SCHLESWIG-HOLSTEINISCHER LANDTAG
19. Wahlperiode

22. Dezember 2021

Unterrichtung 19/382

der Landesregierung

Veröffentlichung der freigegebenen Beschlüsse der 215. Innenministerkonferenz vom 1. bis 3. Dezember 2021 in Stuttgart, Baden-Württemberg

Die Landesregierung unterrichtet den Schleswig-Holsteinischen Landtag gem. § 8 Abs. 1 Parlamentsinformationsgesetz (PIG).

Federführend ist das Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung

Zuständiger Ausschuss: Innen- und Rechtsausschuss

Schleswig-Holstein
Der echte Norden

Schleswig-Holstein
Ministerium für Inneres,
ländliche Räume, Integration
und Gleichstellung

Ministerium für Inneres, ländliche Räume,
Integration und Gleichstellung | Postfach 71 25 | 24171 Kiel

Ministerin

An den
Präsidenten des
Schleswig-Holsteinischen Landtages
Herrn Klaus Schlie
Landeshaus
24105 Kiel

21. Dezember 2021

Beschlüsse der 215. Innenministerkonferenz vom 1. – 3. Dezember 2021 in Stuttgart, Baden-Württemberg

Sehr geehrter Herr Präsident,

beigefügte veröffentlichte Beschlüsse der 215. Innenministerkonferenz übersende ich gem. § 8 Abs. 1 PIG zur Kenntnis.

Ich weise darauf hin, dass die freigegebenen Berichte / Anlagen nur in elektronischer Form übersandt werden.

Mit freundlichen Grüßen

Dr. Sabine Sütterlin-Waack

Dienstgebäude Düsternbrooker Weg 92, 24105 Kiel | Telefon 0431 988-0 | Telefax 0431 988-2833 |
Poststelle@im.landsh.de | www.schleswig-holstein.de/innenministerium | Buslinie 41, 42, 51 |
E-Mail-Adressen: Kein Zugang für verschlüsselte Dokumente.

Sammlung
der zur Veröffentlichung freigegebenen Beschlüsse

der 215. Sitzung

der Ständigen Konferenz der Innenminister und -senatoren der Länder

am 03. Dezember 2021

Hinweise:

Sofern im Folgenden Beschlüsse oder andere Dokumente von Arbeitskreisen und anderen Gremien der IMK bzw. von Bund und Ländern nicht ausdrücklich als zur Veröffentlichung freigegeben gekennzeichnet sind, wird darum gebeten, von Nachfragen abzusehen, da diese Unterlagen nicht an die Öffentlichkeit weitergegeben werden.

Für Beschlüsse anderer Fachministerkonferenzen gelten die dortigen Vorgaben zur Handhabung dieser Unterlagen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 2: Bekämpfung des islamistischen Terrorismus

Berichterstattung:	BMI
Hinweise:	IMK am 10.12.20 zu TOP 46
	AK II am 13./14.10.21 zu TOP 2
	AK IV am 26./27.10.21 zu TOP 3
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Berichte
Az.:	VI D 4.4/9a

Beschluss:

1. Die IMK nimmt den Bericht „Überprüfung der Wirksamkeit beschlossener Handlungs- und Maßnahmenkonzepte zur Bekämpfung des islamistischen Extremismus und Terrorismus im Bereich Polizei und Verfassungsschutz -VS-NfD-“ (Stand: 10.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie begrüßt die Überprüfung bestehender Handlungs- und Maßnahmenkonzepte im Zusammenwirken mit dem Verfassungsschutzverbund und nimmt zur Kenntnis, dass die relevanten ab dem Jahr 2017 durch die Gremien beschlossenen bzw. fortgeschriebenen Unterlagen geprüft und weitere vor diesem Zeitpunkt erstellten Konzepte in die Betrachtung einbezogen wurden, sofern diese ebenfalls für relevant erachtet wurden.

3. Die IMK stellt fest, dass die überprüften Mechanismen und laufenden Initiativen zur Bekämpfung des islamistischen Extremismus und Terrorismus in den Bereichen Polizei und Verfassungsschutz grundsätzlich wirksam sind.

4. Sie konstatiert, dass sich das GTAZ in seiner organisatorischen Aufstellung bewährt hat**,** einem kontinuierlichen Wandlungsprozess unterliegt und sich somit strukturell und inhaltlich fortlaufend den Entwicklungen im Phänomenbereich Islamismus / islamistischer Terrorismus anpasst.

5. Sie nimmt ferner den Bericht „Handlungsempfehlungen zum Umgang mit verurteilten Islamisten nach deren Haftentlassung -VS-NfD-“ (Stand: 05.10.21) *(nicht freigegeben)* zur Kenntnis.

6. Die IMK beauftragt den AK II, unter Beteiligung des AK IV die Prüfung einer gesonderten Erarbeitung sogenannter Leitlinien zum Umgang mit verurteilten Islamisten nach deren Haftentlassung im Zusammenwirken mit Vertretern der Justiz auf Basis bestehender Konzepte vorzunehmen. Hierbei sollten möglichst auch die „Handlungsempfehlungen zum Umgang mit verurteilten Islamisten nach deren Haftentlassung“ berücksichtigt werden.

7. Sie beauftragt den AK II und den AK IV, den im Bericht festgestellten Aktualisierungsbedarf umzusetzen und die Maßnahmen- und Handlungskonzepte entsprechend fortzuschreiben.

8. Die IMK bittet ihren Vorsitzenden, die JuMiKo über diesen Beschluss zu informieren.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 3: Ganzheitliche Fallbearbeitung im Umgang mit islamistisch radikalisierten Personen in der Praxis

Berichterstattung:	BMI
Hinweise:	IMK vom 04. bis 06.12.19 zu TOP 9
	IMK vom 17. bis 19.06.20 zu TOP 14
	AK II am 28.04.21 zu TOP 11
	IMK vom 16. bis 18.06.21 zu TOP 2
	AK II am 13./14.10.21 zu TOP 11
	AK IV am 26./27.10.21 zu TOP 2
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 4.4/17

Beschluss:

Die IMK nimmt den Bericht „Ganzheitliche Fallbearbeitung im Umgang mit islamistisch radikalisierten Personen in der Praxis -VS-NfD-“ (Stand: 01.11.21) *(nicht freigegeben)* mit den überarbeiteten Leitlinien der Arbeitsgruppe Deradikalisierung im Gemeinsamen Terrorismusabwehrzentrum zum ganzheitlichen Umgang mit Rückkehrerinnen und Rückkehrern aus jihadistischen Kampfgebieten zur Kenntnis. Die Leitlinien wurden dabei um weitere Themen der ganzheitlichen Fallbearbeitung im Umgang mit islamistisch radikalisierten Personen in der Praxis ergänzt, die im Rahmen der Arbeit der länderoffenen Bund-Länder-AG „Ganzheitliche Fallbearbeitung im Umgang mit islamistisch radikalisierten Personen in der Praxis“ identifiziert wurden.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 6: Strategie der BDBOS und der Bundeswehr für die Frequenzgewinnung und die Breitbandkommunikation

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 28 i. V. m. TOP 29
	Beschlussvorschlag BMI vom 15.10.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI C 6.3

Beschluss:

1. Die IMK nimmt den Beschluss des Verwaltungsrats der BDBOS zu TOP 3 der Sondersitzung am 12.10.21 einschließlich des Berichts „Weiterentwicklung des BOS-Digitalfunknetzes, Version 3.0 -VS-NfD-“ (Stand: 29.09.21) *(nicht freigegeben)* zur Kenntnis und bittet das BMI, die BDBOS mit der Umsetzung der darin enthaltenen Strategie des phasenweisen Aufbaus eines eigenbeherrschten Breitbandnetzes für die BOS und Bundeswehr zu beauftragen.

2. Sie bestätigt die Notwendigkeit einer ergänzenden Vereinbarung zum Verwaltungsabkommen zur Finanzierung des Breitbandkernnetzes durch den Bund. Sie bittet das BMI, diese nach Abstimmung mit den Ländern der IMK vorzulegen.

3. Die IMK weist darauf hin, dass frühzeitig Maßnahmen in Bund und Ländern zur Vorbereitung des Wechsels auf einen bundesweit einheitlichen Rahmenvertrag zu ergreifen sind.

4. Sie bittet ihren Vorsitzenden, die MPK und die FMK über diesen Beschluss und den Bericht zu informieren und erneut auf die Notwendigkeit eigener standardisierter Frequenzen hinzuweisen.

5. Die IMK löst die AG Breitband auf. Sie dankt den Mitgliedern der AG für die geleistete Arbeit.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 7: Früherkennung von potenziellen Amokläufern und Attentätern zur Verhinderung von Amokläufen und Anschlägen

Berichterstattung:	BMI
Hinweise:	IMK am 10.12.20 zu TOP 50
	AK II am 13./14.10.21 zu TOP 3
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI C 2.2/1

Beschluss:

1. Die IMK nimmt den „Ersten Zwischenbericht der Bund-Länderoffenen Arbeitsgruppe (BLAG) ‚Früherkennung von potenziellen Amokläufern und Attentätern zur Verhinderung von Amokläufen und Anschlägen' -VS-NfD-" (Stand: 20.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie betont, dass die Thematik aufgrund ihres Umfangs und ihrer Komplexität einer intensiven, fachlich versierten sowie breit gefächerten Befassung bedarf und unterstützt die hierfür vorgesehene Einbeziehung und enge Begleitung durch externe Wissenschaftler.

3. Die IMK beauftragt den AK II, ihr zur Herbstsitzung 2022 erneut zum Sachstand zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 8: Früherkennung von und Umgang mit Personen mit Risikopotential außerhalb der PMK

Berichterstattung:	Nordrhein-Westfalen
Hinweise:	Beschlussvorschlag NW vom 10.11.21
	Schreiben NW vom 29.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IX H 1.3/10

Beschluss:

1. Die IMK nimmt den mündlichen Bericht des Vertreters des Landes Nordrhein-Westfalen zu den Erfahrungen und Ergebnissen des Pilotprojekts PeRiskoP sowie der weiteren Vorgehensweise in Nordrhein-Westfalen zur Kenntnis und dankt für die Initiative.

2. Sie bittet Nordrhein-Westfalen, das Konzept PeRiskoP im Rahmen der nächsten AK II-Sitzung vorzustellen und den Ländern das Projekt sowie den Abschlussbericht zur Verfügung zu stellen.

3. Die IMK beauftragt den AK II, das Konzept PeRiskoP in die BLAG „Früherkennung von potenziellen Amokläufern und Attentätern zur Verhinderung von Amokläufen und Anschlägen“ einfließen zu lassen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 9: Bekämpfung von Gewalt im familiären Umfeld

Berichterstattung:	BMI
Hinweise:	IMK vom 17. bis 19.06.20 zu TOP 49
	AK II am 13./14.10.21 zu TOP 4
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 11.4

Beschluss:

1. Die IMK nimmt den „Ergebnisbericht Häusliche Gewalt“ (Stand: 31.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie begrüßt die Erarbeitung einer Definition des Begriffs „Häusliche Gewalt“ und spricht sich für eine bundeseinheitliche Anwendung aus.

3. Die IMK beauftragt den AK II zu prüfen, ob und wie eine Abbildung auch von niederschwelligen Massendelikten im Sinne der umfassenden Definition des Begriffs „Häusliche Gewalt“ im Bundeslagebild erfolgen kann. Hierbei sollen Erkenntnisse aus der Dunkelfeldforschung und die Arbeiten der BLAG „Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ berücksichtigt werden.

4. Die IMK begrüßt, dass der AK II bis zur Umstellung der Datenerfassung Lagebilder auf Basis der vorhandenen Daten vorlegt.

