmen konkret darzulegen und zu berücksichtigen.

34.3 Laut Stellungnahme des Innenministeriums werde die Empfehlung aufgegriffen und fließe in die Ausarbeitung entsprechender Konzepte ein.

Fortbildung

35.1 (1) Wie in TZ 23 ausgeführt, gab es bei den Landeskriminalämtern keine eigenen Ermittlungsbereiche für Cyberkriminalität. Für die Bediensteten der Ermittlungsbereiche war daher standardmäßig auch keine diesbezügliche Ausbildung vorgesehen.

(2) Fortbildungen zu den Themen IT oder Cyberkriminalität für die im Kriminaldienst verwendeten Polizeibediensteten fanden im Rahmen der Schulungen gemäß Kriminaldienst–Fortbildungs–Richtlinie[43] statt. Diese halb– bis ganztägigen IT–Schulungen wurden ab dem Jahr 2017 durchgeführt.

Die Bediensteten der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter bildeten sich insbesondere im Rahmen der Kriminaldienstfortbildungen, bei Fachtagungen, in Workshops und auch in selbst oder extern organisierten Vorträgen, z.B. des Bundeskriminalamts, fort.

Der Schulungsaufgabe betreffend die Bezirks–IT–Ermittlerinnen und –Ermittler und der Vermittlung von Grundkenntnissen für alle Bediensteten der Landeskriminalämter und der nachgeordneten Dienststellen kam der Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien nach, soweit dies angesichts der eingeschränkten

[43] Richtlinie für die Organisation und Durchführung der berufsbegleitenden Fortbildung im Kriminaldienst

personellen Ressourcen möglich war und sich Bedienstete dafür freiwillig zur Verfügung stellten.

Die Bediensteten des Cybercrime Competence Centers besuchten im überprüften Zeitraum zahlreiche selbst organisierte oder externe Fortbildungsveranstaltungen. Dabei spielten auch internationale Bildungsangebote und Kooperationen eine wesentliche Rolle.

(3) Sämtliche von Bediensteten der Organisationseinheiten des Innenministeriums absolvierten dienstlichen Aus– und Fortbildungen sollten ab März 2017 im Bildungspass eingetragen, d.h. in einer zentralen elektronischen Datenbank erfasst werden. Dies geschah – auch aufgrund fehlender Meldungen extern absolvierter Veranstaltungen – für Bedienstete des Assistenzbereichs IT–Beweissicherung des Landeskriminalamts und des Cybercrime Competence Centers nicht durchgehend. Zur Zeit der Gebarungsüberprüfung unterstützte das Cybercrime Competence Center daher die vollständige Erfassung im Bildungspass, indem es die von den eigenen Bediensteten absolvierten Fortbildungsmaßnahmen zusätzlich dokumentierte.

(4) Bedienstete unterschiedlicher Abteilungen bzw. Bereiche und Hierarchieebenen des Landeskriminalamts Wien und des Bundeskriminalamts gaben an, dass das notwendige IT– und Cyberkriminalität–Basiswissen trotz der bestehenden Fortbildungsmöglichkeiten nicht bei allen Bediensteten vorhanden bzw. gewährleistet war. Sie wiesen auf technische Ermittlungsansätze bzw. den Internet–Bezug bei fast allen Delikten sowie die steigende Bedeutung der Bekämpfung von Cyberkriminalität als Querschnittsmaterie hin. Auch das DIGINT–Projektteam verortete Nachholbedarf im IT–Bildungsbereich sowie gravierende Mängel beim diesbezüglichen Wissensniveau.

35.2 Der RH anerkannte, dass die Bediensteten der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter und des Cybercrime Competence Centers sich in selbst organisierten und externen Veranstaltungen fortbildeten und auch als Vortragende zu IT– und Cyberkriminalität–Themen fungierten. Er hielt jedoch kritisch fest, dass im überprüften Zeitraum nicht alle dienstlichen Aus– und Fortbildungen systematisch erfasst wurden und daher kein vollständiger Überblick über den Aus– und Fortbildungsstand bestand. Dieser wäre aber im Sinne einer effizienten und wirksamen Personalentwicklung und –steuerung vor allem im Bereich Cyberkriminalität zweckmäßig.

Der RH empfahl dem Innenministerium, darauf hinzuwirken, dass alle Fortbildungen im Bereich Cyberkriminalität lückenlos in der zentralen elektronischen Datenbank, dem Bildungspass, erfasst werden.

Der RH hielt fest, dass in einigen Fortbildungsschienen für die Bediensteten unterschiedlicher Organisationseinheiten und Hierarchieebenen auch die Themen IT und Cyberkriminalität berücksichtigt wurden. Er wies jedoch kritisch darauf hin, dass die Bediensteten zum Teil trotzdem nicht über das für ihre Tätigkeit notwendige IT– bzw. Cyberkriminalität–Basiswissen verfügten. Angesichts der steigenden Bedeutung für nahezu alle Deliktsbereiche erachtete es der RH als essenziell, Bewusstsein für die Materie und Wissen in diesen Bereichen entsprechend breit zu verankern. Insbesondere für die ermittelnden Bediensteten erachtete er IT– bzw. Cyberkriminalität–Basiswissen als unerlässlich, damit sie Fälle möglichst umfassend selbstständig bearbeiten und technische Ermittlungsansätze verfolgen können. Gleichzeitig würden dadurch die schwerpunktmäßig mit den Themen IT bzw. Cyberkriminalität befassten Bediensteten und Organisationseinheiten entlastet.

Der RH empfahl daher dem Innenministerium, 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.

35.3 Zur lückenlosen Erfassung aller Fortbildungen in der zentralen elektronischen Datenbank teilte das Innenministerium in seiner Stellungnahme mit, dass diese Empfehlung mit März 2017 erlassmäßig umgesetzt worden sei. Darüber hinaus werde es die vom RH empfohlene Nacherfassung der noch nicht eingetragenen Bildungsveranstaltungen weiterverfolgen. An der möglichen Implementierung der in der Bundesverwaltung bereits im Einsatz befindlichen Lösung „Elektronisches Bildungsmanagement“ werde gearbeitet; diese könne einen über die reine Erweiterung der Erfassung von Fortbildungen hinausgehenden Mehrwert generieren.

Die empfohlene Sicherstellung des notwendigen Basiswissens in IT und Cyberkriminalität für alle ermittelnden Bediensteten sei durch die Implementierung der nachfolgenden spezifischen Schulungsangebote bereits umgesetzt:

Von Bediensteten sei 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. Die Dauer sowie der konkrete Inhalt richteten sich dabei nach den individuellen Bedarfen der Ermittlungs– bzw. Assistenzbereiche und würden daher auch jedes Jahr neu evaluiert und bei Bedarf adaptiert. Diesbezügliche Maßnahmen werde das Innenministerium auch in Zukunft weiterverfolgen.

35.4 Der RH anerkannte, dass die Themen IT und Cyberkriminalität in Schulungen berücksichtigt wurden. Jedoch war – laut Angaben von Bediensteten unterschiedlicher Abteilungen bzw. Bereiche und Hierarchieebenen des Landeskriminalamts Wien und des Bundeskriminalamts im Zuge der Gebarungsüberprüfung – das notwendige IT– und Cyberkriminalität–Basiswissen trotz der bestehenden Fortbildungsmöglichkeiten nicht bei allen Bediensteten vorhanden bzw. gewährleistet. Der RH hielt daher seine Empfehlung aufrecht.

Technische Unterstützung im Innenministerium

Infrastruktur

36 Für die Assistenz– und Ermittlungsleistungen im Bereich Cyberkriminalität waren sowohl spezielle Hardwarelösungen (z.B. leistungsstarke Auswerterechner, mobile Auswerteeinheiten, Speichermedien) als auch Softwarelösungen (z.B. Sicherungs–, Entschlüsselungs–, Auswertungssoftware) notwendig.

Das Cybercrime Competence Center beurteilte die Ausstattung in seinem Bereich als ausreichend.

Um auch einen Überblick über die infrastrukturellen Gegebenheiten bei den Bezirks–IT–Ermittlerinnen und –Ermittlern sowie den Assistenzdiensten IT–Beweissicherung der Landeskriminalämter zu erhalten, holte der RH die diesbezüglichen Informationen mittels schriftlicher Anfrage an die Landespolizeidirektionen ein.

Infrastruktur der Bezirks–IT–Ermittlerinnen und –Ermittler und der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter

37.1 (1) Laut Vorgabe des Innenministeriums sollten die Landespolizeidirektionen den Bezirks–IT–Ermittlerinnen und –Ermittlern die erforderliche Hard– und Software – im Wesentlichen Notebooks und Smartphones – zuweisen. Laut Angabe der Landespolizeidirektionen war diese Vorgabe in allen Bundesländern außer Niederösterreich und der Steiermark erfüllt. In Niederösterreich und der Steiermark waren zur Zeit der Gebarungsüberprüfung nur 50 % der Bezirks–IT–Ermittlerinnen und –Ermittler mit der vorgesehenen Hardware ausgestattet. Die Landespolizeidirektion Niederösterreich wies außerdem darauf hin, dass Bezirks–IT–Ermittlerinnen und –Ermittler an ihren Dienststellen über keine Auswerterechner verfügten und Beweismittel folglich beim Landeskriminalamt ausgewertet werden mussten. Dies mache Reisebewegungen notwendig und verursache zusätzlichen Zeitaufwand.

Zur Zeit der Gebarungsüberprüfung waren alle in Wien eingesetzten Bezirks–IT–Ermittlerinnen und –Ermittler mit der vorgesehenen technischen Ausrüstung ausgestattet. Sie verfügten an ihren Dienststellen jedoch nicht über jene Hard– und Software, die für die eigenständige und unmittelbare Sicherung und Auswertung der Inhalte mobiler Endgeräte notwendig war; sie mussten daher die Geräte zu diesem Zweck stets an den Assistenzbereich IT–Beweissicherung des Landeskriminalamts übermitteln. Ob oder wie zeitnah eine Sicherung des mobilen Endgeräts möglich war, hing auch von der Kooperationsbereitschaft der Opfer ab. So konnten in Fällen, in denen z.B. Opfer ihr Mobiltelefon nicht freiwillig für unbestimmte Dauer zur Verfügung stellen wollten, unter Umständen nicht alle Sicherungs– und Ermittlungsmöglichkeiten genutzt werden.

(2) Die Assistenzbereiche IT–Beweissicherung der Landeskriminalämter beurteilten ihre technische und räumliche Infrastruktur durchwegs als (noch) ausreichend. Verbesserungsbedarf bestand z.B. bei der Anzahl der Hardware, der Bandbreite der Internetanschlüsse und bei fehlenden Funktionsräumen.

Den zentralen Beschaffungsprozess über das Innenministerium erachteten die Assistenzbereiche IT–Beweissicherung überwiegend als langwierig und als nicht immer zweckmäßig. So seien durch die mehrere Monate oder Jahre dauernden Beschaffungsprozesse – aufgrund der raschen technischen Entwicklung – die ursprünglichen Anforderungen zum Zeitpunkt des Beschaffungsabschlusses oft bereits überholt. Auch seien die rechtlichen Rahmenbedingungen in Zusammenhang mit Ausschreibungen nur bedingt für die Beschaffung konkret spezifizierter Geräte geeignet. So konnten z.B. im Jahr 2017 vom Assistenzbereich IT–Beweissicherung des Landeskriminalamts Wien über das Innenministerium angeforderte und für die forensische Auswertung mobiler Endgeräte dringend benötigte Hard– bzw. Softwarelösungen erst im März 2019 – nach selbstständigem Ankauf durch die Landespolizeidirektion Wien – beschafft werden. In einem anderen Fall wurden die bereits im Jahr 2017 für die Jahre 2018 und 2019 als erforderlich gemeldeten Auswerteeinheiten (bestehend aus PC, Monitoren, Eingabegeräten, Betriebssystem und Software) dem Assistenzbereich erst im August 2019 übergeben.