5. Sie bittet die Polizeien in Bund und Ländern, den Bericht auf weitere mögliche offene Handlungserfordernisse zu prüfen und diese umzusetzen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 11: Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten

Berichterstattung:	Baden-Württemberg
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 24
	UB AK II vom 12.11.21
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	VI D 11.4

Beschluss:

1. Die IMK nimmt den „Ersten Sachstandsbericht der Bund-Länderarbeitsgruppe ‚Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten'" (Stand: 22.10.21) (*freigegeben)* zur Kenntnis.

2. Sie begrüßt die beschriebene Vorgehensweise der Festlegung einer bundeseinheitlichen Definition „geschlechtsspezifisch gegen Frauen gerichteter Straftaten" als Grundlage für die weiteren, vom Auftrag erfassten Bereiche Statistik, Prävention, Bekämpfungsmaßnahmen und Forschungsbedarfe als zielführende Entwicklungsschritte in der weiteren Erarbeitung.

3. Die IMK beauftragt den AK II, ihr zur Frühjahrssitzung 2022 erneut zum Sachstand zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 12: Verbesserung der Bekämpfung des Menschenhandels und der Zwangsprostitution

Berichterstattung:	Nordrhein-Westfalen
Hinweise:	Beschlussvorschlag NW vom 18.10.21
	überarbeiteter Beschlussvorschlag NW vom 15.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IV E 3.1

Beschluss:

1. Die IMK nimmt den mündlichen Bericht des Vertreters des Landes Nordrhein-Westfalen zur derzeitigen Lage bei der Bekämpfung des Menschenhandels und der Zwangsprostitution zur Kenntnis.

2. Sie stellt fest, dass es sich bei Menschenhandel und Zwangsprostitution um schwere Menschenrechtsverletzungen handelt, welche eine konsequente Bekämpfung erfordern und denen mit einem gezielten und ganzheitlichen Ansatz begegnet werden muss.

3. Die IMK sieht insbesondere folgende Herausforderungen, welche sich u. a. aus dem Bundeslagebild „Menschenhandel und Ausbeutung 2019“ ergeben:

   - Die Identifizierung von Täterinnen und Tätern sowie Opfern wird durch die zunehmende Prostitutionsvermittlung über das Internet und die sozialen Medien erschwert.
   - Die Zuständigkeiten mehrerer Behörden für Kontrollen von Prostituierten und Prostitutionsstätten erfordern behördenübergreifende Kooperationen, um Menschenhandel erfolgreich zu bekämpfen.

- Minderjährige und Heranwachsende, die besonders gefährdet sind, Opfer zu werden, müssen auf Grund ihrer besonderen Vulnerabilität behördenübergreifend mit besonderen Bekämpfungs- und Präventionsmaßnahmen vor Ausbeutung geschützt werden.

4. Sie erachtet eine verstärkte Zusammenarbeit mit anderen Ressorts, Behörden und Institutionen auf nationaler und internationaler Ebene als wesentlichen Baustein für eine zielgerichtete und effektive Bekämpfung des Menschenhandels und der Zwangsprostitution.

5. Die IMK begrüßt die bereits im Bund und den Ländern vorgenommenen Maßnahmen und bittet die bereits bestehende BLAG Menschenhandel unter Federführung des BMFSFJ vor diesem Hintergrund den Vorschlag der IMK aufzugreifen, um die Optimierungspotenziale zur Verbesserung der multidisziplinär ausgerichteten Bekämpfung des Menschenhandels und der Zwangsprostitution zu überprüfen und weiter zu entwickeln.

6. Die IMK bittet das BMI, das BMFSFJ über diesen Beschluss zu informieren, und bittet die BLAG Menschenhandel, in Abstimmung mit der GFMK zu ihrer Herbstsitzung 2022 einen Bericht vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 13: Homophobe und transfeindliche Gewalt bekämpfen

Berichterstattung:	Berlin
Hinweise:	Beschlussvorschlag BE vom 12.10.21
	alternativer Beschlussvorschlag BY vom 16.11.21
	Mail BMI vom 16.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI D 10.1/4

Beschluss:

1. Die IMK nimmt mit Sorge zur Kenntnis, dass es immer wieder zu gewalttätigen, teils schweren Angriffen auf Lesben, Schwule, Bisexuelle, trans- und intergeschlechtliche Menschen (LSBTI) kommt. Erhebungen legen nahe, dass es im Bereich der LSBTI-feindlichen Gewalt zudem eine hohe Dunkelziffer von Übergriffen gibt, die nicht zur Anzeige gebracht werden. Die IMK verurteilt diese Angriffe auf das Schärfste. Sie unterstreicht die gesamtgesellschaftliche Bedeutung der Sichtbarmachung und wirksamen Bekämpfung dieser Form vorurteilsmotivierter Hasskriminalität, auch in Anbetracht der mit solchen Taten für die Opfer verbundenen physischen und psychischen Folgen.

2. Die IMK begrüßt, dass die Polizeien des Bundes und der Länder bereits diverse Maßnahmen getroffen haben, um gegen LSBTI-feindliche Straftaten vorzugehen. So unterliegen die Erfassungskriterien des Kriminalpolizeilichen Meldedienstes (KPMD-PMK) einer ständigen Evaluation. 2020 ist das Merkmal „Geschlecht/Sexuelle Identität“ im KPMD-PMK zusätzlich zum Merkmal „Sexuelle Orientierung“ als Unterthema im Themenfeld Hasskriminalität aufgenommen worden. In zahlreichen Dienststellen der Polizei unterstützen zudem Ansprechpersonen für LSBTI und für den Opferschutz geschultes Personal die tägliche Arbeit.

3. Die IMK sieht gleichwohl weiteren Handlungsbedarf. Sie bittet daher das BMI, ein unabhängiges Expertengremium aus Wissenschaft und Praxis, unter Einbindung von Fachverständigen aus der LSBTI-Gemeinschaft, einzusetzen. Dieses soll zur Herbstkonferenz 2022 einen ersten Bericht mit konkreten Handlungsempfehlungen vorlegen, wie die Bekämpfung von gegen LSBTI gerichteter Gewalttaten weiter verbessert werden kann. Insbesondere folgende Punkte sollen dabei in den Blick genommen werden:

   - Überprüfung bestehender Programme zur Aus- und Fortbildung bei den Polizeien des Bundes und der Länder,
   - weitere Sensibilisierung der Sicherheitsbehörden für die Opfer von homophober und transfeindlicher Gewalt,
   - Überprüfung des Handlungsbedarfs unter Berücksichtigung der bereits bestehenden Ansprechstellen in den Ländern hinsichtlich der standardisierten Vermittlung von Opfern von LSBTI-gerichteter Gewalt von den Polizeien des Bundes und der Länder an Beratungsstellen,
   - Überprüfung der statistischen Erfassung von Fällen der Hasskriminalität gegen LSBTI im KPMD-PMK, insbesondere hinsichtlich einer weiteren opferbezogenen Ausdifferenzierung,
   - Prüfung weiterer Maßnahmen zur Aufhellung des Dunkelfeldes,
   - Verdeutlichung LSBTI-feindlicher Hintergründe von Straftaten in polizeilichen Veröffentlichungen,
   - Überprüfung bestehender Ansätze zur Prävention der Polizeien des Bundes und der Länder und anderer Träger,
   - Prüfung der ausdrücklichen Aufnahme LSBTI-feindlicher Beweggründe und Motive in § 130 StGB sowie § 46 StGB.

4. Die IMK bittet ihren Vorsitzenden, die JuMiKo und die IntMK über diesen Beschluss zu informieren.

Protokollnotiz BMI:

BMI begrüßt grundsätzlich das Anliegen der IMK zur Bekämpfung von homophober und transfeindlicher Gewalt. Es ist jedoch anzunehmen, dass auch die neue Bundesregierung auf diesem Themenfeld eigene Impulse setzen wird. Dem sollte daher mit der in Ziffer 3 des Beschlussvorschlags avisierten Einsetzung eines unabhängigen Expertengremiums nicht vorgegriffen werden. So können auch etwaige Doppelstrukturen vermieden werden.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 14: Praxistauglichkeit des neuen § 99 Absatz 2 StPO – beschränkte Auskunftsmöglichkeiten über Postsendungen

Berichterstattung:	Hessen
Hinweis:	Beschlussvorschlag HE vom 06.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI B 4.1

Beschluss:

1. Die IMK nimmt den mündlichen Bericht des Vertreters des Landes Hessens zur Auskunftsmöglichkeit der Ermittlungsbehörden über die bei den Postdienstleistern gespeicherte Daten nach § 99 Absatz 2 StPO zur Kenntnis.

2. Sie stellt fest, dass von Postdienstleistern aufgrund des neu eingefügten Absatzes 2 in § 99 StPO über bestimmte, abschließend aufgezählte Daten Auskunft verlangt werden kann. Hiervon sind nicht alle Maßnahmen, die bislang als Minusmaßnahme zur „klassischen“ Postbeschlagnahme anerkannt waren, erfasst.

3. Die IMK beauftragt den AK II, bis zu ihrer Frühjahrssitzung 2022 zu prüfen, inwiefern in Bund und Ländern die seit dem 01.07.21 geltende Fassung des § 99 StPO im Rahmen von Ermittlungen zu Problemen geführt hat und ob Rechtssetzungsbedarf gesehen wird.

4. Die IMK bittet ihren Vorsitzenden, die JuMiKo über diesen Beschluss zu informieren.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 15: Digitale Spuren

Berichterstattung:	BMI
Hinweise:	IMK vom 12. bis 14.06.19 zu TOP 27
	IMK am 10.12.20 zu TOP 16
	Schr. Vors AK II an Vors. IMK vom 22.03.21
	AK II am 13./14.10.21 zu TOP 9
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 8

Beschluss:

1. Die IMK nimmt den Bericht „BLPG ‚Handlungsfelder Digitale Spuren' -VS-NfD-" (Stand: 30.06.21) *(nicht freigegeben)* insbesondere mit den Schwerpunkten

   – Sicherung Digitaler Spuren am Tatort,
   – Bewältigung von Massendaten,
   – Stärkung fachlicher Kompetenz,
   – Umgang mit der Kryptoproblematik und
   – Entwicklung neuer Technologien

   zur Kenntnis.

2. Sie weist darauf hin, dass aufgrund der Trendaussagen zur qualitativen und quantitativen Entwicklung Digitaler Spuren und insbesondere durch den exponentiellen Anstieg der Menge an sichergestellten Daten erheblicher Handlungsdruck besteht.

3. Die IMK stellt fest, dass die im Bericht genannten Schlussfolgerungen und Handlungsempfehlungen geeignet sind, um mit den Entwicklungen und Herausforderungen im Bereich der Digitalen Spuren Schritt halten zu können.

4. Sie betrachtet neben den Anforderungen der technischen Handlungsfelder das Handlungsfeld „Fachliche Kompetenz“ als besonders relevant und die Erlangung der damit verbundenen Mindestanforderungen unter Berücksichtigung der Handlungsempfehlungen als geeignete Grundlage, um den weiteren Herausforderungen angemessen begegnen zu können.

5. Die IMK empfiehlt, in den Polizeibehörden des Bundes und der Länder einen Soll-Ist-Abgleich auf Basis der Mindestanforderungen durchzuführen und Maßnahmen zu deren Erreichung im jeweiligen Zuständigkeitsbereich zu initiieren. Mit den formulierten Handlungsempfehlungen werden mögliche Maßnahmen bereits aufgezeigt.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 16: Kryptierte Täterkommunikation

Berichterstattung:	BMI
Hinweise:	AK II am 07./08.10.20 zu TOP 7
	IMK am 10.12.20 zu TOP 17
	AK II am 13./14.10.21 zu TOP 10
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 12.5/3

Beschluss:

1. Die IMK nimmt den Bericht „Kryptierte Täterkommunikation - Bewertung und Handlungsbedarfe -VS-NfD-“ (Stand: 02.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie stellt fest, dass
   - die bislang identifizierten Täterstrukturen durch die Strafverfolgungsmaßnahmen empfindlich geschwächt werden konnten,
   - die auf Basis der EncroChat-Daten erkannten Strukturen der Organisierten (Rauschgift-)Kriminalität aufgrund der Qualität und Quantität der begangenen und geplanten Straftaten eine wesentliche Bedrohung für die Innere Sicherheit darstellen und sich insbesondere aus dem relativ hohen Anteil bewaffneter Tatverdächtiger ein hohes Gefahren- und Bedrohungspotenzial ergibt,
   - Täterstrukturen zunehmend flexibel, arbeitsteilig und multiethnisch agieren und die Täter dabei auch außerhalb der bekannten Strukturen in zunehmendem Maße zweck- und profitorientiert mit anderen kriminellen Gruppierungen global vernetzt zusammenarbeiten,

- in den bislang geführten Ermittlungsverfahren erhebliche kriminelle Erträge festgestellt wurden und dies auf ein hohes finanzielles Potenzial hindeutet, welches von kriminellen Strukturen zum Beispiel zur Reinvestition in legale Wirtschaftszweige oder zur Einflussnahme genutzt werden kann,
- kryptierte Täterkommunikation auch künftig für organisierte kriminelle Gruppierungen von großer Bedeutung sein wird und demzufolge die Auswertung kryptierter Täterkommunikation von herausragender Bedeutung für die Bewertung von Art und Ausmaß der Organisierten Kriminalität sowie deren nachhaltiger Bekämpfung ist,
- die rechtlichen Problemstellungen in Bezug auf die Erhebung und Auswertung von kryptierter Kommunikation sich im Wesentlichen auf zwei Bereiche konzentrieren:
  - die fehlende Verpflichtung der Provider zur unverschlüsselten Ausleitung von Kommunikationsinhalten bei der TKÜ (siehe auch AK II am 07./08.10.20 zu TOP 7),
  - die fehlende Vorratsdatenspeicherung in verschiedenen Fallkonstellationen, insbesondere bei der Identifizierung von Tatverdächtigen aus den vorliegenden Metadaten, wie z. B. IP-Adressen oder Geodaten (siehe auch IMK am 10.12.20 zu TOP 17).

3. Die IMK hält die im Bericht beschriebenen Maßnahmen für geeignet, die Organisierte Kriminalität mit dem Schwerpunkt der Rauschgiftkriminalität wirksam zu bekämpfen und begrüßt die bereits beauftragten Arbeiten.

4. Sie beauftragt den AK II, zu ihrer Frühjahrssitzung 2022 einen fortgeschriebenen Bericht vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 17: Bewahrung der Möglichkeiten zur Telekommunikationsüberwachung

Berichterstattung:	Baden-Württemberg
Hinweis:	Beschlussvorschlag BW vom 12.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI D 12.5/3

Beschluss:

Die IMK fordert das BMI auf, sich – gegebenenfalls auch innerhalb der Europäischen Union – dafür einzusetzen, die Anbieter von internetbasierten Kommunikationsdiensten zu verpflichten, die technischen Voraussetzungen zu schaffen, um den Sicherheitsbehörden auf Basis der jeweils bestehenden rechtlichen Voraussetzungen die Kommunikationsinhalte unverschlüsselt zur Verfügung zu stellen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 19: Salafistisches Radikalisierungspotential in Justizvollzugsanstalten - Verbesserung der Erkenntnislage durch ein wissenschaftliches Auswerteprojekt

Berichterstattung:	BMI
Hinweise:	IMK vom 28. bis 30.11.18 zu TOP 25
	IMK vom 17. bis 19.06.20 zu TOP 15
	AK II am 13./14.10.21 zu TOP 12
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 4.4/9d

Beschluss:

1. Die IMK nimmt den „Abschlussbericht – Kurzfassung ‚Salafistisches Radikalisierungspotenzial in Justizvollzugsanstalten – SaRa-JVA‘ -VS-NfD-“ (Stand: 24.09.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie begrüßt die Befunde der von der Forschungsstelle Terrorismus / Extremismus des BKA durchgeführten Studie, dass sich in den Justizvollzugsanstalten vielfach Handlungsroutinen im Umgang mit Islamisten in Haft etabliert haben und dass das System des Justizvollzugs durchaus in der Lage ist, mit dem Zuwachs an Inhaftierungen umzugehen.

3. Die IMK betont die Wichtigkeit des Informationsaustauschs zwischen allen beteiligten Akteuren zu Radikalisierungs(verdachts)fällen in Haft und bei Haftentlassung, um die jeweiligen Maßnahmen bestmöglich aufeinander abzustimmen.

4. Sie begrüßt, dass die meisten Justizvollzugsanstalten sich im Bereich Deradikalisierung gut aufgestellt sehen. Sie betont, dass Sicherheits-, Justiz- und weitere Behörden sowie zivilgesellschaftliche Akteure gemeinsam zur Reintegration und Deradikalisierung radikalisierter Personen in Haft und nach Haftentlassung beitragen können.

5. Die IMK bittet ihren Vorsitzenden, die JuMiKo über diesen Beschluss und den Abschlussbericht in der Kurzfassung zu informieren.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 20: Nationales Waffenregister (NWR) - Betrieb und Ausbau zum NWR II

a) Sachstandsbericht

b) Vorschlag zur Neuausrichtung der Gremienstruktur für das ausgebaute föderale NWR-Gesamtsystem

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 8
	AK II am 13./14.10.21 zu TOP 15
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Berichte
Az.:	VII D 1

Beschluss:

1. Die IMK nimmt den „Bericht der Bund-Länder-Arbeitsgruppe (BL AG NWR) zum Nationalen Waffenregister an die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK), Version 1.0“ (Stand: 04.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie nimmt den Bericht „Kopfstelle zum Nationalen Waffenregister - Bericht über den Betrieb und die Mittelverwendung für die Jahre 2019 und 2020, Version 1.0“ (Stand: 09.06.21) *(nicht freigegeben)* zur Kenntnis.

3. Die IMK nimmt den im vorgenannten Bericht zur Kopfstelle dargelegten finanziellen Mehrbedarf für den ordnungsgemäßen Betrieb der Kopfstelle beim DVZ zur Kenntnis und stimmt einer Anpassung der föderalen Beiträge bis zum Inkrafttreten der geplanten neuen Verwaltungsvereinbarung (voraussichtlich Frühjahr 2022) für die ordnungsgemäße Aufgabenerfüllung für die Jahre 2022 und 2023 zu. Dieser Beschluss ergänzt insoweit die Verwaltungsvereinbarung zur Finanzierung (des Ausbaus des NWR) aus 2016.

4. Sie beauftragt die BL AG NWR, in Abstimmung mit den Waffenrechtsreferenten des Bundes und der Länder vor dem Hintergrund der Ziffer 3 dieses Beschlusses (finanzieller Mehrbedarf für die Kopfstelle), schnellstmöglich eine neue Verwaltungsvereinbarung für das ausgebaute NWR-IT-Gesamtsystem, möglichst bis zum Frühjahr 2022, vorzulegen. Hierzu sollen die vorhandenen NWR-Verwaltungsvereinbarungen zusammengeführt und erforderliche fachliche oder organisatorische Ergänzungen vorgenommen werden. Ziel ist, zukünftig eine stabile, ausreichende Finanzierung aller Betriebs- und Steuerungskomponenten des föderalen Verfahrens NWR sicherzustellen.

5. Die IMK begrüßt den Vorschlag des BMI und des BVA zum Einsatz des NWR als technisches Erprobungsregister der Registermodernisierung und bittet die BL AG NWR, das Erprobungsregister auch über die Gremienstruktur des NWR zu unterstützen. Sie nimmt zur Kenntnis, die Planung des NWR-Erprobungsregisters mit dem Ziel einer schrittweisen und zeitnahen Inbetriebnahme in 2023 auszurichten und hierfür auch fachliche und finanzielle Unterstützung aus dem Projekt Registermodernisierung zu nutzen. Sollten zur Einführung des NWR als Erprobungsregister rechtliche Anpassungen erforderlich sein, bittet die IMK die BL AG NWR, dieses Projekt zu unterstützen.

6. Sie beauftragt die BL AG NWR, weiterhin alle erforderlichen Maßnahmen zu prüfen und zu ergreifen, um notwendige Optimierungen und Anpassungen (Änderungsmanagement) am föderalen NWR-IT-Gesamtsystem vorzunehmen. Sie beauftragt die BL AG NWR, weiterhin anlass- und themenbezogen zum Sachstand des NWR zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 21: Unnötige Ressourcenbindung bei den Sicherheitsbehörden im Rahmen der waffenrechtlichen Zuverlässigkeitsüberprüfung von Jägern

Berichterstattung:	Brandenburg
Hinweis:	Beschlussvorschlag BB vom 12.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VII D 1.1

Beschluss:

1. Die IMK stellt fest, dass die Überprüfung der waffenrechtlichen Zuverlässigkeit von Inhabern jagdrechtlicher Erlaubnisse durch die Jagdbehörde und in Fällen, in denen Jäger im Besitz eigener Waffen sind, zusätzlich durch die Waffenbehörde erfolgt. Dies bindet doppelte Ressourcen der Sicherheitsbehörden ohne erkennbaren Sicherheitsgewinn.

2. Sie bittet ihren Vorsitzenden, die AMK über diesen Beschluss zu informieren und um Prüfung zu ersuchen, ob mit einer Änderung des § 17 des Bundesjagdgesetzes klargestellt werden kann, dass die Waffenbehörde für die Prüfung der waffenrechtlichen Zuverlässigkeit von Antragstellern auf oder Inhabern jagdrechtliche(r) Erlaubnisse allein zuständige Behörde ist, mithin die Jagdbehörde lediglich auf die Erkenntnisse der Waffenbehörde zurückgreift oder ob den Ländern im Rahmen einer Verordnungsermächtigung im Bundesjagdgesetz die Möglichkeit eingeräumt werden kann, eine entsprechende Landesregelung vorzunehmen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 22: Stellenpool für Auslandsverwendungen und internationale Polizeimissionen

Berichterstattung:	BMI
Hinweise:	IMK vom 28. bis 30.11.18 zu TOP 35
	AK II am 13./14.10.21 zu TOP 18
Veröffentlichung:	Freigabe Beschluss
Az.:	VI G 6.1

Beschluss:

1. Die IMK nimmt den mündlichen Bericht des BMI über die Umsetzung der Planungen für einen sogenannten Stellenpool für Auslandsverwendungen und internationale Polizeimissionen durch eine Verwaltungsvereinbarung zur Förderung des Einsatzes von Polizeibeamtinnen und -beamten der Länder in internationalen Polizeimissionen zur Kenntnis.

2. Sie begrüßt den Abschluss der Verwaltungsvereinbarung zur Förderung des Einsatzes von Polizeibeamtinnen und -beamten der Länder in internationalen Polizeimissionen durch die Erstattung der Personalkosten der Länder durch den Bund.

3. Die IMK bekräftigt ihr Bekenntnis zu einem starken Engagement mit Polizistinnen und Polizisten in internationalen Friedensmissionen und im Rahmen der institutionellen Beteiligung.