Wie die Einschau des RH vor Ort zeigte, entsprach die räumliche Situation des Assistenzbereichs IT–Beweissicherung des Landeskriminalamts Wien nicht mehr den aktuellen Anforderungen. Der Assistenzbereich gab an, dass dies auch für die Netzwerkstruktur inklusive Internetanschlüsse – d.h. die zur Verfügung stehende Bandbreite – gelte. Die technische Infrastruktur sei ohne Gesamtkonzept gewachsen und teilweise veraltet. Der Leiter des Assistenzbereichs IT–Beweissicherung stellte daher wiederholt – letztmalig im Oktober 2019 – Anträge, um die Situation zu verbessern. Als Folge der mangelnden technischen und personellen Ressourcen war der Assistenzbereich IT–Beweissicherung mit der Untersuchung von Geräten bzw. der Aktenbearbeitung in Rückstand und führte daher ein Priorisierungssystem ein. Eine

möglichst zeitnahe Aktenbearbeitung war dabei z.B. in jenen Fällen von großer Bedeutung, in welchen durch Ermittlung der Täterinnen und Täter weitere Tatbegehungen verhindert und potenzielle Opfer geschützt werden könnten.

Im Zeitraum Oktober 2018 bis September 2019 langten in Summe 1.984 Mobiltelefone und SIM–Karten zur Untersuchung ein. Mit 1. Oktober 2019 war im Bereich der Forensik und mobilen Forensik eine beträchtliche Anzahl an Notebooks, Speichermedien, Mobiltelefonen, SIM–Karten, Tablet–PC und Navigationsgeräten seit mehreren Monaten zur Untersuchung offen. Der älteste im Oktober 2019 zur Bearbeitung offene Akt lag dem Assistenzbereich seit mehr als einem Jahr vor.

37.2 Der RH bemängelte, dass im überprüften Zeitraum nicht alle mit der Bekämpfung von Cyberkriminalität befassten Organisationseinheiten des Innenministeriums über die dafür zweckmäßige technische und räumliche Ausstattung verfügten. So waren z.B. in zwei Bundesländern (Niederösterreich und Steiermark) nur 50 % der Bezirks–IT–Ermittlerinnen und –Ermittler mit der vorgesehenen Hardware ausgestattet. Bei den Assistenzbereichen IT–Beweissicherung der Landeskriminalämter bestanden Defizite bei den Bandbreiten der zur Verfügung stehenden Internetanschlüsse und bei benötigten Räumen und Geräten. Die Beschaffungsprozesse waren nicht immer geeignet, den sich rasch entwickelnden und spezifischen technischen Anforderungen an die zu beschaffenden Geräte Rechnung zu tragen.

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

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 speziell 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. Der RH verwies auf seine Feststellungen und Empfehlungen in den TZ 21 bis TZ 24, TZ 26 bis TZ 30 und TZ 33 bis TZ 35.

Der RH empfahl dem Innenministerium, 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.

37.3 Das Innenministerium wies in seiner Stellungnahme darauf hin, dass Cyberkriminalität – 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 des Landeskriminalamts Wien ein Bedarf an Assistenzleistung festgestellt worden. Zum Zweck der Unterstützung für Ermittlungen im Bereich Cyberkriminalität seien bereits im Jahr 2019 im Zuge eines Probebetriebs bei der Landespolizeidirektion Wien in der Außenstelle des Landeskriminalamts Zentrum–Ost IT–Ermittlerinnen und –Ermittler des Assistenzbereichs IT–Beweissicherung zur Assistenzleistung zugewiesen worden.

Es sei nun intendiert, diesen Probebetrieb auf alle Außenstellen des Landeskriminalamts Wien zu erweitern und damit weitere Erkenntnisse gewinnen zu können. Grundsätzlich solle sich der Aufgabenbereich der in den Außenstellen eingesetzten Mitarbeiterinnen und Mitarbeiter des Assistenzbereichs IT–Beweissicherung auf Assistenzleistungen bei Cyberkriminalität im weiteren Sinn beziehen. Durch die Ausweitung des Probebetriebs auf alle Außenstellen des Landeskriminalamts Wien könne IT–spezifisches Know–how ziel– und bedarfsorientiert genau dorthin verlagert werden, wo es laufend benötigt werde, und so die Effizienz und Effektivität der Ermittlungen gesteigert werden. Dadurch werde dem wesentlich erhöhten Bedarf an einer komplexeren, effizienteren und qualitativ höherwertigen Bekämpfung der Cyberkriminalität Rechnung getragen.

37.4 Wie in seiner Gegenäußerung in TZ 25 wies der RH darauf hin, dass der Probebetrieb der IT–Ermittlerinnen und –Ermittler bereits zur Zeit der Gebarungsüberprüfung auf alle Außenstellen des Landeskriminalamts Wien ausgedehnt war und sich bewährt hatte. Allerdings betraf der Probebetrieb der IT–Ermittlerinnen und –Ermittler lediglich das Landeskriminalamt Wien. Dieser Probebetrieb allein war nach Ansicht des RH nicht ausreichend, um im Sinne seiner Empfehlung österreichweit angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen zu schaffen. Er hielt seine Empfehlung daher aufrecht.

Kriminalpolizeiliche Infrastruktur

38.1 (1) Sämtliche Dienststellen des Innenministeriums waren im BAKS im Rahmen eines geschlossenen Netzwerks verbunden. Über das BAKS hatten die Anwenderinnen und Anwender im Umfang ihrer Berechtigungen auch Zugang zu den Webapplikationen des Ministeriums (wie z.B. PAD, kriminalpolizeiliches Informationssystem EKIS, Erlasssammlungen, Lernplattformen oder verschiedene Lageberichte). Aus Sicherheitsgründen bestanden im BAKS restriktive Einstellungen.

Für den Kriminaldienst und kriminalpolizeiliche Tätigkeiten gab es keine eigenständige vernetzte IT–Infrastruktur. Wegen der restriktiven Sicherheitseinstellungen war eine operative Fallbearbeitung innerhalb des BAKS, vor allem auch im Bereich Cyberkriminalität, nicht bzw. nur sehr eingeschränkt möglich. Dies betraf insbesondere die Speicherung bzw. Archivierung kriminalpolizeilicher Ermittlungsdaten, den Einsatz spezifischer Software zur Fallbearbeitung und zur Auswertung elektronischer Beweismittel sowie uneingeschränkte Recherchemöglichkeiten im Internet.

Die Einschränkungen führten im kriminalpolizeilichen Bereich zu Insellösungen unter Verwendung von Standalone–Geräten. Diese mussten die betroffenen Dienststellen vielfach selbstständig betreiben und warten; eine fachgerechte, zentrale Servicierung durch das Innenministerium erfolgte nur eingeschränkt. Das Bundeskriminalamt gab an, im eigenen Bereich 80 solcher Geräte im Einsatz zu haben (außerhalb des Cybercrime Competence Centers).

(2) Um den mit der zunehmenden Digitalisierung verstärkten kriminalpolizeilichen Anforderungen entsprechen zu können, erstellte das Cybercrime Competence Center ein Grobkonzept für den Aufbau einer eigenen bundesweiten IT–Infrastruktur für kriminalpolizeiliche Zwecke. Im Oktober 2018 beauftragte der damalige Generalsekretär des Innenministeriums auf Basis dieses Grobkonzepts das Projekt „Kriminalpolizeiliche Infrastruktur“. Projektziel war es, eine eigene Plattform für alle für kriminalpolizeiliche Tätigkeiten notwendigen Applikationen oder Daten zu schaffen, die aus sicherheitstechnischen Gründen nicht im BAKS implementiert werden konnten. Die Umsetzung sollte mittels einer virtuellen IT–Infrastruktur erfolgen, die basierend auf der bestehenden IT–Infrastruktur des Ministeriums bzw. der dafür zuständigen Sektion IV (Service) betrieben wird. Weiters sollte eine Organisationseinheit aus 25 Fachexpertinnen und –experten für den laufenden Betrieb, die Wartung und die Integration von Anwendungsfällen eingerichtet werden. Das Projektende war für Ende März 2020 mit Abschluss des Pilotbetriebs und Überführung in die Linienorganisation vorgesehen.

Im Laufe des Jahres 2019 beschaffte das Innenministerium die für den Betrieb der kriminalpolizeilichen Infrastruktur erforderlichen Basiskomponenten (Server, Datenspeicher, Lizenzen) mit einem Auftragswert von rd. 750.000 EUR.

Die Umsetzung des Projekts verzögerte sich laut Information der zuständigen Sektion IV durch vorerst unklare und nicht genau spezifizierte Anforderungen sowie fehlende Budgetmittel und Personalressourcen. Die technische Plattform für die kriminalpolizeiliche Infrastruktur stehe seit Juni 2020 zur Verfügung. Auf dieser technischen Basis–Infrastruktur habe das Bundeskriminalamt nunmehr die virtuelle Umgebung für die kriminalpolizeiliche Infrastruktur einzurichten.

38.2 Der RH hielt fest, dass wesentlichen kriminalpolizeilichen Anforderungen innerhalb der regulären informationstechnologischen Infrastruktur des Innenministeriums, dem BAKS, wegen dessen restriktiver Sicherheitseinstellungen nicht entsprochen werden konnte. Das betraf insbesondere auch die für die Bekämpfung von Cyberkriminalität erforderlichen Instrumente zur Auswertung und Analyse elektronischer Beweismittel, zur Archivierung kriminalpolizeilicher Ermittlungsdaten oder zur Recherche im Internet. Dies machte den Einsatz von Standalone–Geräten notwendig und führte zu Insellösungen. Damit waren nach Ansicht des RH eine ausreichende Kontrolle, Wartung und Servicierung durch die zuständigen Stellen des Innenministeriums, eine einheitliche Nutzung von Softwareanwendungen sowie die Datensicherheit nicht durchgängig gewährleistet.

Der RH beurteilte daher die Bestrebungen des Innenministeriums, eine eigenständige kriminalpolizeiliche Infrastruktur einzurichten, als zweckmäßig. Im Rahmen des dazu bestehenden Projekts sollten Defizite im Bereich der Kriminalpolizei behoben und die Voraussetzungen für ein System zur Analyse großer Datenmengen und zum sicheren Datenaustausch mit der Justiz (TZ 46, TZ 47) geschaffen werden. Er kritisierte allerdings, auch unter Verweis auf die bereits getätigten Investitionen von rd. 750.000 EUR, die deutlich verzögerte Umsetzung.

Der RH empfahl dem Innenministerium, den Aufbau einer eigenständigen kriminalpolizeilichen Infrastruktur unter Bedachtnahme auf Kosten–Nutzen–Aspekte sicherzustellen, um eine zeitgemäße und anforderungsgerechte IT–Infrastruktur für kriminalpolizeiliche Ermittlungen, insbesondere zur Bekämpfung von Cyberkriminalität, zu gewährleisten.

Er empfahl weiters, im Zusammenwirken mit den Bedarfsträgern einheitliche und sichere Softwarelösungen für den kriminalpolizeilichen Bereich im Rahmen der geplanten kriminalpolizeilichen IT–Infrastruktur zu etablieren sowie deren Servicierung sicherzustellen.

38.3 Laut Stellungnahme des Innenministeriums werde die Empfehlung zum Aufbau einer eigenständigen kriminalpolizeilichen Infrastruktur im Rahmen eines bereits gestarteten Projekts umgesetzt.

Die Empfehlung zur Etablierung einheitlicher und sicherer Softwarelösungen in diesem Bereich werde aufgegriffen und im Rahmen eines entsprechenden Projekts Berücksichtigung finden.

Aktenführung und –übermittlung an die Staatsanwaltschaft

39.1 Die Dienststellen im Bereich der Landespolizeidirektionen erfassten Strafanzeigen sowie die zugehörigen Ermittlungsmaßnahmen und –ergebnisse aktenmäßig im PAD. Aus dieser Applikation übermittelten sie auch ihre Berichte samt Beilagen automationsunterstützt an die zuständige Staatsanwaltschaft im Wege des Elektronischen Rechtsverkehrs (**ERV**).