4. Sie bittet ihren Vorsitzenden, die MPK über diesen Beschluss zu unterrichten und diese darum zu ersuchen, sich dem Bekenntnis der IMK zum polizeilichen Auslandsengagement anzuschließen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 23: Leitlinien zur Vorbereitung und Durchführung polizeilicher Einsätze anlässlich der Fußballeuropameisterschaft 2024

Berichterstattung:	Nordrhein-Westfalen
Hinweise:	UB IMK vom 25.03.19
	AK II am 13./14.10.21 zu TOP 20
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI C 2.2/4b

Beschluss:

1. Die IMK nimmt den Bericht „Leitlinien und taktische Ziele zur Vorbereitung und Durchführung polizeilicher Einsätze der ‚Projektgruppe zur Vorbereitung und Durchführung der polizeilichen Einsätze sowie zur Erarbeitung und Fortschreibung einer abgestimmten Rahmenkonzeption der Polizeien des Bundes und der Länder für die Fußballeuropameisterschaft der Männer 2024 (PG EM 2024)‘ -VS-NfD-“ (Stand: 10.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie erklärt ihre Absicht, die Leitlinien zur Grundlage der Vorbereitung der Polizeien des Bundes und der Länder zur Durchführung von Maßnahmen vor und während der EM 2024 zu machen. Hierbei sollen in Bezug auf präventive Maßnahmen gegenüber den verschiedenen Gefahrenpotenzialen die mit zunehmender Nähe zur Veranstaltung konkretisierten Lageerkenntnisse und wahrscheinlichen Gefahrenszenarien im Vordergrund stehen**.**

3. Die IMK ist sich der überaus bedeutenden Verantwortung der Polizeien des Bundes und der Länder für die Gewährleistung der öffentlichen Sicherheit während der EM 2024 bewusst und appelliert an alle Beteiligten, ihren Beitrag für eine sichere Durchführung der Europameisterschaft zu leisten. Einer engen Zusammenarbeit mit den zuständigen Polizeibehörden kommt dabei bereits in der Vorbereitungsphase eine besondere Bedeutung zu.

4. Die IMK bittet die im Nationalen Koordinierungsausschuss zur Erarbeitung des „Nationalen Konzepts EURO 2024“ vertretenen Behörden, Einrichtungen und Institutionen sowie den ebenfalls darin vertretenen Ausrichter der EM 2024, die erforderlichen Teilkonzepte aus ihren Verantwortungsbereichen zeitnah zu erstellen, dem Nationalen Koordinierungsausschuss zu übermitteln und eigenverantwortlich fortzuschreiben.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 24: Nationaler Koordinierungsausschuss UEFA EURO 2024

Berichterstattung:	BMI
Hinweise:	UB IMK vom 25.03.19
	AK II am 13./14.10.21 zu TOP 21
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	VI C 2.2/4b

Beschluss:

1. Die IMK nimmt den „Bericht zum Sachstand des IMK-Auftrags vom 25.03.19 anlässlich der Vorbereitung der UEFA EURO 2024“ (Stand: 05.08.21) *(freigegeben)* zur Kenntnis.

2. Sie stellt fest, dass es einer ganzheitlichen Befassung mit sicherheitsrelevanten, politischen und gesamtgesellschaftlichen Themenfeldern bedarf, um den Herausforderungen für die UEFA EURO 2024 gerecht zu werden.

3. Die IMK erkennt daher den Bedarf einer Modifizierung des für die Durchführung der FIFA Fußball-Weltmeisterschaft 2006 eingesetzten Bund-Länder-Ausschusses (BLA) für die nun bevorstehende UEFA Fußball-Europameisterschaft 2024.

4. Sie stimmt der Umbenennung des „Bund-Länder-Ausschusses“ in „Nationaler Koordinierungsausschuss (NKA)“ mit der damit einhergehenden Modifizierung im Sinne einer gesamtheitlichen Befassung zu.

5. Die IMK beauftragt den AK II, weiter anlassbezogen über den Stand der Umsetzung zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 26: Unterstützung der Special Olympics World Games 2023 durch die Polizeien der Länder und des Bundes

Berichterstattung:	Baden-Württemberg
Hinweis:	Beschlussvorschlag BW vom 26.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI F 2

Beschluss:

1. Die IMK nimmt zur Kenntnis, dass die Special Olympics World Games 2023 in Berlin ausgerichtet werden. Sie anerkennt deren besondere Bedeutung für die mit der Veranstaltung verknüpften Ziele der Inklusion, Teilhabe und Bewusstseinsbildung in der Bundesrepublik Deutschland.

2. Sie unterstützt die polizeiliche Beteiligung im Rahmen der rechtlichen Möglichkeiten sowie im Sinne einer freiwilligen Teilnahme von Polizeibeamtinnen und Polizeibeamten am Fackellauf.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 27: Sicherheit bei Sportveranstaltungen – Einbringen von pyrotechnischen Gegenständen in Sportstätten

Berichterstattung:	Nordrhein-Westfalen
Hinweise:	IMK vom 04. bis 06.12.19 zu TOP 16
	IMK vom 16. bis 18.06.21 zu TOP 10
	AK II am 13./14.10.21 zu TOP 22
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI C 2.2/4b

Beschluss:

1. Die IMK nimmt den „Abschlussbericht der AG ‚Verhinderung des Einbringens von Pyrotechnik in Sportstätten'" (Stand: 25.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie hält die unter Beteiligung von DFB und DFL erarbeiteten Handlungsempfehlungen für geeignet, die Sicherheit in Stadien zu erhöhen. Die IMK beauftragt den AK II, die Umsetzung der Handlungsempfehlungen unter Einbeziehung des Nationalen Ausschusses Sport und Sicherheit (NASS) und insbesondere unter Beteiligung des DFB und der DFL zu begleiten.

3. Sie beauftragt den AK II, bis zur Herbstsitzung 2022 über die Umsetzung der Handlungsempfehlungen zu berichten.

4. Die IMK bittet das BMI, sich innerhalb der Bundesregierung für einen Gesetzgebungsvorschlag zur Einführung eines Verbotes des Mitführens von Pyrotechnik in Sportstätten durch einen Ordnungswidrigkeiten- oder Straftatbestand einzusetzen.

Protokollnotiz BMI:

Hinsichtlich der Handlungsempfehlungen unter 4.1 (Arbeitspaket 1 - Rechtslage) des Abschlussberichts der Arbeitsgruppe des UA FEK zur Verhinderung des Einbringens von Pyrotechnik in Sportstätten weist der Bund darauf hin, dass die konkrete Ausgestaltung der dort genannten Änderungen im Sprengstoffgesetz weiterer Prüfung im Rahmen eines künftigen Gesetzgebungsverfahrens bedarf, um die gewollte Regelung hinreichend präzise zu fassen. Für die vorgeschlagene Erweiterung des § 40 Absatz 5 Satz 2 SprengG gilt dies insofern, als ein konkreter Verwendungszweck nicht für alle pyrotechnischen Gegenstände hinreichend genau festgeschrieben ist bzw. sich festschreiben lässt. Hinsichtlich des vorgeschlagenen Ordnungswidrigkeitstatbestandes in § 41 SprengG müssten sowohl die konkreten pyrotechnischen Gegenstände (als Kategorien im Sinne des Sprengstoffrechts) als auch die gemeinten Veranstaltungen näher eingegrenzt werden. Anderenfalls wären schlechthin alle pyrotechnischen Gegenstände, einschließlich Kleinstfeuerwerk (z. B. Wunderkerzen) und sonstiger pyrotechnischer Gegenstände, auch für technische Zwecke (z. B. Airbags) miterfasst, deren Mitführen oder auch Verwenden bei bestimmen Veranstaltungen erwünscht bzw. gar geboten sein könnte.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 31: Erhöhung der Verkehrssicherheit / Überarbeitung der Bußgeldkatalog-Verordnung (BKatV) und Änderung des Ordnungswidrigkeitengesetzes (OWiG)

Berichterstattung:	Brandenburg
Hinweis:	aktualisierter Beschlussvorschlag BB vom 10.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VII C 1.4

Beschluss:

1. Am 9. November 2021 ist die Erste Verordnung zur Änderung der Bußgeldkatalog-Verordnung (BKatV) in Kraft getreten. Die IMK begrüßt, dass damit die Regelungen des Artikels 3 der 54. Verordnung zur Änderung der StVO u. a. Vorschriften (StVRÄndV) bestätigt und neu gefasst werden.

2. Sie hält gleichwohl eine erneute ganzheitliche Diskussion der Bußgeldkatalog-Verordnung (und des OWiG) für erforderlich, um den im Zuge der Nichtigkeitserklärung des Artikels 3 der o. g. Verordnung begonnenen konstruktiven Austausch zwischen Bund und Ländern zur Erhöhung der Verkehrssicherheit fortzusetzen sowie bestehende Divergenzen (z. B. Verwarnungsgeldobergrenze, Gebühren für Halterkostenbescheide) zu beseitigen.

3. Die IMK bittet ihren Vorsitzenden, die VMK über diesen Beschluss zu informieren und darum zu ersuchen, die erforderlichen Schritte für den unter Ziffer 2 genannten Diskussionsprozess zu initiieren.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 32: Initiierung einer Bund-Länder-Arbeitsgemeinschaft „Kampfmittelräumung“

Berichterstattung:	Mecklenburg-Vorpommern
Hinweise:	IMK vom 04. bis 06.12.19 zu TOP 45
	IMK am 10.12.20 zu TOP 20
	AK II am 13./14.10.21 zu TOP 31
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VII F

Beschluss:

1. Die IMK nimmt den „2. Bericht der Bund-Länder-Arbeitsgruppe des UA FEK unter Beteiligung des AK V, der Bundesanstalt für Immobilienaufgaben und der Leitstelle des Bundes für Kampfmittelräumung zum Stand der Kampfmittelräumung in den Ländern -VS-NfD-“ (Stand: 16.08.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie begrüßt den Vorschlag einer intensiven Erörterung zwischen der BLAG Kampfmittelräumung und dem Expertengremium der Bund/Länder-Arbeitsgemeinschaft Nord- und Ostsee (BLANO) zum Themenkomplex „Munition im Meer“.

3. Die IMK hält es für erforderlich, die Zuständigkeiten für die Entsorgung von sogenannter Nato-Munition zwischen dem Bund (Bundeswehr) und den Ländern zu aktualisieren. Sie wird sich hierzu gegenüber dem Bundesministerium für Verteidigung (BMVg) positionieren.

4. Die IMK sieht die Notwendigkeit, die Entsorgungswege und -kapazitäten von Kampfmitteln in den Ländern und beim Bund vertiefend zu analysieren und Lösungsvorschläge für eine sachgerechte Erhöhung der Vernichtungskapazität zu entwickeln.

5. Sie begrüßt den Vorschlag, weitere Standards bei dem Einsatz geophysikalischer Verfahren, der Qualitätskontrolle und Ergebnisdokumentation sowie dem Qualifizierungsniveau von Beteiligten in der Kampfmittelräumung unter der Beteiligung der Arbeitsgemeinschaft der Leiter der Kampfmittelräumdienste zu erarbeiten.

6. Die IMK beauftragt den AK II in Abstimmung mit dem AK V, eine weitere vertiefende Untersuchung, insbesondere zur Darstellung und zur Identifizierung von konkreten Problemstellungen und Harmonisierungspotenzialen (u. a. organisatorische und rechtliche Aspekte) durchzuführen und zur Herbstsitzung 2022 einen Bericht vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 35: Geldautomatensprengung

Berichterstattung:	Bayern
Hinweise:	UB IMK vom 02.10.19
	Schr. Deutsche Kreditwirtschaft an Vors. IMK vom 26.11.19
	AK II am 13./14.10.21 zu TOP 40
	alternativer Beschlussvorschlag NI vom 29.11.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI E 1.10/7

Beschluss:

1. Die IMK nimmt den „Ergebnisbericht der UA RV-Arbeitsgruppe ‚Geldautomatensprengung'" (Stand: 01.04.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie stellt fest, dass die weitere Befassung mit der Einführung einer Verpflichtung von Herstellern und Betreibern von Geldautomaten zum Ergreifen von Maßnahmen zur Sicherung von Geldautomaten mittels EU-Verordnung, analog der Abgasverordnung bei Kfz, bis zum Ergebnis der erneuten Evaluation 2022 zur Thematik Geldautomatensprengung zurückgestellt werden sollte.