Das Bundeskriminalamt verwendete für die Fallbearbeitung grundsätzlich die Integrierte Kriminalpolizeiliche Datenanwendung (**IKDA**). Diese Applikation war nur für die Aktenverwaltung in Form eines Workflows, nicht aber zur generellen Führung der Ermittlungsakten oder zur Berichtslegung an die Staatsanwaltschaft mittels ERV geeignet. Ein automationsunterstützter Austausch mit nachgeordneten Dienststellen – z.B. Übermittlungen von Anzeigen oder Ermittlungsergebnissen zur übergeordneten Bearbeitung von Cyberkriminalität–Massendelikten oder im Rahmen von Sonderkommissionen beim Bundeskriminalamt – war mangels Schnittstelle zwischen dem PAD und IKDA nicht möglich. Die Versendung musste daher nach Aufbereitung jeweils per E–Mail oder in physischer Form (etwa per Post oder Boten) erfolgen.

Lediglich einige Fachbereiche des Bundeskriminalamts (Büro für Organisierte Kriminalität, Referate Cold Case Management sowie Sexualstraftaten und Kinderpornografie) verfügten zusätzlich über einen vollen Zugang zum PAD und übermittelten daraus auch die Berichte mittels ERV an die Staatsanwaltschaft.

39.2 Der RH hielt kritisch fest, dass das Bundeskriminalamt nicht umfassend in das bei allen anderen kriminalpolizeilichen Dienststellen verwendete zentrale Aktenverwaltungssystem PAD eingebunden war. Dies erschwerte den internen Informationsaustausch im Rahmen übergreifender Ermittlungen z.B. bei Cyberkriminalität–Massendelikten oder bei Sonderkommissionen. Weiters war dadurch eine automationsunterstützte Berichterstattung bzw. Aktenübermittlung an die Staatsanwaltschaft mittels ERV nicht möglich.

Der RH empfahl daher dem Innenministerium, alle mit kriminalpolizeilichen Ermittlungen befassten Organisationseinheiten des Bundeskriminalamts umfassend in die zentrale Applikation Protokollieren, Anzeigen, Daten (PAD) einzubinden, um einen vollständig automationsunterstützten Informations– und Aktenaustausch mit den nachgeordneten Polizeidienststellen wie auch mit den Staatsanwaltschaften sicherzustellen.

39.3 Laut Stellungnahme des Innenministeriums finde im Bereich des Bundeskriminalamts derzeit ein Probebetrieb zur Bewertung der Vor– und Nachteile sowie der notwendigen Kosten einer Einbindung der zentralen Applikation PAD statt. Abhängig vom Evaluierungsergebnis werde es nach Abschluss des Probebetriebs weitere Maßnahmen setzen.

Lagebild Cyberkriminalität

40.1 (1) Ein automationsunterstützter Abgleich von Fällen der Polizeidienststellen mit relevanten Daten anderer im PAD erfasster Fälle war aus datenschutzrechtlichen Gründen nicht zulässig und daher nicht möglich. Die Bediensteten bei den Landeskriminalämtern konnten im PAD innerhalb des eigenen Bundeslands Übereinstimmungen zwischen Fällen recherchieren, bundesländerübergreifende Abfragen waren nicht möglich.

Für Statistik– oder Analysezwecke waren – jeweils nach datenschutzrechtlicher Genehmigung – zentrale Datenanwendungen des Bundeskriminalamts eingerichtet, die nach vorgegebenen Kriterien mittels automatisierten Datentransfers aus dem PAD mit relevanten Daten befüllt wurden. Solche Anwendungen waren z.B. die Kriminalstatistik, der Sicherheitsmonitor[44] oder sogenannte Lagebilder zu spezifischen Kriminalitätsbereichen. Lagebilder bestanden zur Zeit der Gebarungsüberprüfung des RH z.B. für Raub, illegale Migration, Kraftfahrzeugdiebstahl oder Falschgeld, nicht aber für Betrug oder Cyberkriminalität.

Der RH hatte in seinem Bericht „Bundeskriminalamt“ (Reihe Bund 2015/14, TZ 27) festgehalten, dass Lagebilder eine gute Methode zur Erkennung von Kriminalitätsentwicklungen bilden. Er hatte in diesem Zusammenhang kritisiert, dass ein Lagebild für den Bereich Betrug fehlte, und empfohlen, ein solches möglichst rasch zu entwickeln. Dies wäre wichtig, um überregionale Verflechtungen insbesondere bei Tatbegehung unter Verwendung elektronischer Medien erkennen zu können.

(2) Im Rahmen eines geförderten[45], gemeinsam mit Universitäten, Finanzdienstleistern und einem Forschungsberatungsunternehmen betriebenen Projekts arbeitete die Abteilung Wirtschaftskriminalität des Bundeskriminalamts seit dem Jahr 2014 u.a. an der Entwicklung eines Lagebilds Cyberkriminalität; dies insbesondere im Hinblick auf die Bekämpfung von Internetbetrug. Das Innenministerium selbst trafen keine Finanzierungsverpflichtungen daraus. Es beteiligte sich mit einem Personalein-

[44] Der Sicherheitsmonitor lieferte als Führungsinstrument für kurz– und mittelfristige Planungen (im Gegensatz zur Kriminalstatistik) aktuellste Informationen zum Kriminalitätsgeschehen, z.B. hinsichtlich zeitlicher Entwicklungen oder regionaler Häufungen.

[45] Die Förderung erfolgte im Rahmen von KIRAS, einem nationalen Programm zur Förderung der Sicherheitsforschung in Österreich.

satz von 13 Personenmonaten, was auf Basis der durchschnittlichen Personalkosten des Bundes im Jahr 2019 rd. 127.000 EUR entsprach.

Im Jahr 2016 erstellte das Forschungsberatungsunternehmen ein Grobkonzept für die Prozesse eines Lagebilds Cyberkriminalität. Der zuständige Rechtsschutzbeauftragte des Innenministeriums erteilte der auf dem Grobkonzept basierenden Applikationsbeschreibung die datenschutzrechtliche Genehmigung.

In der Folge entwickelten die Projektpartner den Prototyp einer Schnittstellen–Software für die Übernahme bestimmter Daten zu Betrugsfällen aus dem PAD, der aber nach einer Systemumstellung auf das „PAD der nächsten Generation (PAD NG)" Anfang 2018 nicht mehr funktionsfähig war. Eine Einbindung der für Kriminalanalyse zuständigen Abteilung des Bundeskriminalamts sowie des Cybercrime Competence Centers erfolgte erst im Rahmen einer Besprechung im Juli 2019.

Im März 2020 entschied die Leitung des Bundeskriminalamts, das bei der Abteilung Wirtschaftskriminalität geführte Projekt Lagebild Cyberkriminalität zu beenden. Gleichzeitig beauftragte sie das Cybercrime Competence Center mit der Entwicklung eines umsetzungsfähigen Projekts.

(3) Bereits im Februar 2020 hatte das Bundeskriminalamt die Entscheidung getroffen, die Entwicklung des Lagebilds Cyberkriminalität in ein Projekt zur grundlegenden Neugestaltung aller bestehenden Lagebilder einzubeziehen. Wesentlicher Grund dafür war, dass die Lagebilder – wie auch andere Applikationen zur Kriminalitätsanalyse – über jeweils eigene Schnittstellen aus dem PAD befüllt wurden. Programmtechnische Änderungen des PAD machten daher auch gesonderte, mit zusätzlichen Kosten verbundene Anpassungen der Schnittstellen erforderlich. Mit dem Projekt zur Überarbeitung u.a. aller Lagebilder sollten eine allgemeine, einheitliche Schnittstelle geschaffen und damit künftig Kosten gespart werden.

40.2 Der RH hielt fest, dass es die beim Bundeskriminalamt für spezifische Kriminalitätsbereiche geführten Lagebilder ermöglichten, relevante Informationen zu den angezeigten Straftaten bundesweit zusammenzuführen. Er kritisierte, dass für den stark ansteigenden Bereich Cyberkriminalität kein solches Lagebild bestand. Nach Ansicht des RH war es gerade im Bereich Cyberkriminalität im Hinblick auf effiziente Ermittlungen und zur Vermeidung von Doppelgleisigkeiten wesentlich, anhand des Abgleichs bestimmter Daten Zusammenhänge zwischen Straftaten dem Grunde nach und ohne Zeitverlust zu erkennen. Solche Daten konnten vor allem E–Mail– oder IP–Adressen, Kontonummern, Namen oder Firmenbezeichnungen sein.

Der RH kritisierte daher, dass das Bundeskriminalamt das bereits seit 2014 laufende Projekt Lagebild Cyberkriminalität nicht abgeschlossen hatte. Seiner Ansicht nach war dies auch auf die nicht ausreichend abgestimmte Vorgehensweise innerhalb des

Bundeskriminalamts zurückzuführen. Weiters kritisierte der RH, dass ein bereits erarbeiteter Prototyp des Lagebilds Cyberkriminalität nach der Umstellung der Basisapplikation nicht mehr funktionsfähig war. Damit entstand dem Innenministerium aus dem Projekt ein frustrierter Personalaufwand.

Der RH empfahl dem Bundeskriminalamt, zeitnah ein Lagebild Cyberkriminalität einzurichten, das es ermöglicht, Zusammenhänge zwischen Straftaten im Bereich Cyberkriminalität möglichst rasch erkennen zu können, und dabei die im Rahmen eines Vorprojekts gemachten Erfahrungen zu berücksichtigen.

Der RH hielt auch kritisch fest, dass die für die Lagebilder bzw. sonstigen Analyseinstrumente mit Datenübernahmen aus dem PAD bestehenden, jeweils eigenen Schnittstellen vermeidbare Kosten verursachten. Das Vorhaben des Bundeskriminalamts, eine gemeinsame Schnittstelle einzurichten, erachtete der RH daher als zweckmäßig.

Der RH empfahl dem Bundeskriminalamt, eine gemeinsame Schnittstelle für alle Lagebilder und sonstigen Anwendungen, die Daten aus der Applikation Protokollieren, Anzeigen, Daten (PAD) übernehmen, zeitnah umzusetzen.

40.3 Laut Stellungnahme des Innenministeriums sei eine entsprechende gemeinsame Schnittstelle bereits in Planung. Nach deren Fertigstellung solle das Lagebild „Cybercrime“ umgesetzt werden.

Organisation und Personaleinsatz im Justizministerium

Zusammenwirken Kriminalpolizei und Justiz bei der Verfolgung von Cyberkriminalität

41 Die Strafprozessordung (StPO) bildet die Grundlage für das Strafverfahren in Österreich, das sich in Ermittlungs– und Hauptverfahren unterteilt.

Die Kriminalpolizei ermittelt auf der Grundlage von Anzeigen oder eigenen Wahrnehmungen in der Regel selbstständig den Sachverhalt und Tatverdacht. Sobald diese geklärt sind, übermittelt sie einen Abschlussbericht an die Staatsanwaltschaft. Diese entscheidet, ob sie Anklage erhebt und somit das Hauptverfahren einleitet, von der Verfolgung zurücktritt (Diversion) oder das Verfahren einstellt. Bei unbe-

kannter Täterschaft bricht die Staatsanwaltschaft das Ermittlungsverfahren in der Regel ab.

Die Zusammenarbeit zwischen Kriminalpolizei und Staatsanwaltschaft ist regelmäßig bereits zu einem früheren Zeitpunkt im Ermittlungsverfahren notwendig. Im Bereich Cyberkriminalität ist dies insbesondere der Fall, wenn

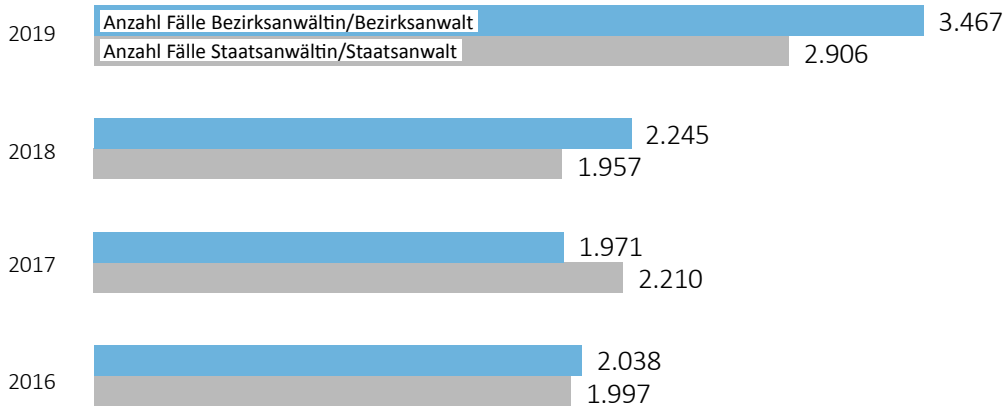
- es sich um eine schwerwiegende Straftat oder eine von besonderem öffentlichem Interesse handelt und die Staatsanwaltschaft daher unmittelbar eingebunden werden muss,
- die Kriminalpolizei Bewilligungen (Anordnungen) der Staatsanwaltschaft benötigt, z.B. für Auskünfte von Internetprovidern und Betreibern von sozialen Medien, um Datenträger sicherzustellen oder um nach gerichtlicher Bewilligung Hausdurchsuchungen durchführen zu können oder
- große Datenmengen bzw. komplexe Daten zu sichern, auszuwerten sowie zu archivieren sind.