3. Die IMK bittet das BMI, sich innerhalb der Bundesregierung für eine Prüfung der rechtlichen Verpflichtung von Herstellern und Betreibern von Geldautomaten zum Ergreifen von Maßnahmen zur Sicherung von Geldautomaten einzusetzen und der IMK in der Frühjahrssitzung 2022 über die Möglichkeiten zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 38: Erhöhung der Obergrenze der Beteiligung Deutschlands an der Mission der Europäischen Union zum Ausbau der Kapazitäten in Somalia (EUCAP Somalia) mit Polizeibeamtinnen und -beamten des Bundes und der Länder

Berichterstattung:	BMI
Hinweis:	Beschlussvorschlag BMI vom 15.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI G 6.13

Beschluss:

1. Die IMK nimmt den Beschluss der Bundesregierung vom 20.10.21 zur Erhöhung der Obergrenze der Beteiligung deutscher Polizeibeamtinnen und -beamter an der EU-Mission zum Ausbau der Kapazitäten in Somalia (EUCAP Somalia) von bisher fünf auf zukünftig bis zu zehn Beamtinnen und Beamte zur Kenntnis.

2. Die Innenministerinnen, Innenminister und -senatoren der Länder unterstützen die Bemühungen der Europäischen Union.

3. Die IMK stimmt der Entsendung von zukünftig bis zu zehn Beamtinnen und Beamten der Polizeien des Bundes und der Länder in die EU-Mission EUCAP Somalia im Rahmen der „Leitlinien für die gemeinsame Beteiligung des Bundes und der Länder an internationalen Polizeimissionen“ zu.

4. Der Einsatz der Polizeibeamtinnen und -beamten des Bundes und der Länder erfolgt grundsätzlich unbewaffnet. Insofern für besondere Funktionen z. B. im Bereich des Personenschutzes durch die Mission eine Bewaffnung vorgesehen ist, erfolgt diese im Einklang mit den hierzu einschlägigen Vorschriften der Mission bzw. mit dem Status of Mission Agreement.

5. Die IMK beauftragt die Arbeitsgruppe Internationale Polizeimissionen (AG IPM), die erforderlichen Maßnahmen zu treffen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 43: Entwicklung des Linksextremismus in Deutschland am Beispiel der Stadt Leipzig

Berichterstattung:	Sachsen
Hinweis	Beschlussvorschlag SN vom 01.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI D 4.3/2

Beschluss:

1. Die IMK nimmt den mündlichen Bericht des Vertreters des Freistaates Sachsen zur Kenntnis

2. Sie erachtet es als notwendig, die Zusammenarbeit von Bund und Ländern und ihre Anstrengungen bei der Aufklärung und Bekämpfung des Linksextremismus weiter zu verstärken.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 44: Lehren aus dem vereitelten Anschlag auf eine Synagoge in Hagen

Berichterstattung:	Nordrhein-Westfalen
Hinweise:	Beschlussvorschlag NW vom 25.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IX H 1.3/10

Beschluss:

1. Die IMK verurteilt die feigen Pläne für einen Anschlag auf die Synagoge in Hagen. Sie dankt Verfassungsschutz und Polizei für das entschlossene und koordinierte Vorgehen zur Verhinderung des Anschlags.

2. Sie betont die besondere Bedeutung des Internets für die Radikalisierung von Extremisten und für die Vorbereitung von Anschlägen und nimmt zur Kenntnis, dass den Hinweisen ausländischer Nachrichtendienste gerade für die Verhinderung von extremistischen Anschlägen ein besonderes Gewicht zukommt.

3. Die IMK stellt fest, dass es die Arbeitsmöglichkeiten der Sicherheitsbehörden fortlaufend zu modernisieren gilt, um die sich ständig verändernden Gefährdungen der inneren Sicherheit auch in Zukunft bestmöglich abwehren zu können.

4. Die IMK beauftragt den AK IV, zu ihrer Frühjahrssitzung 2022 einen Bericht zur weiteren Verbesserung der Früherkennung von sich radikalisierenden Personen im Internet vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 45: **Lehren aus Katastrophenlagen ziehen: Stabsausbildung an der Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung ausweiten**

Berichterstattung:	Hessen
Hinweise:	Beschlussvorschlag HE vom 06.10.21
	aktualisierter Beschlussvorschlag HE vom 01.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	X E 7

Beschluss:

1. Bei flächendeckenden, langanhaltenden Katastrophen- bzw. Großschadenslagen sind aufwuchsfähige Stabsstrukturen Kernbestandteil einer erfolgreichen Lagebewältigung.

2. Die IMK bittet das BMI, das Angebot der Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ) in diesem Bereich deutlich auszuweiten und dabei insbesondere auch weitere Ausbildungs- und Übungsangebote für sämtliche Verwaltungs- und Katastrophenschutzstäbe vorzusehen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 46: Länderoffene Bund-Länder-Kommission „Stärkung des Bevölkerungsschutzes“

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 33
	Beschlussvorschlag BMI vom 19.10.21
	ergänzter Beschlussvorschlag BMI vom 09.11.21
Veröffentlichung:	Freigabe Beschluss und Bericht, keine Freigabe des Entwurfs der Verwaltungsvereinbarung
Az.:	X A 3.2

Beschluss:

1. Die IMK nimmt den Bericht zum Sachstand der Länderoffenen Bund-Länder-Kommission „Stärkung des Bevölkerungsschutzes“ (Stand: 09.11.21) *(freigegeben)* zur Kenntnis.

2. Sie nimmt den Entwurf einer Vereinbarung über die Errichtung eines Gemeinsamen Kompetenzzentrums Bevölkerungsschutz (Stand: 09.11.21) *(nicht freigegeben)* des Bundes und der Länder zur Kenntnis. Sie sieht in dem Entwurf eine gute Grundlage für die Errichtung eines Gemeinsamen Kompetenzzentrums Bevölkerungsschutz des Bundes und der Länder.

3. Die IMK beauftragt die Bund-Länder-Kommission, eine unterzeichnungsreife Fassung der Vereinbarung auf Arbeitsebene zwischen BMI und Ländern zu erstellen und zur Frühjahrssitzung 2022 der IMK vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 47: Bund-Länder-Vereinbarung über Finanzhilfen des Bundes zur Verbesserung der Warninfrastruktur in den Ländern

– Sonderförderprogramm Sirenen –

Berichterstattung:	Hamburg
Hinweise:	Beschlussvorschlag von HH vom 15.10.21
	alternativer Beschlussvorschlag BMI vom 10.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	X E 5

Beschluss:

1. Die IMK betont die Wichtigkeit der Warnung der Bevölkerung im Katastrophenfall als Kernelement des Bevölkerungsschutzes. Insbesondere der Warnung mittels Sirenen im Katastrophen- und Zivilschutz kommt dabei aufgrund ihres Weckeffekts weiterhin eine essentielle Rolle zu.

2. Sie betrachtet die Weiterentwicklung der hierzu bereits bestehenden Sirenenwarnnetze als geeignet und unverzichtbar und begrüßt das Sirenenförderprogramm des Bundes. Sie sieht in dem bestehenden Förderprogramm des Bundes allerdings noch keine ausreichende Finanzierungsbasis für eine effektive Weiterentwicklung des Sirenenprogramms und fordert den Bund daher auf, das Förderprogramm zu verstetigen und auch über das geplante Förderende 2022 hinaus weitere Fördermittel bereitzustellen.

3. Die IMK stellt fest, dass der vom Bund als Fördervoranmeldung verlangte zahlungswirksame Mittelabfluss bis 31.12.22 die volle Ausschöpfung des Förderprogramms und den von den Ländern geplanten Umfang der Modernisierung des Sirenenwarnsystems gefährdet.

4. Die IMK fordert den Bund daher auf, die Förderzusage auf alle Maßnahmen auszudehnen, über die bis Ende 2022 Verträge geschlossen sind, auch wenn die Mittel erst in 2023 oder 2024 abfließen.

Protokollnotiz BMI:

Der Bund sagt zu, sich im Rahmen seiner Finanzierungskompetenzen der kommenden Haushaltsverhandlungen für weitere Mittel zum Aufbau von Sirenen einzusetzen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 48: Mehr Gestaltungsspielräume für Kommunen hinsichtlich des Umgangs mit Silvesterfeuerwerk

Berichterstattung:	Bremen
Hinweise:	IMK am 10.12.20 zu TOP 39
	Beschlussvorschlag von HB vom 13.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	X D 2

Beschluss:

Die IMK bittet das BMI, zur IMK im Frühjahr 2022 über den Sachstand der - im Rahmen der von ihm geplanten Novellierung des Sprengstoffrechts - erbetenen Prüfung der Einführung einer Ermächtigungsgrundlage zur Einschränkung des Abbrennens erlaubnisfreien Feuerwerks für Kommunen in der Ersten Verordnung zum Sprengstoffgesetz zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 49: Einschleusung von Asylsuchenden aus Belarus nach Deutschland

Berichterstattung:	Brandenburg / Sachsen
Hinweis:	Beschlussvorschlag BB und SN vom 22.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IV E 5

Beschluss:

Die IMK fordert das BMI auf, weitere geeignete Maßnahmen zu ergreifen, um die Einschleusung von Asylsuchenden aus Belarus nach Deutschland zu unterbinden.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 50: Sekundärmigration aus Griechenland

Berichterstattung:	Brandenburg / Sachsen
Hinweise:	Beschlussvorschlag BB und SN vom 25.10.21
	Mail BMI vom 16.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IV B 2.2b

Beschluss:

Die IMK fordert das BMI auf, geeignete Maßnahmen zu ergreifen, um die Sekundärmigration aus Griechenland einzudämmen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 51: Entwicklung der Zugänge von Asylsuchenden

Berichterstattung:	Sachsen-Anhalt
Hinweis:	Beschlussvorschlag ST vom 02.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IV A 2.1

Beschluss:

Die IMK nimmt den mündlichen Bericht des BMI - unter Einbeziehung des Auswärtigen Amtes und des BMZ - zu den konkreten Maßnahmen, die in der Vergangenheit ergriffen wurden und zukünftig ergriffen werden, um die wirtschaftliche Situation in den Herkunftsländern der Asylsuchenden und in den jeweiligen Nachbarstaaten zu stabilisieren mit dem Ziel, die Fluchtbewegungen einzudämmen, zur Kenntnis.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 52: Lage in Afghanistan

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 64
	Schreiben RP, BE, HB und TH an BMI vom 20.07.21
	Beschlussvorschlag BMI vom 15.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI G 6.12

Beschluss:

Die IMK nimmt den mündlichen Bericht des BMI zur Lage in Afghanistan zur Kenntnis.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 54: Aufnahme ehemaliger Ortskräfte und weiterer afghanischer Staatsangehöriger - Organisation zwischen Bund und Ländern

Berichterstattung:	Bayern
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 64
	AK I am 30.09./01.10.21 zu TOP 4
	alternativer Beschlussvorschlag BMI vom 10.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI G 6.12

Beschluss:

1. Die IMK stellt fest, dass die Unterbringung und Versorgung von ehemaligen Ortskräften und besonders gefährdeten Afghaninnen und Afghanen vor dem Hintergrund der ansteigenden Zugangszahlen eine große Herausforderung darstellt.

2. Sie begrüßt, dass das BMI aufgrund der hohen Zugangszahlen in einem einheitlichen und zentral durchgeführten Verfahren eine Erstunterbringung der Personen als notwendige Voraussetzung für die koordinierte Aufnahme organisiert und finanziert. In diesem Zusammenhang weist sie auch auf die sehr kurzen Vorlaufzeiten bei der Einreise von nach § 22 Satz 2 AufenthG aufgenommenen Personen hin, die eine zentrale Erstunterbringung durch den Bund für mindestens fünf Werktage zwingend erforderlich macht.

3. Die IMK nimmt die Zusage des BMI zur Kenntnis, den Ländern auch künftig zeitnah alle relevanten Informationen zum Sachstand der organisierten Einreisen und zur rechtlichen Einschätzung entweder im Rahmen regelmäßiger Jours Fixes oder im Wege gesonderter Ausarbeitungen zur Verfügung zu stellen oder gegebenenfalls einen Ansprechpartner im zuständigen Ressort zu vermitteln.

noch TOP 54

Protokollnotiz BMI:

1. Das BMI erkennt an, dass die Unterbringung und Versorgung von ehemaligen Ortskräften und besonders gefährdeten Afghaninnen und Afghanen vor dem Hintergrund der ansteigenden Zugangszahlen eine große Herausforderung für die Länder darstellt.
2. Das BMI weist darauf hin, dass die Aufnahme und Unterbringung von nach § 22 Satz 2 AufenthG aufgenommenen Personen ebenso wie die Aufnahme und Unterbringung von Asylbegehrenden nach den geltenden gesetzlichen Regelungen den Ländern obliegt. Aufgrund der hohen Zugangs-zahlen hat das BMI bereits im Wege einer weiten Auslegung des § 75 Nr. 8 AufenthG eine Erstunterbringung der Personen organisiert und finanziert.
3. Das BMI will auch künftig in Fällen, in denen Informationen über Sammeleinreisen nicht mit einem Vorlauf von mindestens 5 Werktagen übermittelt werden, eine zentrale Erstunterbringung vorzugsweise in einer Bundeswehrkaserne einer von den Ländern zur Verfügung gestellten Erstaufnahmeeinrichtung organisieren und finanzieren.
4. Das BMI hält eine zentrale Auskunftsstelle für nicht zielführend, sagt jedoch zu, den Ländern auch künftig zeitnah alle relevanten Informationen zum Sachstand der organisierten Einreisen und zur rechtlichen Einschätzung entweder im Rahmen regelmäßiger Jour Fixe oder im Wege gesonderter Ausarbeitungen zur Verfügung zu stellen oder gegebenenfalls einen Ansprechpartner im zuständigen Ressort zu vermitteln.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 55: Vorstellung des Assistenzsystems zur Behördenvernetzung im Asylbereich „FLORA“

Berichterstattung:	Sachsen
Hinweis:	Beschlussvorschlag SN vom 08.10.21
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	IV F 4

Beschluss:

Die IMK nimmt den „Berichtsstand zu IT-Pilotisierung ‚Förderale Blockchain-Infrastruktur Asyl (FLORA) - Assistenzsystem zur Behördenvernetzung“ (Stand: 28.10.21) *(freigegeben)* sowie die mündlichen Ergänzungen des BMI über das in der AnkER-Einrichtung Dresden realisierte Pilotprojekt für eine föderale Blockchain-Infrastruktur Asyl (FLORA) zur Kenntnis.

TOP 56: Fehlende Kooperationsbereitschaft anderer Staaten bei der Rücknahme eigener, in Deutschland ausreisepflichtiger, Staatsangehöriger

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 63
	Beschlussvorschlag BMI vom 15.10.21
	alternativer Beschlussvorschlag NW vom 11.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	IV E 1.1

Beschluss:

1. Die IMK nimmt den mündlichen Bericht des BMI zur Kenntnis.

2. Sie bittet das BMI, sich künftig verstärkt für ein kohärentes Vorgehen einzusetzen, insbesondere mit Blick auf den Abschluss ganzheitlicher Kooperationsabkommen mit bestimmten Drittstaaten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 57: **Verbesserung der Durchsetzung von Ausweisungen und Abschiebungen bei straffälligen Ausländen/ Flüchtlingen und Gefährdern**

- Abschlussbericht zu TOP 29 Ziffer 2 und 3 der Herbst-IMK 2019 zur „Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht“

Berichterstattung:	BMI
Hinweise:	MPK am 05.12.18 zu TOP 4
	Schr. Vors. MPK an Vors. IMK vom 12.12.18
	IMK vom 12. bis 14.06.19 zu TOP 2
	IMK vom 04. bis 06.12.19 zu TOP 29
	Beschlussvorschlag BMI vom 10.09.21
	AK I am 30.09./01.10.21 zu TOP 2
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	IV E 1.3

Beschluss:

1. Die IMK nimmt den „Abschlussbericht des BMI zu TOP 29 Ziffer 2 und 3 der 211. Innenministerkonferenz vom 4. bis 6. Dezember 2019 in Lübeck zur ‚Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht‘“ (Stand: 10.09.21) *(freigegeben)* zur Kenntnis.

2. Sie bittet das BMI ausgehend von dem Abschlussbericht zu prüfen, mit welchen Maßnahmen der Vollzug der Ausreisepflicht weiter verbessert werden kann und zur Frühjahrsitzung 2022 zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 60: „Cybersicherheitsstrategie für Deutschland 2021“ der Bundesregierung

Berichterstattung:	BMI
Hinweis:	Beschlussvorschlag BMI vom 15.10.21
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	VI D 8

Beschluss:

1. Die IMK nimmt die „Cybersicherheitsstrategie für Deutschland 2021“ (Stand: August 2021) *(freigegeben)* der Bundesregierung zur Kenntnis.

2. Sie begrüßt, dass die Länder eng in den Erarbeitungsprozess eingebunden und in der Strategie berücksichtigt worden sind.

3. Die IMK betont, dass die vielfältigen staatlichen Aufgaben im Cyberraum nur durch eine gemeinsame Anstrengung von Bund und Ländern erfüllt werden können. Eine intensive Verzahnung der Aktivitäten der Bundes- und Landesebene auf dem Wege einer kooperativen und komplementären Zusammenarbeit ist hierbei unumgänglich. Die IMK begrüßt, dass die Strategie der Bundesregierung diese Prämisse abbildet.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 64: Bericht aus dem Nationalen Cyber-Sicherheitsrat und der Länderarbeitsgruppe Cybersicherheit

Berichterstattung:	Hessen
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 40
	Beschlussvorschlag HE vom 07.10.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 8

Beschluss:

Die IMK nimmt den „Bericht aus dem Nationalen Cyber-Sicherheitsrat (NCSR) und der Länderarbeitsgruppe Cybersicherheit" (Stand: 12.10.21) *(nicht freigegeben)* zur Kenntnis und bittet Hessen, zur Frühjahrssitzung 2022 erneut zu berichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 65: Bessere Koordinierung und Abstimmung von Maßnahmen von Bund und Ländern im Bereich IT-Sicherheit

Berichterstattung:	Hessen
Hinweise:	IMK vom 28. bis 30.11.18 zu TOP 57
	IMK vom 16. bis 18.06.21 zu TOP 41
	Beschlussvorschlag HE vom 07.10.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 8.2/1

Beschluss:

1. Die IMK nimmt den „Sachstandsbericht: Konzept zur künftigen Koordinierung der Maßnahmen von Bund und Ländern im Bereich Cybersicherheit“ (Stand: 12.10.21) *(nicht freigegeben)* zur Kenntnis:

2. Sie beauftragt die LAG Cybersicherheit, die Umsetzung weiter zu begleiten und in regelmäßigen Abständen darüber zu berichten.

TOP 66: Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge

Berichterstattung:	Hessen
Hinweise:	IMK vom 28. bis 30.11.18 zu TOP 56
	IMK vom 12. bis 14.06.19 zu TOP 49
	Beschlussvorschlag HE vom 07.10.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 8.3

Beschluss:

1. Die IMK nimmt den vorliegenden „Sachstandsbericht: Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge (IoT)“ (Stand: 12.10.21) *(nicht freigegeben)* zur Kenntnis.

2. Die IMK bittet den Bund bis zur Frühjahrstagung 2022 zu berichten, welche Maßnahmen im Zusammenhang mit dem Internet of Things / Internet der Dinge (IoT) umgesetzt worden sind.

TOP 67: Bericht aus dem IT-Planungsrat

Berichterstattung:	Niedersachsen
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 39
	Beschlussvorschlag NI vom 19.10.21
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	V E 4

Beschluss:

Die IMK nimmt den „Bericht zum IT-Planungsrat“ *(freigegeben)* des Ansprechpartners der IMK über die Sitzungen des IT-Planungsrats am 23.06. und 29.10.21 zur Kenntnis.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 68: Bericht des Ländervertreters im JI-Rat der EU

Berichterstattung:	Hessen
Hinweise:	IMK am 10.12.20 zu TOP 43
	IMK vom 16. bis 18.06.21 zu TOP 45
	Beschlussvorschlag HE vom 08.10.21
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	I F 1

Beschluss:

Die IMK nimmt den „Bericht des Beauftragten des Bundesrates in Ratstagungen der Europäischen Union für den Rat Justiz und Inneres (JI-Rat), Bereich Inneres“ (Stand: 29.10.21) *(freigegeben)* zur Kenntnis.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 69: Beirat der Stiftung Datenschutz;

Vorschlag an die IMK für die Benennung eines neuen Mitglieds

Berichterstattung:	Baden-Württemberg
Hinweise:	IMK vom 28. bis 30.11.18 zu TOP 59
	AK I am 30.09./01.10.21 zu TOP 12
Veröffentlichung:	Freigabe Beschluss
Az.:	V B 2

Beschluss:

1. Die IMK schlägt vor, Herrn Dr. Joachim Wilkens (Sachsen-Anhalt) gemäß § 11 Absatz 2 Satz 1 Buchstabe b und Satz 2 der Satzung der Stiftung Datenschutz für drei Jahre als Mitglied des Beirats der Stiftung zu benennen.

2. Sie bittet das BMI, den Verwaltungsrat der Stiftung über diesen Beschluss zu unterrichten.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 72: Starkregen- und Flutereignisse im Juli 2021

Berichterstattung:	Rheinland-Pfalz / Nordrhein-Westfalen / Sachsen / Bayern
Hinweis:	Beschlussvorschlag RP, NW, SN und BY vom 28.10.21
Veröffentlichung:	Freigabe Beschluss
Az.:	X D 2

Beschluss:

1. Die IMK spricht allen Betroffenen der Starkregen- und Flutereignisse ihr Mitgefühl aus. Zahlreiche Tote sind zu beklagen und viele Menschen haben ihr Obdach und ihre Habe verloren.

2. Vor diesem Hintergrund dankt sie allen Hilfsorganisationen, Katastrophenschutzeinheiten, Feuerwehreinheiten, Unternehmen und Privatleuten, die bei der Bewältigung dieser Katastrophen mitgewirkt haben und dies weiter tun.

3. Die IMK dankt auch der Bundesregierung und insbesondere der Bundespolizei, dem THW, der Bundeswehr und dem BBK für die Unterstützung.

4. Sie dankt für die große gelebte Solidarität zwischen dem Bund und den Ländern, die die Unterstützung durch viele Helferinnen und Helfer sowie die schnelle Schaffung des Hilfefonds mit 30 Milliarden Euro ermöglicht haben.

noch TOP 72

5. Die IMK beauftragt den AK V, auf Basis der Aufarbeitung in den Ländern Erkenntnisse aus den Starkregen- und Flutereignissen zu sammeln und Handlungsempfehlungen für den zukünftigen Umgang mit großflächigen Schadensereignissen zu erarbeiten.

6. Sie bittet ihren Vorsitzenden, die UMK über diesen Beschluss zu informieren.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 73: Asyl- und aufenthaltsrechtliche Folgen für bereits im Bundesgebiet aufhältige afghanische Staatsangehörige

Berichterstattung:	Niedersachsen / Hamburg
Hinweise:	Beschlussvorschlag NI vom 09.11.21
	alternativer Beschlussvorschlag NW vom 11.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI G 6.12

Beschluss:

1. Die IMK begrüßt, dass die Bundesregierung in einem einheitlichen und zentral durchgeführten Verfahren die notwendigen Voraussetzungen für die koordinierte Aufnahme von Ortskräften, ihren Familien und besonders gefährdeten Menschen geschaffen hat.

2. Sie stellt fest, dass Bund und Länder jeweils ihren Teil der Verantwortung für die Ausreise, die Aufnahme und Versorgung der auf diesem Wege ausgereisten afghanischen Staatsangehörigen übernommen haben und weiterhin übernehmen werden.