Zuständigkeiten für Ermittlungsverfahren im Bereich Cyberkriminalität

42.1 (1) Die Führung der Ermittlungsverfahren oblag grundsätzlich den bei den Landesgerichten eingerichteten Staatsanwaltschaften. Je nachdem, ob ein etwaiges Hauptverfahren beim Landes– oder Bezirksgericht zu führen wäre, war für die Bearbeitung eine Staatsanwältin bzw. ein Staatsanwalt oder eine Bezirksanwältin bzw. ein Bezirksanwalt zuständig. Im Regelfall war bei Vergehen oder Verbrechen mit einer Strafdrohung von bis zu einem Jahr Freiheitsstrafe das Bezirksgericht, ansonsten das Landesgericht zuständig. Bei den Cyberkriminalitätsdelikten im engeren Sinn richtete sich die Strafdrohung in der Regel nach der Höhe des eingetretenen Schadens oder nach besonderen Tatumständen (Zuständigkeit Landesgericht z.B. ab definierter Schadenshöhe, bei kritischer Infrastruktur als Angriffsziel oder bei Begehung durch eine kriminelle Vereinigung).

(2) Im Bereich Cyberkriminalität im engeren Sinn verteilten sich die angefallenen Ermittlungsverfahren nach Zuständigkeit der Bezirksanwältinnen bzw. Bezirksanwälte und Staatsanwältinnen bzw. Staatsanwälte in den Jahren 2016 bis 2019 wie im Folgenden dargestellt. Der RH errechnete diese Zahlen anhand von Auswertungen der zur Verfahrensunterstützung eingesetzten Applikationen. Bezüglich der eingeschränkten Zuverlässigkeit und Aussagekraft der Zahlen des Justizministeriums verwies er auf seine Ausführungen in den TZ 4 und TZ 5.

Abbildung 4: Zuständigkeitsverteilung für Cyberkriminalität (im engeren Sinn) im Ermittlungsverfahren der Staatsanwaltschaften



Quelle: BMJ; Berechnung und Darstellung: RH

Der deutliche Zuwachs bei den Ermittlungsverfahren zu Cyberkriminalität im Jahr 2019 war vor allem auf die Entwicklungen beim Betrügerischen Datenverarbeitungsmissbrauch zurückzuführen. Dessen Anteil an den Cyberkriminalität–Fällen lag 2016 bei 37 %, im Jahr 2019 waren es 60 %.

42.2 Der RH hielt fest, dass im überprüften Zeitraum bei den erledigten Ermittlungsverfahren zu Cyberkriminalität (im engeren Sinn) tendenziell die Zuständigkeit der Bezirksanwältinnen und –anwälte leicht überwog.

Organisation der Staatsanwaltschaften in Cyberkriminalität–Ermittlungsverfahren

43.1 (1) Für die Ermittlungsverfahren im Bereich Cyberkriminalität galten die in der StPO festgelegten allgemeinen örtlichen Zuständigkeitsregeln.[46] In den wenigen Fällen von Internetbetrug oder Betrügerischem Datenverarbeitungsmissbrauch mit einer vermuteten Schadenssumme von über 5 Mio. EUR konnte eine bundesweite Zuständigkeit der Zentralen Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (**WKStA**) zum Tragen kommen. Die WKStA verfügte im Gegensatz zu den anderen Staatsanwaltschaften über eigene – bei der Justizbetreuungsagentur angestellte und der Behörde zur Verfügung gestellte – Expertinnen bzw. Experten für IT.

Auch innerhalb der Staatsanwaltschaften gab es keine Spezialisierung für Cyberkriminalität (im engeren Sinn). Zu Cyberkriminalität im weiteren Sinn bestanden zwar grundsätzlich Sonderzuständigkeiten für Delikte aus dem Bereich strafbarer Handlungen gegen die sexuelle Integrität und Selbstbestimmung, dafür war allerdings nicht die Cyberkriminalität–Komponente ausschlaggebend. Bei der Staatsanwaltschaft Wien bestanden Abteilungen, die für jene Paragrafen des StGB und Verbotsgesetzes zuständig waren, die auch unter den Begriff „Hass im Netz" subsumiert wurden. Eine verstärkte fachliche und methodische Unterstützung bei Ermittlungsverfahren zu Cyberkriminalität, z.B. die Etablierung spezialisierter interner Ansprechstellen oder ein Leitfaden zur Hilfestellung bei Cyberkriminalität–Ermittlungen für Bedienstete mit geringerer Erfahrung, gab es nicht. Dies wäre aber nach Auskunft der Leitung und von Staatsanwältinnen bzw. –anwälten der Staatsanwaltschaft Wien zweckmäßig.

(2) Der Bereich Cyberkriminalität stellte nicht nur die Polizei, sondern auch die Staatsanwaltschaften vor besondere Herausforderungen. Dies betraf z.B. die oftmals internationale Dimension von Cyberkriminalität, neu auftretende kriminelle Phänomene, das einschlägige Know–how der Täterinnen und Täter, Handlungen zur Identitätsverschleierung im Internet oder auch die teilweise große Menge auszuwertender Daten. Bei unbekannter Täterschaft richtete sich die örtliche Zuständigkeit der Staatsanwaltschaften in der Regel nach dem Ort des Schadenseintritts (Wohnort des jeweiligen Opfers), was insbesondere bei an sich zusammengehörigen Massendelikten zu einer

[46] Gemäß § 25 StPO ist grundsätzlich jene Staatsanwaltschaft zuständig, in deren Sprengel die Straftat ausgeführt wurde oder ausgeführt werden sollte. Liegt dieser Ort im Ausland oder kann er nicht festgestellt werden, so ist der Ort maßgebend, an dem der Erfolg eingetreten ist oder eintreten hätte sollen.

auf unterschiedliche Staatsanwaltschaften zersplitterten Bearbeitung führen[47] und das Finden geeigneter Ermittlungsansätze erschweren konnte.

Im Hinblick auf diese besonderen Herausforderungen richtete im Vergleich dazu z.B. in Deutschland das Bundesland Nordrhein–Westfalen eine Zentral– und Ansprechstelle Cyberkriminalität mit überregionaler Zuständigkeit für herausgehobene Ermittlungsverfahren im Bereich der Internetkriminalität und als bundesweite Ansprechstelle für grundsätzliche, verfahrensunabhängige Fragestellungen ein. Auch in anderen deutschen Bundesländern wurden Schwerpunktstaatsanwaltschaften oder eigene Abteilungen zur Bekämpfung von Internetkriminalität errichtet.

Der Evaluierungsbericht des Rates der EU aus 2017 enthielt die Empfehlung, „auf die Bekämpfung von Cyberkriminalität spezialisierte Staatsanwälte zu ernennen und/oder den Kenntnisstand und die Zahl der Fachstaatsanwälte (und –richter) für die einzelnen Arten von Cyberkriminalität zu erhöhen".

Auch das Regierungsprogramm 2020–2024 beinhaltete Maßnahmen im Sinne einer Cyberkriminalität–Spezialisierung bei den Staatsanwaltschaften.

43.2 Nach Ansicht des RH waren die Staatsanwaltschaften im Hinblick auf die besonderen Herausforderungen bei der wirksamen Bekämpfung von Cyberkriminalität organisatorisch und methodisch nicht ausreichend gerüstet. Die fehlende Spezialisierung und fehlende organisatorische Verankerung bei den Staatsanwaltschaften im Bereich Cyberkriminalität sah er daher kritisch.

Der RH erachtete es als zweckmäßig, zumindest Grundkenntnisse z.B. hinsichtlich der ermittlungstechnischen Möglichkeiten oder der gezielten Informationsgewinnung und –aufbereitung bei den Staatsanwaltschaften flächendeckend zu etablieren (TZ 45) sowie eine Spezialisierung bei der Führung von Ermittlungsverfahren im Bereich Cyberkriminalität zu erreichen. Zum Beispiel könnten dazu eigene Ansprechstellen zur Unterstützung bei Cyberkriminalität–Ermittlungen eingerichtet oder Sonderzuständigkeiten festgelegt werden.

Der RH empfahl dem Justizministerium, basierend auf internationalen Beispielen und den Erfahrungen besonders betroffener Staatsanwaltschaften organisatorische Rahmenbedingungen für eine spezialisierte Bearbeitung von Ermittlungsverfahren im Bereich Cyberkriminalität festzulegen.

[47] Zum Beispiel übernahm die Staatsanwaltschaft Klagenfurt zentral die Bearbeitung im Zusammenhang mit dem bundesweit aufgetretenen Phänomen der Schadsoftware „Polizeitrojaner", nachdem die diesbezüglichen Fälle zuvor von den unterschiedlichen örtlich zuständigen Staatsanwaltschaften bearbeitet worden waren. Die Landeskriminalämter übermittelten der Staatsanwaltschaft Klagenfurt zwischen 2013 und 2018 monatliche Berichte über die einschlägigen Anzeigen.

Der RH hielt weiters fest, dass die allgemeinen Regeln für die örtliche Zuständigkeit bei unbekannter, aber mutmaßlich gleicher Täterschaft zu einer zersplitterten Bearbeitung von Cyberkriminalität–Massendelikten durch unterschiedliche Staatsanwaltschaften führen konnten. Im Hinblick auf zielgerichtete Ermittlungen erachtete er es als grundlegend, die Bearbeitung solcher Fälle möglichst zeitnah bei einer Staatsanwaltschaft zusammenzuführen und damit eine einheitliche Ansprechstelle für die Polizei zu schaffen.

Der RH empfahl dem Justizministerium, Vorkehrungen zu treffen, die eine möglichst zeitnahe bundesweite Zusammenführung der Bearbeitung von Cyberkriminalität–Massendelikten mit unbekannter, aber mutmaßlich gleicher Täterschaft bei einer Staatsanwaltschaft sicherstellen.

43.3 Das Justizministerium teilte in seiner Stellungnahme mit, dass das Regierungsprogramm 2020–2024 die Bündelung staatsanwaltschaftlicher Ermittlungskompetenzen zur Bekämpfung digitaler Verbrechen (Cyberkriminalität) enthalte. Dazu bestünden zwei grundsätzliche Möglichkeiten: die Schaffung einer „Spezial"–Staatsanwaltschaft mit dem ausschließlichen Fokus auf digitale Verbrechen oder die Schaffung von Sonderreferaten für digitale Verbrechen bei den einzelnen Staatsanwaltschaften.

Im Hinblick auf die Attraktivität des staatsanwaltschaftlichen Berufsbilds sei der zweiten Möglichkeit der Vorzug zu geben, weil – je nach Auslastungsfaktor – auch bei bestehender Sonderzuständigkeit eine Durchmischung des Geschäftsanfalls mit allgemeinen Delikten erfolgen könne. Das Problem von sogenannten Wanderakten[48] infolge unklarer Zuständigkeit, wie es bei einer Spezialbehörde üblicherweise auftrete, könne bei diesem Lösungsansatz ebenfalls vermieden werden.

Die Durchführungsverordnung zum Staatsanwaltschaftsgesetz biete bereits die Möglichkeit der Schaffung von Sonderreferaten auch für Cyberkriminalität. Die praktische Umsetzung dieser Möglichkeit wie auch einer expliziten Anführung des Cyberkriminalitätsbereichs scheitere jedoch derzeit am unklaren Umfang der von diesem Begriff erfassten Delikte.

Vor Setzung dahingehender Schritte sei aber auch die im Regierungsprogramm 2020–2024 vorgesehene „Erarbeitung zeitgemäßer und Erweiterung bzw. Präzisierung vorhandener Straftatbestände zur Bekämpfung aller Arten von Cybercrime" abzuwarten.

Bezüglich der Zusammenführung von Cyberkriminalität–Massendelikten seien legistische Anpassungen u.a. aufgrund der damit verbundenen Unschärfen, der möglichen Fülle erforderlicher Zuständigkeitsentscheidungen und der Auslastungssituation

[48] Anmerkung RH: Als Wanderakten werden Akten bezeichnet, die bei Zuständigkeitsstreitigkeiten zwischen Staatsanwaltschaften abgetreten werden, was zu entsprechenden Zeit– und Effizienzverlusten führt.

nicht zweckmäßig. Dem aufgezeigten Problemfeld sei mit Blick auf die bestehenden gesetzlichen Zuständigkeitsregelungen vielmehr durch Sensibilisierung der staatsanwaltschaftlichen Leitungsebenen zu begegnen, was für eine kommende Besprechung mit den Leitenden Oberstaatsanwältinnen und Oberstaatsanwälten vorgemerkt werde.

43.4 Der RH entgegnete dem Justizministerium, dass seine Empfehlung zur Bearbeitung von Cyberkriminalität–Massendelikten mit unbekannter, aber mutmaßlich gleicher Täterschaft nicht auf legistische Änderungen abzielte. Aus seiner Sicht sollten neben einer Sensibilisierung der Leitungsebene auch allgemeine organisatorische Vorkehrungen getroffen werden, um der Polizei im Anlassfall eine einheitliche Ansprechstelle in der Justiz gegenüberzustellen.

Zur Abgrenzung und Festlegung des Umfangs der vom Begriff Cyberkriminalität erfassten Delikte verwies der RH auf seine Ausführungen in TZ 4. Wesentlich war nach Ansicht des RH, dass herausgehobene Ermittlungsverfahren im Bereich der Cyberkriminalität qualifiziert bearbeitet werden, sei es im Rahmen einer „Spezial"–Staatsanwaltschaft, durch Sonderreferate bei ausgewählten Staatsanwaltschaften oder mittels Unterstützung durch spezifische zentrale Ansprechstellen.

Aus– und Fortbildung Justizministerium

44.1 (1) Die Ausbildung der Richteramtsanwärterinnen und –anwärter – die auch die Grundlage für eine spätere Tätigkeit als Staatsanwältin bzw. Staatsanwalt darstellte – und die Ausbildung der Bezirksanwältinnen und Bezirksanwälte beinhalteten u.a. auch die im Bereich Cyberkriminalität relevanten strafrechtlichen Bestimmungen. Für die umfassende Bearbeitung von Cyberkriminalitätsdelikten notwendiges technisches und IT–Wissen oder Informationen z.B. zu möglichen Ermittlungsansätzen waren nicht Inhalt der Ausbildung.

Staatsanwältinnen und Staatsanwälten, Richterinnen und Richtern und auch den Richteramtsanwärterinnen und –anwärtern stand die Teilnahme an Fortbildungsveranstaltungen unterschiedlicher Anbieter (z.B. Justizministerium, Oberlandesgerichte, Oberstaatsanwaltschaften, Standesvertretungen, private Bildungseinrichtungen, Innenministerium) offen, welche vereinzelt auch das Thema Cyberkriminalität behandelten. Grundlage für die Festlegung des Fortbildungsprogramms waren Bedarfserhebungen, Schwerpunkte in Regierungsprogrammen oder Empfehlungen aus internationalen Staatenprüfungen. Dem Justizministerium kam dabei eine koordinierende Funktion zu. Die genannten Justizbediensteten waren zwar generell verpflich-

tet, sich fortzubilden[49], es gab aber keine Vorgaben hinsichtlich der Inhalte bzw. der konkret zu besuchenden Veranstaltungen. Ein spezifisches Aus– und Fortbildungskonzept bezogen auf Cyberkriminalität gab es nicht.

Die Staatsanwaltschaft Wien war daher bei Cyberkriminalität–Ermittlungsverfahren in der Praxis regelmäßig auf die fachliche Unterstützung der ermittelnden Polizeibediensteten angewiesen. Dies betraf z.B. Anordnungen an die Kriminalpolizei oder die Bearbeitung technisch formulierter Berichte der Kriminalpolizei.

(2) Der Rat der EU hielt in seinem Evaluierungsbericht aus 2017 fest, dass Schulungen und Spezialisierungen die Fähigkeiten der Staatsanwältinnen und Staatsanwälte in Bezug auf Cyberkriminalität im engeren Sinn verbessern könnten. Er erachtete für die Bearbeitung von Cyberkriminalitätsdelikten aktuelles Wissen und Verständnis zu den Modi Operandi und verwendeten Hilfsmitteln sowie zu den Ermittlungsmethoden und –möglichkeiten als erforderlich.

Er merkte weiters an, dass das Schulungsangebot nicht ausreichte und die Teilnahme der Justizbediensteten an Veranstaltungen auf freiwilliger Basis erfolgte. Daher sah es der Rat der EU als nicht gewährleistet, dass der mit Fällen von Cyberkriminalität befasste Personenkreis über entsprechende allgemeine Kenntnisse verfügte. Er empfahl in diesem Zusammenhang, das Schulungsangebot auszuweiten und gemeinsame Schulungen der Bediensteten der Strafverfolgungsbehörden – auch für den Erfahrungsaustausch – zu erwägen.

44.2 Der RH kritisierte, dass im Justizministerium kein Konzept vorhanden war, um alle mit dem Thema Cyberkriminalität befassten Bediensteten auf einen bedarfsgerechten Aus– bzw. Fortbildungsstand zu bringen und um diesen das notwendige technische Grundwissen zu vermitteln. Er hielt kritisch fest, dass das Thema Cyberkriminalität sowohl in der Ausbildung als auch in der Fortbildung nur rudimentär behandelt wurde. Zudem waren technisches und IT–Wissen oder Informationen z.B. zu möglichen Ermittlungsansätzen im Bereich Cyberkriminalität nicht Inhalt der Ausbildung. Dieses Wissen musste auch nicht verpflichtend durch Fortbildungen erworben werden. Damit war nicht gewährleistet, dass alle Bediensteten über den erforderlichen Wissensstand verfügten; dies obwohl insbesondere bei Staatsanwaltschaften das technische bzw. IT–Verständnis eine entscheidende Rolle spielte, um in Ermittlungsverfahren alle Möglichkeiten ausschöpfen und sowohl effizient als auch wirksam mit der Kriminalpolizei zusammenarbeiten zu können.

Der RH empfahl daher dem Justizministerium, ein Aus– und Fortbildungskonzept zu erarbeiten und umzusetzen, das Schulungsangebot auszuweiten und den selbstständigen Wissenserwerb und –transfer zu unterstützen, damit alle mit Cyberkrimi-

[49] § 57 Abs. 1 Richter– und Staatsanwaltschaftsdienstgesetz

nalität befassten Bediensteten der Staatsanwaltschaften über das für eine effiziente Fallbearbeitung notwendige technische Grundwissen verfügen. Diesbezüglich wäre verstärkt mit dem Innenministerium zusammenzuarbeiten.

44.3 Das Justizministerium teilte in seiner Stellungnahme mit, dass es beabsichtige, auf Basis des konkreten Bedarfs an den mit Cyberkriminalitätsfällen befassten Dienststellen ein effizientes und zeitgemäßes Bildungskonzept zum Thema Cyberkriminalität umzusetzen. Neben den bereits bestehenden Fortbildungsmöglichkeiten, die fortgeführt werden sollten, solle das Angebot auch um E–Learning–Programme ergänzt werden, die einen selbstständigen und individuellen Wissenserwerb ermöglichen. Konkret sei bereits ein E–Learning–Modul u.a. zum Thema „Hass im Netz“ in Ausarbeitung, das auch informationstechnologische Aspekte behandeln werde. Darüber hinaus sollten sowohl das analoge als auch das virtuelle Bildungsangebot laufend und bedarfsgerecht erweitert werden.

Digitale Forensik und Datenanalyse – Innenministerium und Justizministerium

Allgemeines

45 Die Sicherung, Aufbereitung und Auswertung von Daten waren im Bereich Cyberkriminalität – mittlerweile aber auch in vielen anderen Kriminalitätsbereichen – grundlegende und wichtige Instrumente zur Ermittlung strafrechtlich relevanter Sachverhalte und zur gerichtlichen Verwertung elektronischer Beweismittel. Damit kam einer geeigneten technischen Unterstützung im Bereich der digitalen Forensik wie auch der Analyse der daraus gewonnenen Daten steigende Bedeutung zu.

Analysesoftware

46.1 (1) Im Zuge von Ermittlungsverfahren sichergestellte bzw. beschlagnahmte Datenträger lieferten teilweise große Datenmengen, die zur Aufklärung von Straftaten – oftmals auch gemeinsam mit zusätzlichen (eingescannten) Papierdokumenten – gezielt durchsucht und aufbereitet werden mussten. Für solche Zwecke verwendete das Cybercrime Competence Center eine Suchmaschine für Massendaten, die nach Maßgabe der vorhandenen Lizenzen von den ermittelnden Bediensteten (auch aus den Landeskriminalämtern) nach Anforderung und Zulassung genutzt werden konnte.

(2) Insbesondere bei großen Wirtschaftsverfahren mit komplexen Daten mussten Kriminalpolizei und Staatsanwaltschaften Daten auch zielgerichtet analysieren. Im Jahr 2016 richteten daher Innen– und Justizministerium gemeinsam mit dem

Bundesministerium für Finanzen[50] eine Arbeitsgruppe IKT–Großstrafverfahren ein. Diese sollte Lösungskonzepte hinsichtlich der Anforderungen an die einzusetzende Analysesoftware und die Bereitstellung von Speicherkapazitäten sowie für die Schnittstellen zwischen den Beteiligten und für den Datenzugriff erarbeiten. Weiters sollte eine ressortübergreifende Organisation definiert und damit die Basis für den Abschluss eines Verwaltungsübereinkommens geschaffen werden.

Die Arbeitsgruppe legte im Dezember 2016 ihren abschließenden Bericht vor, in dem sie die wesentlichen Eckpunkte für ein Verwaltungsübereinkommen über die Kooperation betreffend IKT–Einsatz in Großstrafverfahren skizzierte.

Im April 2018 trafen das Innen– und das Justizministerium ein Verwaltungsübereinkommen zur Kooperation beim Einsatz eines spezifischen Software–Tools zur Auswertung und Analyse großer Datenmengen in Strafverfahren. Die Nutzung der zugrunde liegenden Basis–Software erfolgte unentgeltlich auf der Basis einer unbefristeten Vereinbarung zwischen dem Justizministerium und einem Software–Unternehmen als Lizenzgeber. Weitere Dienstleistungen des Software–Unternehmens zur Unterstützung bei der Bearbeitung konkreter Fälle und dafür notwendige Weiterentwicklungen wurden über einen zwischen dem Justizministerium und der Bundesrechenzentrum GmbH geschlossenen Vertrag[51] bezogen. Das Verwaltungsübereinkommen war als Pilotprojekt für eine Laufzeit bis Ende 2019 sowie einen Rahmen von 300 Beratertagen ausgelegt. Für dieses verpflichtend abzurufende Kontingent von 300 Personentagen war ein Entgelt von rd. 292.000 EUR vereinbart. Die Kosten trugen in der Regel (ausgenommen spezifische Leistungen an eines der Ressorts z.B. für Schulungen) Innen– und Justizministerium zu gleichen Teilen.

Im Mai 2020 legte die gemeinsame Steuerungsgruppe von Innen– und Justizministerium[52] ihren Abschlussbericht zum Einsatz des Analysetools in insgesamt acht in das Pilotprojekt einbezogenen Fällen vor. Dabei handelte es sich im Wesentlichen um von der WKStA mit dem Bundeskriminalamt oder dem Landeskriminalamt Wien bearbeitete Fälle. Die Steuerungsgruppe kam zum Schluss, dass das Verwaltungsübereinkommen fortgesetzt sowie Software und Infrastruktur funktional weiterentwickelt werden sollten. Als wesentliche Probleme identifizierte sie etwa die fehlende bzw. erst im Aufbau befindliche technische Infrastruktur, insbesondere bei der Krimi-

50 Das Bundesministerium für Finanzen wirkte mit, weil ursprünglich auch (größere) gerichtliche Finanzstrafverfahren eingebunden werden sollten.