3. Die IMK fordert die Bundesregierung auf, vor dem Hintergrund der derzeit realistisch nicht bestehenden Rückführungsperspektiven nach Afghanistan über den Umgang mit Personen im laufenden Asylverfahren und von Personen mit Duldungsstatus zeitnah zu entscheiden.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 74: Effiziente Durchsetzung der Meldepflichten nach dem Netzwerkdurchsetzungsgesetz (NetzDG)

Berichterstattung:	Niedersachsen
Hinweis:	Beschlussvorschlag NI vom 09.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI D 4.3

Beschluss:

1. Die IMK stellt fest, dass die in § 3a NetzDG eingeführten und am 01.02.22 in Kraft tretenden Meldepflichten für Anbieter sozialer Netzwerke über bestimmte rechtswidrige oder strafbare Inhalte einen wichtigen Beitrag zur besseren Bekämpfung von Rechtsextremismus und Hasskriminalität leisten.

2. Sie bittet das BMI darauf hinzuwirken, dass die Vorbereitungen für die technische und organisatorische Umsetzung des Meldesystems trotz der von Facebook und Google eingereichten gerichtlichen Eilanträge weiter vorangetrieben werden, damit nach Abschluss der Eilverfahren ohne weitere Verzögerungen Meldungen der sozialen Netzwerke entgegengenommen und weiterverarbeitet werden können.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 75: Vereinbarung zwischen den Ländern zur Finanzierung und Besetzung der Stellen beim Gemeinsamen Kompetenzzentrum Bevölkerungsschutz des Bundes und der Länder

Berichterstattung:	Baden-Württemberg
Hinweis:	UB AK V vom 10.11.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe des Entwurfs der Verwaltungsvereinbarung
Az.:	X A 3.2

Beschluss:

1. Die IMK nimmt den Entwurf der Vereinbarung zwischen den Ländern zur Finanzierung und Besetzung der Stellen beim Gemeinsamen Kompetenzzentrum Bevölkerungsschutz des Bundes und der Länder (GeKoB) *(nicht freigegeben)* zur Kenntnis.

2. Sie bittet die Länder, auf Grundlage dieses Entwurfs die Finanzierung für ihren jeweiligen Bereich sicherzustellen.

3. Die IMK bittet ihren Vorsitzenden, den Entwurf der Vereinbarung gemäß dem Beschluss der Konferenz der Regierungschefinnen und Regierungschefs der Länder vom 14.03.13 der Finanzministerkonferenz mit der Bitte um Zustimmung zuzuleiten.

4. Sie beauftragt den AK V, in der IMK-Frühjahrssitzung 2022 zu berichten und die Vereinbarung zur abschließenden Beratung und Unterzeichnung vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 76: 2. Fortschreibung des Sonderlagebildes "Gefahren- und Risikopotential insbesondere durch Extremisten und fremde Dienste"

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 54
	UB AK IV vom 11.11.21
	alternativer Beschlussvorschlag TH vom 30.11.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	IX H 1.3/10

Beschluss:

1. Die IMK nimmt die zweite Fortschreibung des Berichtes „Gezielte Falschmeldungen, Verschwörungstheorien und Desinformationskampagnen - Sonderlagebild Gefahren- und Risikopotential insbesondere durch Extremisten und fremde Dienste -VS-NfD-“ (Stand: 15.10.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie erneuert ihren Beschluss vom 18.06.21 zu TOP 54 zur Fortschreibung des Sonderlagebildes "Gefahren- und Risikopotential insbesondere durch Extremisten und fremde Dienste" und hält es weiter für erforderlich, die Beobachtung von demokratiefeindlichen und sicherheitsgefährdenden Bestrebungen zur Delegitimierung des Staates durch die Verfassungsschutzbehörden von Bund und Ländern zu intensivieren.

3. Die IMK zeigt sich in Anbetracht der wieder verschärften Pandemieschutzmaßnahmen sehr besorgt, dass bei dem verstärkten Protestgeschehen Demonstrationsteilnehmer regelmäßig die geltenden Vorschriften nicht beachten und häufig keine inhaltliche oder räumliche Abgrenzung zu Rechtsextremisten oder „Reichsbürgern“ aufgebaut wird.

4. Sie sieht die Gefahr, dass insbesondere die rechtsextremistische und Querdenkerszene weiter versuchen, die in Teilen der Bevölkerung vorhandene Skepsis angesichts der Einschränkungen des öffentlichen Lebens für ihre Zwecke zu instrumentalisieren und ihren Einfluss und ihren Wirkungsbereich zu vergrößern.

5. Die IMK unterstreicht, dass es neben einer konsequenten Durchsetzung der geltenden Pandemieschutzmaßnahmen weiterhin eine gesamtgesellschaftliche Aufgabe ist und Anstrengungen aller erfordert, gezielten Falschmeldungen, Verschwörungstheorien und Desinformationskampagnen entgegenzutreten.

6. Sie beauftragt den AK IV unter Beteiligung des AK II, das Sonderlagebild fortzuschreiben und zur Frühjahrskonferenz 2022 vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 77: Lagebericht „Politisch motivierte Straftaten gegen Amts- und/oder Mandatsträger; Berichtszeitraum 2019/2020“

Berichterstattung:	BMI
Hinweise:	IMK vom 16. bis 18.06.21 zu TOP 4
	UB AK II vom 12.11.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 10.1

Beschluss:

1. Die IMK nimmt den Lagebericht „Politisch motivierte Straftaten gegen Amts- und/oder Mandatsträger; Berichtszeitraum 2019/2020 -VS-NfD-“ (Stand: 25.10.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie stellt fest, dass die gegen Amts- und/oder Mandatsträger gerichteten Straftaten im Jahr 2020 im Vergleich zum Vorjahr stark gestiegen sind und das Tatmittel Internet hier einen Schwerpunkt darstellt. Den phänomenologischen Schwerpunkt bilden Straftaten aus den Bereichen der PMK -rechts-, PMK - links- sowie PMK -nicht zuzuordnen-.

3. Die IMK begrüßt die Ausarbeitung von Handlungsempfehlungen auf Grundlage der Erfahrungen des Bundes und der Länder und bittet die Länder, die Anwendung im jeweiligen Zuständigkeitsbereich individuell zu prüfen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 79: **Verbesserung der Erkenntnislage zu Rückkehrern aus dem sogenannten Islamischen Staat**

Projekt zur Untersuchung der (De-)Radikalisierungsverläufe von rückgekehrten Personen, die ursprünglich aus Deutschland nach Syrien bzw. Irak ausgereist sind, um sich dort dem sogenannten Islamischen Staat (IS) anzuschließen

Berichterstattung:	BMI
Hinweise:	IMK vom 28. bis 30.11.18 zu TOP 24
	UB AK II und AK IV vom 15.11.21
Veröffentlichung:	Freigabe Beschluss, keine Freigabe Bericht
Az.:	VI D 4.4/9d

Beschluss:

1. Die IMK nimmt den Bericht „Verbesserung der Erkenntnislage zu Rückkehrern aus dem sogenannten Islamischen Staat - Projekt zur Untersuchung der (De-)Radikalisierungsverläufe von rückgekehrten Personen, die ursprünglich aus Deutschland nach Syrien bzw. Irak ausgereist sind, um sich dort dem sogenannten Islamischen Staat (IS) anzuschließen; Abschlussbericht 2021 - Relevante Befunde zu den Stichtagen 31.12.19 und 01.06.21 -VS-NfD-“ (Stand: 01.11.21) *(nicht freigegeben)* zur Kenntnis.

2. Sie dankt der Forschungs- und Beratungsstelle Terrorismus und Extremismus (FTE) des BKA, dem Hessischen Informations- und Kompetenzzentrum gegen Extremismus (HKE) und dem BfV für die Erstellung der Studie. Sie dankt der Abteilung TE des BKA sowie den beteiligten Verfassungsschutz- und Polizeibehörden in den Ländern für ihre Mitwirkung.

3. Die IMK begrüßt die detaillierte Darstellung der biografischen Daten und von Radikalisierungsfaktoren sowie die Betrachtung möglicher Gefährdungspotentiale und stabilisierender Faktoren.

4. Sie bittet die FTE, die Studie zur IMK-Herbstsitzung 2022, ggf. mit einer Erweiterung auf weitere jihadistische Schauplätze, zu aktualisieren und einen entsprechenden Bericht vorzulegen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 80: Strafverschärfung für Schleusertätigkeit

Berichterstattung:	Hessen / Brandenburg / Sachsen
Hinweis:	Beschlussvorschlag HE / BB / SN vom 15.11.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VI D 2.2/4

Beschluss:

1. Die IMK stellt fest, dass Deutschland nach wie vor ein Hauptzielland illegaler Migration in Europa ist. Trotz pandemiebedingter Einschränkungen wurden auch im Jahr 2020 über 40.000 unerlaubte Einreisen nach Deutschland festgestellt. Der Anteil geschleuster Personen nahm dabei auf 15 % deutlich zu.

2. Sie verweist darauf, dass im zweiten Halbjahr 2020 ein signifikanter Anstieg an (Behältnis-)Schleusungen zu verzeichnen war, die oftmals mit hohen Gefahren für Leib oder Leben der geschleusten Personen einhergehen.

3. Die IMK bittet das BMI, in Abstimmung mit dem BMJV und dem AA aber auch im Rahmen internationaler Zusammenarbeit auf geeignete Maßnahmen zur Eindämmung der Schleuserkriminalität hinzuwirken.

4. Ferner spricht sie sich für eine Erhöhung der Mindeststrafen für das Einschleusen von Menschen in §§ 96, 97 AufenthG aus.

5. Die IMK bitten ihren Vorsitzenden, die JuMiKo über diesen Beschluss in Kenntnis zu setzen.

Sammlung

der zur Veröffentlichung freigegebenen Beschlüsse

der Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder
am 03.12.20

TOP 82: Auswirkungen einer veränderten Verkehrsplanung und Verkehrsraumgestaltung auf das Erreichen von Einsatzorten durch Polizei und Feuerwehr

Berichterstattung:	Hamburg
Hinweis:	Beschlussvorschlag HH vom 02.12.21
Veröffentlichung:	Freigabe Beschluss
Az.:	VII C 1

Beschluss:

1. Die IMK weist darauf hin, dass Polizei, Feuerwehr und andere Einsatzorganisationen so schnell wie möglich an Einsatzorte gelangen müssen, um dort Gefahrenzustände wirksam zu bekämpfen und Menschen und Sachwerte zu schützen. Die im Zusammenhang mit der Mobilitätswende, dem Klima- und Lärmschutz sowie von veränderten städtebaulichen Planungsansätzen erfolgenden Veränderungen des Straßenraumes haben Auswirkungen auf das schnelle Erreichen von Einsatzorten durch Polizei, Feuerwehr und andere Einsatzorganisationen. Insbesondere Herabsetzungen der Geschwindigkeiten, Umgestaltungen mit veränderten Flächenzuweisungen und Verkehrsberuhigungsmaßnahmen wirken auch auf die Anfahrt von Einsatzkräften.

2. Die IMK beauftragt den AK II unter Beteiligung des AK V, die Auswirkungen auf Polizei und Feuerwehr aufzubereiten und geeignete Ansätze, um die schnelle Erreichbarkeit von Einsatzorten weiter zu gewährleisten, aufzuzeigen und der IMK zur Frühjahrsitzung 2022 zu berichten.

3. Die IMK bittet ihren Vorsitzenden, diesen Beschluss der VMK und der BMK zur Kenntnis zu geben.

Bundesministerium
des Innern, für Bau
und Heimat

Bundesministerium des Innern, für Bau und Heimat, 11014 Berlin

Inspekteur der Bereitschafts-
polizeien der Länder
Andreas Backhoff

Bundesallee 216 - 218
10719 Berlin
Postanschrift
11014 Berlin
Tel +49 30 18 681-14658
Fax +49 30 18 681-14348

IBP@bmi.bund.de
www.bmi.bund.de

IBP-42103/7#20
Berlin, 5. August 2021

Bericht zum Sachstand des IMK-Auftrags vom 25.03.2019 anlässlich der Vorbereitung der UEFA EURO 2024

Bezug: 1) Schreiben IMK-Vorsitz vom 08.03.2019
2) Umlaufbeschluss der Innenministerkonferenz vom 25.03.2019

Mit dem im Bezug genannten Beschluss im Umlaufverfahren vom 25.03.2019 hat die IMK das BMI gebeten, unter Beteiligung des DFB und der im Nationalen Ausschuss Sport und Sicherheit vertretenen Stellen einen Bund-Länder-Ausschuss mit dem Auftrag einzurichten, ein Sicherheitskonzept für die Fußballeuropameisterschaft 2024 zu erstellen.