51 Die Bundesrechenzentrum GmbH – als Dienstleister des Justizministeriums in IT–Angelegenheiten – hatte wiederum das Softwareunternehmen beauftragt und verrechnete dessen Leistung an das Justizministerium weiter.

52 Die Steuerungsgruppe trat während der Projektphase bedarfsorientiert (je nach Anforderung als strategische oder operative Steuerungsgruppe) in unterschiedlicher Besetzung zusammen. Die Koordination und Festlegung der Teilnehmenden erfolgte durch die Abteilung III 3 (Rechtsinformatik, Informations– und Kommunikationstechnologie) im Justizministerium und die für die IKT im Innenministerium zuständige Sektion IV (Service).

nalpolizei, aber auch bei der Justiz, sowie die teilweise mangelhafte Koordination zwischen Polizei und Staatsanwaltschaft.

(3) Ein hoher Datenanfall bei Großverfahren war nur mit entsprechender technischer Unterstützung zweckmäßig und effizient abzuarbeiten (siehe dazu den RH–Bericht „Bundeskriminalamt“ (Reihe Bund 2015/14, TZ 18) und die nachfolgende Follow–up–Überprüfung (Reihe Bund 2018/6, TZ 10)).

Das Regierungsprogramm 2020–2024 sah Maßnahmen im Hinblick auf die effektive Analyse großer Datenmengen mittels eines gemeinsamen Systems für Polizei und Staatsanwaltschaft vor.

46.2 Der RH erachtete eine zielgerichtete, zwischen Kriminalpolizei und Staatsanwaltschaft koordinierte Durchsuchung und Analyse sichergestellter Daten für unverzichtbar. Gerade bei großen Datenmengen mit Komplexität war es wesentlich, die zur Führung des Strafverfahrens notwendigen Inhalte zeitnah zu filtern und zu strukturieren, um effektive und effiziente Ermittlungen sicherzustellen.

Der RH beurteilte das bis Ende 2019 befristete Pilotprojekt von Innen– und Justizministerium zur gemeinsamen Datenanalyse in Großstrafverfahren daher grundsätzlich positiv. Im Hinblick auf eine dauerhafte effektive Zusammenarbeit wären allerdings die Aufgabenverteilung zwischen Kriminalpolizei und Staatsanwaltschaft (bzw. deren IT–Expertinnen und –Experten) und die Kostentragung klar zu regeln. Weiters wäre eine grundlegende Entscheidung bezüglich der einzusetzenden Analysesysteme zu treffen.

Der RH empfahl dem Innenministerium und dem Justizministerium, die Kooperation bei der Datenanalyse in Großstrafverfahren auf Basis der im Pilotprojekt gemachten Erfahrungen institutionalisiert fortzuführen und dabei klare rechtliche, organisatorische und finanzielle Rahmenbedingungen festzulegen.

Er empfahl weiters, nach entsprechender Markterkundung geeignete, anforderungsspezifisch weiterentwickelbare Softwareprodukte für die Analyse großer Datenmengen in Strafverfahren zu beschaffen.

46.3 (1) Laut Stellungnahme des Innenministeriums habe es zur Datenanalyse in Großstrafverfahren auf Basis der bisherigen Erfahrungen ein detailliertes Umsetzungskonzept in Form einer Handlungsanleitung erstellt, das entsprechend klare Vorgaben für eine zügige und flüssige Projektabwicklung beinhalte und als Grundlage für die nächsten Schritte dienen solle. Ein ressortübergreifendes, kollaboratives Arbeiten durch eine gemeinsame Softwarelösung zwischen der Kriminalpolizei, der Staatsanwaltschaft und dem Bundesministerium für Finanzen stelle dabei aus Sicht des Innenministeriums einen wesentlichen Erfolgsfaktor dar.

Zusätzlich zu den bereits laufenden Anwendungen werde eine ständige Markterkundung bzw. Testung geeigneter Softwareprodukte durchgeführt. Weiters plane das Innenministerium die Konzeption eines breiten Portfolios an Softwareprodukten in Form einer „Toolbox", das mit den Anforderungen im Kriminalitätsbereich weiterentwickelt werde und neben Basisprodukten neue innovative Produkte beinhalten solle.

(2) Das Justizministerium führte in seiner Stellungnahme aus, dass in gemeinsamen Arbeitsgruppen organisatorische und technische Rahmenbedingungen für Kooperationen und Schnittstellen erarbeitet würden.

Neben den laufenden Marktbeobachtungen werde bis zur Identifikation von Alternativen der Einsatz des bereits vorhandenen Softwareprodukts forciert.

46.4 (1) Der RH wiederholte gegenüber dem Innenministerium, dass für die ressortübergreifende Zusammenarbeit unter Verwendung einer gemeinsamen Softwarelösung auch klare rechtliche, organisatorische und finanzielle Rahmenbedingungen festgelegt werden sollten.

(2) Dem Justizministerium entgegnete der RH, dass ein institutionalisierter Rahmen für die Datenanalyse in Großverfahren durch Polizei und Justiz geschaffen werden sollte; gemeinsame Arbeitsgruppen können nur die Grundlagen dafür erarbeiten. Er bekräftigte auch gegenüber dem Justizministerium, dass für die Zusammenarbeit in diesem Bereich auch klare rechtliche, organisatorische und finanzielle Rahmenbedingungen festzulegen sind.

Elektronische Beweismittel, Datenaustausch und –archivierung

47.1 Grundsätzlich wertete die Kriminalpolizei sichergestellte Daten selbstständig bzw. nach (ergänzenden) staatsanwaltschaftlichen Aufträgen aus. Die Staatsanwaltschaften und Gerichte beauftragten gegebenenfalls auch externe Sachverständige, um konkrete Fragestellungen zu beantworten. Für solche Zwecke übermittelte die Polizei diesen entsprechende Datenabzüge. Gemäß § 114 StPO hatte die Kriminalpolizei bis zur Berichterstattung an die Staatsanwaltschaft für die Verwahrung sichergestellter Gegenstände zu sorgen, sofern der Grund für die Sicherstellung nicht wegfiel und sie dem Verfügungsberechtigten zurückgegeben werden mussten. Danach war die Staatsanwaltschaft zuständig für die Verwahrung. Abweichende Regelungen für immaterielle „Gegenstände" – etwa gespeicherte Daten – bestanden nicht.

Ein automationsunterstützter Austausch sichergestellter Daten zwischen Kriminalpolizei und Justiz erfolgte in der Praxis nicht. Die Polizeidienststellen übermittelten der Staatsanwaltschaft – insbesondere wegen der dort fehlenden Kapazitäten zur

Archivierung und mangels gesicherter Übertragungswege – lediglich die wesentlichen aufbereiteten Ergebnisse und Beweismittel in Papierform oder mittels Datenträger. Die Staatsanwaltschaft schloss diese dem jeweiligen Ermittlungsakt physisch an. Die Verwahrung und Archivierung der sichergestellten Daten bzw. elektronischen Beweismittel in ihrer Gesamtheit verblieben bei der Polizei.

Die Arbeitsgruppe IKT–Großstrafverfahren hatte in ihrem Abschlussbericht vom Dezember 2016 ein Architekturbild für eine interministerielle Datenaustauschplattform zwischen Kriminalpolizei und Justiz mit Netzwerkverbindungen und Schnittstellen, einem gegenseitigen Nutzungskonzept sowie einer umfassenden Archivierungslösung erarbeitet. Weitere Umsetzungsschritte unterblieben.

47.2 Der RH hielt fest, dass die im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel abweichend von der grundsätzlichen Regelung der StPO auch nach der Berichterstattung der Kriminalpolizei an die Staatsanwaltschaft bei der Kriminalpolizei aufbewahrt wurden und die Kriminalpolizei den Staatsanwaltschaften lediglich die wesentlichen Auswertungsergebnisse in Papierform oder mittels Datenträger übermittelte. Ursächlich für diese Vorgehensweise waren insbesondere auch die bei der Justiz fehlenden Kapazitäten für eine ordnungsgemäße Archivierung.

Der RH empfahl dem Justizministerium, ausreichende Kapazitäten für die Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel aufzubauen.

Der RH kritisierte, dass das Innen– und das Justizministerium die bereits 2016 im Rahmen der gemeinsamen Arbeitsgruppe IKT–Großstrafverfahren erarbeiteten Vorschläge für eine interministerielle Datenaustauschplattform samt umfassender Archivierungslösung für elektronische Beweismittel nicht weiterverfolgten. Damit gab es weiterhin keinen automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten sowie keine zuverlässige und vollständige Dokumentation sämtlicher Bearbeitungsschritte.

Er hielt in diesem Zusammenhang fest, dass die lückenlose Dokumentation der Bearbeitung elektronischer Beweismittel unerlässlich ist, um volle Beweiskraft zu sichern.

Der RH empfahl dem Innenministerium und dem 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.

47.3 (1) Laut Stellungnahme des Innenministeriums unterliege die Umsetzung der Empfehlung zum automationsunterstützten Datenaustausch auch „externen Einflüssen“ (z.B. legistischer Änderungsbedarf oder technische Adaptierungen außerhalb der Sphäre des Innenministeriums). Es werde aber Gespräche mit den relevanten Stakeholdern führen und an der Umsetzung der Empfehlung arbeiten.

(2) Laut Stellungnahme des Justizministeriums werde im Rahmen des Projekts zum Ausbau des Einsatzes von IT–Expertinnen und –Experten im Strafverfahren auch die Voraussetzung für einen automationsunterstützten Datenaustausch geschaffen. Für Großverfahren mit enormen Datenmengen (> 10 Terabyte) würden jedoch weiterhin rein physikalische Grenzen bleiben, welche die faktische Übertragungsmöglichkeit über elektronische Schnittstellen maßgeblich beeinflussen würden.

Der Aufbau von entsprechenden IT–Infrastruktur–Kapazitäten sei bereits geplant. Diese würden die Voraussetzungen für die „Inhouse–Speicherung“ von Beweismitteln (statt der Speicherung bei Sachverständigen) schaffen.

47.4 Der RH entgegnete dem Justizministerium, dass seine Empfehlungen auf die Einrichtung eines systematischen automationsunterstützten Datenaustauschs zwischen Kriminalpolizei und Staatsanwaltschaften, verbunden mit der Schaffung ausreichender Kapazitäten für die Archivierung bei der Justiz, gerichtet waren. In einem solchen gesamtheitlichen System wäre jedenfalls auch sicherzustellen, dass externe Sachverständige eingebunden werden können und sämtliche Bearbeitungen von Daten vollständig dokumentiert werden. Die Einrichtung eines automatisierten Datenaustauschs in Strafverfahren mit Einsatz der IT–Expertinnen und –Experten und die Schaffung der Voraussetzungen für eine „Inhouse–Speicherung“ von Beweismitteln (statt der Speicherung bei Sachverständigen) beurteilte der RH als wichtige Schritte, eine Beschränkung darauf greift aus seiner Sicht aber zu kurz.

Bezüglich der sogenannten Großverfahren mit besonders großen Datenmengen verwies der RH auf seine Ausführungen in TZ 46 zu Kooperationen in solchen Verfahren mit Einsatz spezifischer Analysesoftware.

Resümee

48 Cyberkriminalität nimmt seit vielen Jahren kontinuierlich und rasch zu. Insbesondere seit der im Frühjahr 2020 aufgetretenen COVID–19–Pandemie war die klassische Kriminalität in Österreich rückläufig, während Cyberkriminalität (z.B. durch Hackerangriffe, Ausnutzung von technischen Sicherheitslücken) verstärkt anstieg. Die durch Cyberkriminalität verursachten Gefahren und Schäden betreffen Bürgerinnen und Bürger gleichermaßen wie Wirtschaft und staatliche Institutionen.

Das Innenministerium traf in den letzten Jahren zwar Maßnahmen auf den wesentlichen Organisationsebenen und schuf damit die Grundlage für Prävention und Bekämpfung von Cyberkriminalität. Es bestand aber Verbesserungspotenzial vor allem bei der Prävention, beim Personal und der Organisation. Das Justizministerium befand sich bei der Bekämpfung von Cyberkriminalität noch im Anfangsstadium. Insbesondere bei der Organisation und Aus– bzw. Fortbildung bei Staatsanwaltschaften bestand Aufholbedarf.

Eine Grundvoraussetzung für die effiziente und effektive Prävention und Bekämpfung von Cyberkriminalität war aus Sicht des RH die abgestimmte Zusammenarbeit der beiden Ressorts – insbesondere in strategischen, statistischen und technischen Bereichen. Der RH stellte zusammenfassend Handlungsbedarf auf mehreren Ebenen fest:

- Es wäre grundsätzlich erforderlich, zwischen dem Innenministerium und dem Justizministerium abgestimmte Strategien zur Bekämpfung von Cyberkriminalität zu entwickeln (TZ 9, TZ 10).
- Um vergleichbare Zahlen erheben und darstellen zu können, wären zwischen dem Innen– und Justizministerium vereinheitlichte Begriffsbestimmungen und eine abgestimmte statistische Erfassung von Cyberkriminalität notwendig (TZ 4, TZ 5).
- Es wäre wesentlich, die Prävention zu verstärken, da sich die Bekämpfung und Aufklärung von Cyberkriminalität oftmals schwierig gestalteten sowie die Zahl der Delikte in den letzten Jahren und damit auch die einhergehenden Schäden stiegen (TZ 12).
- Damit die Polizei Cyberkriminalität wirksamer bekämpfen kann, wären die bestehenden Strukturen und Prozesse umfassend zu evaluieren und angemessene organisatorische, personelle und infrastrukturelle Rahmenbedingungen zu schaffen (TZ 27, TZ 37).

- Es wäre notwendig, bei den Staatsanwaltschaften eine Spezialisierung im Bereich Cyberkriminalität zu erreichen und diesbezüglich das für eine effiziente Fallbearbeitung notwendige technische Grundwissen aufzubauen (TZ 44, TZ 45).
- Aus operativer Sicht wäre es wichtig, im Hinblick auf die Sicherung, Aufbereitung und Auswertung von Daten sowie die Erstellung elektronischer Beweismittel eine geeignete technische Infrastruktur aufzubauen. Diese sollte einen automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten und Dokumentation sämtlicher Bearbeitungsschritte, anforderungsspezifisch weiterentwickelbare Analysesoftware sowie eine eigenständige kriminalpolizeiliche IT–Infrastruktur umfassen (TZ 38, TZ 46, TZ 47).

Schlussempfehlungen

49 Zusammenfassend empfahl der RH:

Bundesministerium für Inneres; Bundesministerium für Justiz

(1) 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)

(2) Die polizeilichen und justiziellen Kriminalstatistiken wären aufeinander abgestimmt weiterzuentwickeln und methodische Angleichungen vorzunehmen. (TZ 5)

(3) Die Voraussetzungen für eine systematische Nachverfolgung der Erledigung polizeilicher Anzeigen gegen tatverdächtige Personen z.B. auf Basis bereichsspezifischer Personenkennzeichen wären zu schaffen. (TZ 5)

(4) Die Kooperation bei der Datenanalyse in Großstrafverfahren wäre auf Basis der im Pilotprojekt 2018 bis 2019 gemachten Erfahrungen institutionalisiert fortzuführen; dabei wären klare rechtliche, organisatorische und finanzielle Rahmenbedingungen festzulegen. (TZ 46)

(5) Nach entsprechender Markterkundung wären geeignete, anforderungsspezifisch weiterentwickelbare Softwareprodukte für die Analyse großer Datenmengen in Strafverfahren zu beschaffen. (TZ 46)

(6) 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. (TZ 47)

Bundesministerium für Inneres

(7) Eine mit dem Justizministerium abgestimmte Strategie für den Bereich Cyberkriminalität wäre – auch im Hinblick auf das Regierungsprogramm 2020–2024 – zu entwickeln und konsequent zu verfolgen. (TZ 9)

(8) Es wären, auch im Hinblick auf das entsprechende Wirkungsziel, Anreize für Präventionstätigkeiten zu schaffen, um weitere Präventionsbedienstete für Cyberkriminalität zu gewinnen. (TZ 14)

(9) In den Assistenzbereichen Kriminalprävention der Landeskriminalämter wäre der Bereich Cyberkriminalität – z.B. durch die Einrichtung von eigenen, auf die Prävention von Cyberkriminalität spezialisierten Gruppen – stärker zu verankern. (TZ 15)

(10) Es wäre dafür zu sorgen, dass in der Landespolizeidirektion Vorarlberg ausreichend Präventionsbedienstete mit Expertise für Cyberkriminalität zur Verfügung stehen. (TZ 15)

(11) Kooperationen zur Dunkelfeldforschung mit Wissenschaft und Forschung wären einzurichten, um ein umfassenderes Bild von Umfang und Struktur von Cyberkriminalität sowie dem tatsächlichen Kriminalitätsaufkommen zu erhalten. (TZ 18)

(12) Die organisatorische Stellung der Bezirks–IT–Ermittlerinnen und –Ermittler wäre zu evaluieren und darauf aufbauend der künftig notwendige Bedarf festzulegen. (TZ 21)

(13) In Wien wären zur Qualitätssicherung eine geeignete Fachaufsicht über die Bezirks–IT–Ermittlerinnen und –Ermittler sowie entsprechende Ressourcen dafür sicherzustellen. (TZ 22)

(14) Die Vorgaben an die Organisationsstruktur der Assistenzbereiche IT–Beweissicherung der Landeskriminalämter wären den praktischen Notwendigkeiten anzupassen, sodass bei der Umsetzung auch laufende Entwicklungen im Ermittlungs– oder Forensikbereich flexibel berücksichtigt werden können. (TZ 23)

(15) Es wäre 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 und die Planstellen dem Assistenzbereich IT–Beweissicherung zugeordnet werden. (TZ 25)

(16) 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 26)

(17) In Zusammenarbeit mit dem zuständigen 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. (TZ 30)

(18) Im Einvernehmen mit dem Bundesministerium für Justiz wäre eine zentrale Koordinierungsstelle für Auskunftsverlangen an Betreiber sozialer Medien und Internetprovider zeitnah einzurichten und mit ausreichenden Personalressourcen und Know–how auszustatten. (TZ 31)

(19) Das Ausbildungsprogramm der Bezirks–IT–Ermittlerinnen und –Ermittler wäre einheitlich umzusetzen und damit ein entsprechendes Qualitätsniveau sicherzustellen. (TZ 33)

(20) Ein ganzheitliches, über alle Ausbildungsebenen bedarfsabgestimmtes Ausbildungskonzept für den Bereich Cyberkriminalität wäre zu entwickeln und zeitnah umzusetzen; dabei wären getroffene Annahmen und finanzielle Auswirkungen angedachter Maßnahmen konkret darzulegen und zu berücksichtigen. (TZ 34)

(21) Es wäre darauf hinzuwirken, dass alle Fortbildungen im Bereich Cyberkriminalität lückenlos in der zentralen elektronischen Datenbank, dem Bildungspass, erfasst werden. (TZ 35)

(22) 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. (TZ 35)

(23) 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. (TZ 37)

(24) Der Aufbau einer eigenständigen kriminalpolizeilichen Infrastruktur wäre unter Bedachtnahme auf Kosten–Nutzen–Aspekte sicherzustellen, um eine zeitgemäße und anforderungsgerechte IT–Infrastruktur für kriminalpolizeiliche Ermittlungen, insbesondere zur Bekämpfung von Cyberkriminalität, zu gewährleisten. (TZ 38)

(25) Im Zusammenwirken mit den Bedarfsträgern wären einheitliche und sichere Softwarelösungen für den kriminalpolizeilichen Bereich im Rahmen der geplanten kriminalpolizeilichen IT–Infrastruktur zu etablieren sowie deren Servicierung sicherzustellen. (TZ 38)

(26) 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. (TZ 39)

Bundesministerium für Justiz

(27) Im Zuge der Weiterentwicklung der internen Informationstechnologie wäre sicherzustellen, dass zuverlässige und aussagekräftige Statistiken zu Anfall und Erledigung von Strafverfahren durch Staatsanwaltschaften und Gerichte generiert werden können; insbesondere sollten auch deliktspezifische Statistiken für den Bereich Cyberkriminalität ermöglicht werden. (TZ 5)

(28) Eine mit dem Innenministerium abgestimmte Strategie für den Bereich Cyberkriminalität wäre – auch im Hinblick auf das Regierungsprogramm 2020–2024 – zu entwickeln und konsequent zu verfolgen. (TZ 10)

(29) Basierend auf internationalen Beispielen und den Erfahrungen besonders betroffener Staatsanwaltschaften wären organisatorische Rahmenbedingungen für eine spezialisierte Bearbeitung von Ermittlungsverfahren im Bereich Cyberkriminalität festzulegen. (TZ 43)

(30) Es wären Vorkehrungen zu treffen, die eine möglichst zeitnahe bundesweite Zusammenführung der Bearbeitung von Cyberkriminalität–Massendelikten mit unbekannter, aber mutmaßlich gleicher Täterschaft bei einer Staatsanwaltschaft sicherstellen. (TZ 43)

(31) 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. (TZ 44)

(32) Ausreichende Kapazitäten für die Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel wären aufzubauen. (TZ 47)

Bundeskriminalamt

(33) Es wäre sicherzustellen, dass bedarfsorientierte Präventionsmaßnahmen im Bereich Cyberkriminalität auf Ebene der Bezirks– und Stadtpolizeikommanden verstärkt für die Zielgruppe der über 18–Jährigen gesetzt werden. (TZ 14)

(34) 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. (TZ 16)

(35) Es wäre regelmäßig – etwa in Form eines Präventionsberichts – ein Überblick über (neue) Phänomene und gesetzte Präventionstätigkeiten bzw. –projekte zu veröffentlichen. Dies sollte insbesondere für den Bereich Cyberkriminalität das Bewusstsein in der Bevölkerung erhöhen und eine Plattform für die Arbeit der Präventionsbediensteten bieten. (TZ 17)

(36) Das Projekt zur Wirkungs– und Erfolgsmessung der Präventionsmaßnahmen im Bereich Cyberkriminalität wäre weiterzuverfolgen, die Ergebnisse wären in der Folge zu verwerten und umzusetzen. (TZ 19)

(37) 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. (TZ 27)

(38) 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. (TZ 28)

(39) Ein Lagebild Cyberkriminalität wäre zeitnah einzurichten, das es ermöglicht, Zusammenhänge zwischen Straftaten im Bereich Cyberkriminalität möglichst rasch erkennen zu können; dabei wären die im Rahmen des von 2014 bis 2019 betriebenen Vorprojekts gemachten Erfahrungen zu berücksichtigen. (TZ 40)

(40) Eine gemeinsame Schnittstelle für alle Lagebilder und sonstigen Anwendungen, die Daten aus der Applikation Protokollieren, Anzeigen, Daten (PAD) übernehmen, wäre zeitnah umzusetzen. (TZ 40)

Rechnungshof Österreich

Wien, im Juni 2021
Die Präsidentin:

Dr. Margit Kraker

Anhang

Tabelle A: Wesentliche internationale Kooperationen des Bundeskriminalamts im Bereich Cyberkriminalität

Kooperationspartner bzw. –formate	Gegenstand und Ziele	Art der Kooperation
Europol und Eurojust	gemeinsames Ermittlungsteam (Joint Investigation Team – JIT) MOZART zur Bekämpfung von Internetbetrug	operativ
European Cybercrime Center (EC3, Europol)	operative Analysen, forensische Unterstützung, rasche Identifikation von Opfern, rasche Reaktion auf Cyberkriminalität	operativ
Joint Cybercrime Action Teams	Koordination von operativen Maßnahmen bei länderübergreifenden Fällen	operativ
Victim Identification Task Force (Europol)	Ergänzung und Hochladen neuer Datensätze in eine internationale Datenbank für sexuelle Ausbeutung von Kindern, um Opfer rascher identifizieren zu können	operativ
European Cybercrime Taskforce (EUCTF)	2010 in Europol etabliert; Ziele sind Identifikation und Priorisierung von Kernaufgaben mit Entwicklung und Harmonisierung der Ziele in der EU gegen kriminellen Missbrauch von Informations– und Kommunikationstechnik und der Bekämpfung von Cyberkriminalität	strategisch
European Multidisciplinary Platform Against Criminal Threats (EMPACT)	zur wirksameren Bekämpfung von internationaler und organisierter Kriminalität sowie Cyberkriminalität	operativ, strategisch
Europäisches Amt für Betrugsbekämpfung – European Anti–Fraud Office (OLAF)	stellt Ausbildungen für europäische Polizeibehörden zur Verfügung, die IT–forensische Assistenzdienste für nationale Betrugsbekämpfungsbehörden bieten	operativ
Toolsammlung FREETOOL	eine Toolsammlung für operative Ermittlungen und Analysen, welche unter Beteiligung der Mitgliedstaaten entwickelt und unter Mitwirkung durch Europol und European Cybercrime Training and Education Group (https://www.ecteg.eu/; abgerufen am 28. August 2020) (ECTEG) über eine Downloadplattform zur Verfügung gestellt wird	operativ
Projekte im Rahmen des EU–Programms für Forschung und Innovation Horizon 2020; z.B. Horizon 2020 Titanum	dienen der Sicherheitsforschung im Bereich Kryptowährungen	strategisch

Quelle: BMI

Tabelle B: Polizeiliche Anzeigen im Bereich Cyberkriminalität (Polizeiliche Kriminalstatistik)

Delikt	2016	2017	2018	2019
	Anzahl Anzeigen			
Cyberkriminalität im engeren Sinn:				
Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 107c StGB)	–[1]	359	308	330
Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)	457	363	403	684
Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)	–[1]	16	11	11
Missbräuchliches Abfangen von Daten (§ 119a StGB)	42	41	45	47
Datenbeschädigung (§ 126a StGB)	659	1.186	415	467
Störung der Funktionsfähigkeit eines Computers (§ 126b StGB)	282	105	102	93
Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)	234	189	201	243
Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)	817	1.056	1.415	5.537
Datenfälschung (§ 225a StGB)	139	231	170	210
Summe Cyberkriminalität im engeren Sinn	**2.630**	**3.546**	**3.070**	**7.622**
Cyberkriminalität im weiteren Sinn:				
Internetbetrug:				
Betrug (§ 146 StGB)	8.361	9.943	11.417	14.494
Schwerer Betrug (§ 147 StGB)	735	1186	1.248	1.560
Gewerbsmäßiger Betrug (§ 148 StGB)	576	632	663	777
Summe Internetbetrug	**9.672**	**11.761**	**13.328**	**16.831**
Sonstige Kriminalität im Internet:				
Erpressung (§ 144 StGB)		474	1.599	1.874
Schwere Erpressung (§ 145 StGB)		29	92	84
Pornografische Darstellungen Minderjähriger (§ 207a StGB)	681	733	1.161	1.666
Sexueller Missbrauch von Jugendlichen (§ 207b StGB)		1	1	4
Sittliche Gefährdung von Personen unter 16 Jahren (§ 208a StGB)	80	106	108	101
Sexuelle Belästigung und öffentliche geschlechtliche Handlung (§ 218 StGB)	3	6	10	12
Urkundenfälschung (§ 223 StGB)	22	28	24	42
Fälschung besonders geschützter Urkunden (§ 224 StGB)	7	34	7	21
Urkundenunterdrückung (§ 229 StGB)			1	
Gebrauch fremder Ausweise (§ 231 StGB)	1	6	15	16
Geldfälschung (§ 232 StGB)	5	9	35	62
Fälschung unbarer Zahlungsmittel (§ 241a StGB)	2			4
Verbotsgesetz (§§ 3d und 3g VerbotsG)		61	176	95
Summe Sonstige Kriminalität im Internet	**801**	**1.497**	**3.229**	**3.986**
Summe Cyberkriminalität im weiteren Sinn (Internetbetrug und Sonstige Kriminalität im Internet)	**10.473**	**13.258**	**16.557**	**20.817**
Summe Cyberkriminalität	**13.103**	**16.804**	**19.627**	**28.439**

StGB = Strafgesetzbuch Quelle: BMI

[1] noch nicht als Cyberkriminalität im engeren Sinn erfasst

Tabelle C: Vergleich polizeiliche Anzeigen und Aktenanfall bei den Staatsanwaltschaften (Cyberkriminalität im engeren Sinn)

Delikt	2016		2017		2018		2019	
	PKS	StA	PKS	StA	PKS	StA	PKS	StA
Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 107c StGB)	–[1]	445	359	585	308	476	330	470
Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)	457	582	363	512	403	546	684	818
Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)	–[1]	26	16	32	11	33	11	37
Missbräuchliches Abfangen von Daten (§ 119a StGB)	42	53	41	56	45	45	47	72
Datenbeschädigung (§ 126a StGB)	659	681	1.186	803	415	406	467	445
Störung der Funktionsfähigkeit eines Computers (§ 126b StGB)	282	310	105	184	102	138	93	143
Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)	234	274	189	225	201	246	243	326
Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)	817	1.487	1.056	1.536	1.415	2.117	5.537	3.825
Datenfälschung (§ 225a StGB)	139	177	231	248	170	195	210	237
Summe Cyberkriminalität im engeren Sinn	**2.630**	**4.035**	**3.546**	**4.181**	**3.070**	**4.202**	**7.622**	**6.373**

PKS: Anzeigen gemäß Polizeilicher Kriminalstatistik
StA: Aktenanfall bei den Staatsanwaltschaften
StGB = Strafgesetzbuch

Quellen: BMI; BMJ; Berechnung und Zusammenstellung: RH

[1] noch nicht als Cyberkriminalität im engeren Sinn erfasst

Tabelle D: Erledigung von Cyberkriminalität im engeren Sinn durch die Justiz: Anzahl je Delikt (2016 bis 2019)

Paragraf Strafgesetzbuch	107c	118a	119	119a	126a	126b	126c	148a	225a	Summe
	Anzahl									
Tatverdächtige gemäß Polizeilicher Kriminalstatistik[1]	1.002	450	36	32	296	36	212	2.689	673	**5.426**
Aktenanfall bei den Staatsanwaltschaften (bekannte Täterschaft)[1]	1.421	675	92	67	419	57	220	3.069	657	**6.677**
Erledigungen durch die Justiz (Staatsanwaltschaften und Gerichte zusammengefasst)[2]	1.207	575	88	57	347	41	188	2.724	634	**5.861**
davon										
Einstellung durch die Staatsanwaltschaft	*1.084*	*510*	*73*	*54*	*254*	*34*	*164*	*1.622*	*272*	*4.067*
Diversion (Staatsanwaltschaften und Gerichte insgesamt)	*60*	*31*	*8*	*1*	*42*	*2*	*17*	*192*	*213*	*566*
Verurteilung (Gerichte)	*46*	*15*	*2*	*1*	*28*	*4*	*3*	*782*	*99*	*980*
Freispruch (Gerichte)	*17*	*19*	*5*	*1*	*23*	*1*	*4*	*128*	*50*	*248*

[1] Für die §§ 107c und 119 StGB umfasst die Summe nur die Jahre 2017 bis 2019, da diese Delikte in der Polizeilichen Kriminalstatistik erst ab 2017 als Cyberkriminalität erfasst wurden.
[2] nur inhaltliche Erledigungen, d.h. ohne Abbrechung und sonstige Erledigungen

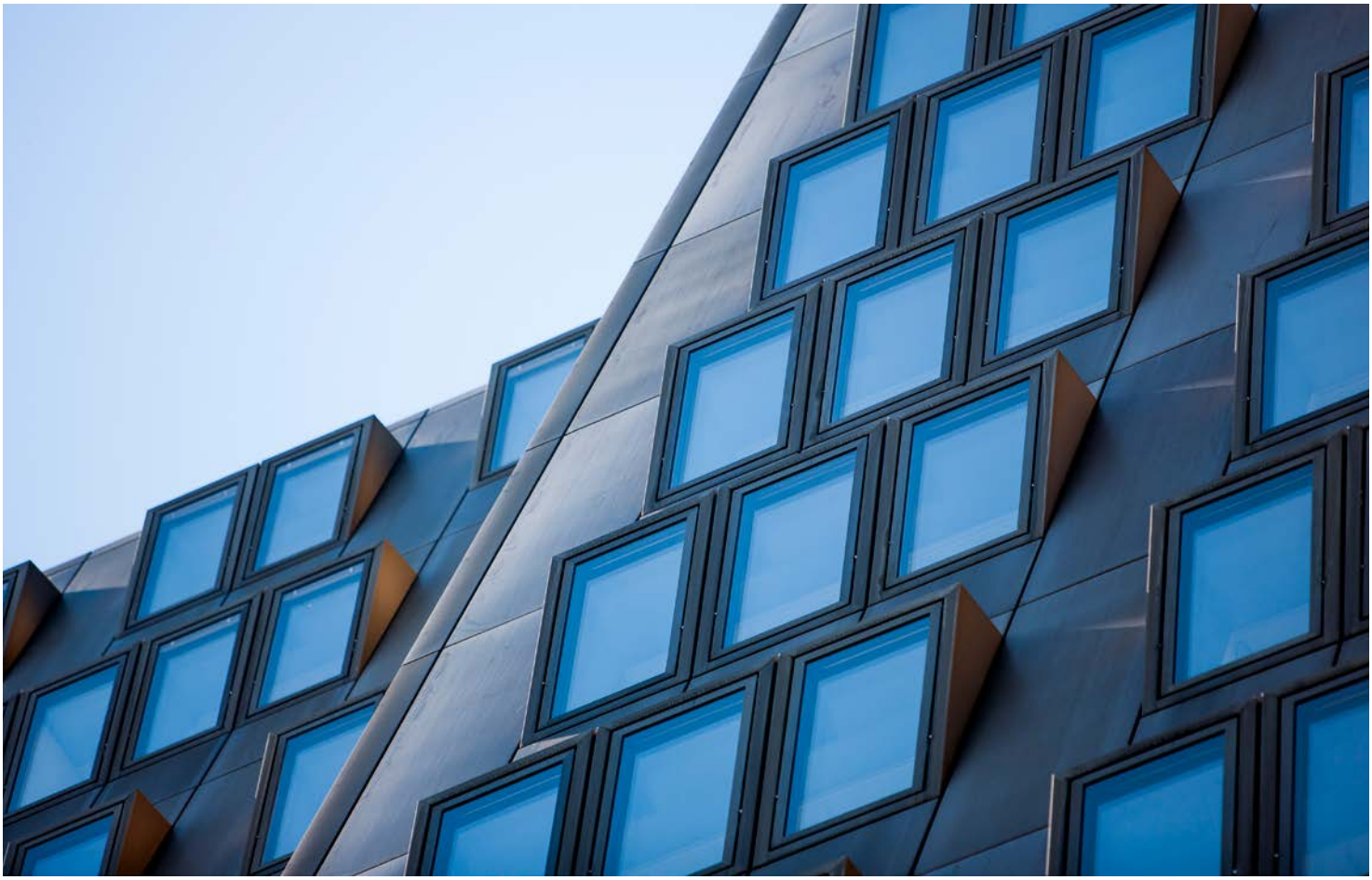
Quellen: BMI; BMJ; Berechnung und Zusammenstellung: RH

Tabelle E: Erledigungen von Cyberkriminalität im engeren Sinn durch die Justiz: Anteil der Erledigungsarten je Delikt (2016 bis 2019)

Paragraf Strafgesetzbuch	107c	118a	119	119a	126a	126b	126c	148a	225a	Summe
	in %									
Einstellung durch die Staatsanwaltschaft	90	89	83	95	73	83	87	60	43	69
Diversion (Staatsanwaltschaften und Gerichte insgesamt)	5	5	9	2	12	5	9	7	34	10
Verurteilung (Gerichte)	4	3	2	2	8	10	2	29	16	17
Freispruch (Gerichte)	1	3	6	2	7	2	2	5	8	4

Rundungsdifferenzen möglich

Quellen: BMI; BMJ; Berechnung und Zusammenstellung: RH

nur inhaltliche Erledigungen, d.h. ohne Abbrechung und sonstige Erledigungen

R
H