Nach Auswertung und Analyse der unterschiedlichen Turnieranforderungen und Aufgabenschwerpunkte für die Durchführung der FIFA Fußball-Weltmeisterschaft 2006 und der anstehenden UEFA Fußball-Europameisterschaft 2024 ist das BMI zu dem Ergebnis gekommen, dass es einer Modifizierung des 2006 eingesetzten Bund-Länder-Ausschusses (BLA) bedarf.

Um den Herausforderungen für die UEFA EURO 2024 gerecht zu werden, bedarf es einer ganzheitlichen Befassung sicherheitsrelevanter, politischer und gesamtgesellschaftlicher Themenfelder. Zur Bewältigung dieser Aufgaben beabsichtigt das BMI einen Nationalen Koordinierungsausschuss (NKA) einzurichten. Der NKA wird neben der Zusammenführung von Maßnahmen ein Nationales Konzept erstellen, in dem u.a. auch die Aspekte des Nationalen Sicherheitskonzeptes aufgehen werden.

Zustell- und Lieferanschrift:
Verkehrsanbindung: U-Bahnhof Spichernstraße

Bundesministerium
des Innern, für Bau
und Heimat

Berlin, den 9. November 2021

Gemeinsamer Bericht des AK V / BMI
für die 215. IMK vom 1. bis 3. Dezember 2021 in Stuttgart
zum Sachstand der länderoffenen Bund-Länder-Kommission „Stärkung des Bevölkerungsschutzes“

1 Beschlusslage und Aufgabenstellung

Auf der 214. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder (weiter: IMK) vom 16. bis 18.06.2021 in Rust wurde unter TOP 33 beschlossen, dass die vom Bund initiierte Entwicklung eines Kompetenzzentrums zu einer gemeinsamen Einrichtung von Bund und Ländern gleichberechtigt von Beginn an gemeinsam gestaltet wird. Eine solche neue Kooperationsplattform soll von den originären Aufgabenträgern im Bevölkerungsschutz und Krisenmanagement, also von Bund und Ländern, partnerschaftlich getragen werden.

Zu diesem Zweck wurde das BMI gebeten, in Abstimmung mit dem Arbeitskreis V, Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung, der IMK (weiter: AK V), eine länderoffene Bund-Länder-Kommission "Stärkung des Bevölkerungsschutzes" (weiter: Kommission) einzurichten, eine gemeinsame Leitung zu bestimmen und themenbezogen die Fachministerkonferenzen einzubeziehen.

Die Kommission hat laut Beschluss der IMK zunächst den Auftrag, bis zum Jahresende ein Gemeinsames Kompetenzzentrum Bevölkerungsschutz (weiter: Kompetenzzentrum) als gemeinsame Bund-Länder-Einrichtung auf Basis einer Vereinbarung zu entwickeln, Vorschläge zu Aufgaben, Rolle und Ausstattung vorzulegen und die notwendigen rechtlichen und ressourcenbezogenen Erfordernisse zu beschreiben. Weitere Themen sollen im Einvernehmen später zum Gegenstand der Kommission gemacht werden.

Die IMK hat den AK V ferner beauftragt, der IMK über den Fortgang der Arbeiten zur Reform des Bevölkerungsschutzes bis zur Frühjahrskonferenz 2022 zu berichten.

Vorliegender Sachstandsbericht gibt einen Überblick über die bisherigen Tätigkeiten der Kommission sowie über die bisherigen Ergebnisse.

2 Arbeit der länderoffenen Bund-Länder-Kommission „Stärkung des Bevölkerungsschutzes“

Die Kommission, zu deren Mitgliedern die zuständigen Abteilungsleitungen der Innenressorts von Bund und Ländern sowie der Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (weiter: BBK) gehören, hat ihre Arbeit in der konstituierenden Sitzung am 5. August 2021 auf Basis einer gemeinsam verabschiedeten Geschäftsordnung zur Entwicklung eines Kompetenzzentrums aufgenommen. Die Kommission wird von einem gemeinsamen Vorsitz von Bund (Abteilungsleitung BMI Nationales Krisenmanagement) und Ländern (Vorsitz AK V) geleitet.

Die Arbeit der Kommission erfolgte in bisher drei Sitzungen konstruktiv und auf das gemeinsame Ziel der Stärkung des Bevölkerungsschutzes ausgerichtet.

Als Ergebnis konnte der Entwurf einer Verwaltungsvereinbarung für ein Kompetenzzentrum konsentiert werden. Der Entwurf wird der IMK auf deren 215. Sitzung zur Beschlussfassung vorgelegt werden.

Die Abteilungsleitungen der Länder haben zur Vorlage der 215. IMK-Sitzung den Entwurf einer Vereinbarung zwischen Ländern zur Finanzierung der Stellen für die von den Ländern zu entsendenden Verbindungspersonen erarbeitet.

3 Verwaltungsvereinbarung von Bund und Ländern

Die Verwaltungsvereinbarung regelt den Rahmen für die Errichtung eines Kompetenzzentrums und die partnerschaftliche Arbeit zwischen Bund und Länder. Erforderliche Regelungen zu den Detailfragen werden als Ergänzung der Verwaltungsvereinbarung in der Aufgabenbeschreibung und einer noch abzustimmenden Geschäftsordnung des Kompetenzzentrums vereinbart.

Die Verwaltungsvereinbarung gibt Ziele vor und regelt grundlegende Aspekte der Zusammenarbeit im Kompetenzzentrum:
Mit der Errichtung und Etablierung eines dauerhaften und strukturiert organisierten Kompetenzzentrums für den Bevölkerungsschutz sowie für das ressortübergreifende Risiko- und Krisenmanagement sollen bevölkerungsschutzrelevante Themen unter Wahrung der Zuständigkeiten des Bundes im Zivilschutz und der Länder im Katastrophenschutz konzentriert und der Informationsstand aller Beteiligten für eine bessere Krisenvorsorge und Krisenbewältigung optimiert werden.

Getragen wird das Kompetenzzentrum von den für den Bevölkerungsschutz originär zuständigen Behörden des Bundes und der Länder. Sie bilden den Kern in einer auf

Dauer angelegten arbeitstäglichen Zusammenarbeit von Vertreterinnen und Vertretern des Bundes sowie der Länder. Bund und Länder entsenden mindestens je fünf Verbindungspersonen. Jedem Partner steht es offen, weitere Verbindungspersonen zu entsenden. Die Einbindung weiterer Akteure im Bevölkerungsschutz erfolgt auf Basis der Regelungen der Verwaltungsvereinbarung, welche eine beratende Beteiligung vorsieht.

Die Rolle des Kompetenzzentrums wird durch ihre Organisation als Kooperationsplattform ohne Behördeneigenschaft geprägt. Die Aufgaben werden in der Verwaltungsvereinbarung sowohl mit Blick auf die Alltagsorganisation als auch auf die Krisenorganisation skizziert und in einer Anlage konkretisiert.

Die strategische Steuerung des Kompetenzzentrums erfolgt durch einen gemeinsamen Lenkungskreis von Bund und Ländern, wohingegen die administrativ/operative Steuerung durch eine Leitung erfolgt.

3.1 Aufgaben des Kompetenzzentrums

Die Aufgaben des Kompetenzzentrums sind weitestgehend abgestimmt und werden, wie oben genannt, in einer ergänzenden Anlage zur Verwaltungsvereinbarung konkretisiert.

3.2 Finanzierung des Kompetenzzentrums

Die Punkte der Finanzierung des Kompetenzzentrums werden zum einen bilateral zwischen Bund und Ländern erörtert und zum anderen multilateral zwischen den Ländern selbst. Die Verwaltungsvereinbarung wird hierzu im § 7 noch ergänzt. Die konkreten Ergebnisse werden spätestens zur Frühjahrs IMK 2022 vorliegen.

3.3 Pilot Gemeinsames Lagebild Bevölkerungsschutz

In der AK V Sitzung am 21./22. April 2021 wurde unter TOP 23 vorgeschlagen, mit der Erstellung eines „Gemeinsamen Lagebildes Bevölkerungsschutz“ als Pilotvorhaben für das Kompetenzzentrum zu beginnen.
Die technische Unterstützung der Arbeit im Kompetenzzentrum, insbesondere für das Gemeinsame Lagebild Bevölkerungsschutz, soll IT-gestützt erfolgen. Für die Umsetzung stehen Bund und Länder gemeinsam mit einem Software-Unternehmen im Austausch. Der Bund stellt die für die Erarbeitung einer prototypischen Software-Lösung erforderlichen Finanzierungsmittel zur Verfügung.

4. Ausblick

Die Kommission wird dem Auftrag der IMK gemäß die noch ausstehenden Punkte zur Entwicklung des Kompetenzzentrums in den kommenden Wochen weiter ausarbeiten. Sie sind weitestgehend abgeschlossen. Die inhaltlichen Arbeiten an dem Pilotvorhaben „Gemeinsames Lagebild Bevölkerungsschutz“ werden auf Arbeitsebene weitergeführt. Dazu gehört insbesondere die Einbindung der nichtbehördlichen Akteure sowie den weiteren fachlichen Kompetenzen in den Bereichen des Bevölkerungsschutzes.

Bund und Länder sind sich einig, dass in Ansehnung der geänderten Gefahrenlagen eine ebenen- und ressortübergreifende Zusammenarbeit im fachlichen und politischen Krisenmanagement zur Fortentwicklung des Bevölkerungsschutzes partnerschaftlich weitergeführt und vorangetrieben werden soll.

Bundesamt
für Migration
und Flüchtlinge

Bundesamt für Migration und Flüchtlinge, 90343 Nürnberg

Bundesministerium des Innern, für Bau und
Heimat
Projektgruppe AnkER

Frankenstraße 210
90461 Nürnberg

Postanschrift:
90343 Nürnberg

Tel. +49 911 943-
Fax +49 911 943-

per Mail

Berichtsstand zu IT-Pilotierung "Föderale Blockchain-Infrastruktur Asyl (FLORA) - Assistenzsystem zur Behördenvernetzung"
Ihr Zeichen: PG AnkER-12010/1#38

Nürnberg, 28.10.2021

Sehr geehrte Damen und Herren,

im Folgenden finden Sie einen aktuellen Sachstandsbericht zum BAMF-Projekt FLORA bezugnehmend auf Ihre E-Mail vom 18.10.2021. Dieser umfasst den erfolgreichen Abschluss der Pilotierung des FLORA-Teilvorhabens „Assistenzsystem für die AnkER-Einrichtung Dresden" sowie das weitere geplante Vorgehen. Zudem wurde die Konzeptionierung im Rahmen des FLORA-Teilvorhabens EBSI aufgenommen.

Blockchain-basiertes Assistenzsystem für Asylverfahren in der AnkER-Einrichtung Dresden
Der Fokus des FLORA-Teilvorhabens „Assistenzsystem für die AnkER-Einrichtung Dresden" lag in der Zeit seit dem letzten BMI-Bericht im März 2021 auf der Pilotierung der Blockchain-basierten IT-Lösung im beschränkten Wirkbetrieb. Kern dieses Pilotbetriebs ist die Erprobung und Evaluierung des Assistenzsystems hinsichtlich Praxistauglichkeit und Prozessverbesserungspotenzial einer Blockchain-basierten IT-Anwendung.

Durch die umfassende Evaluierung im Pilotbetrieb konnten signifikante positive Veränderungen festgestellt werden. Besonders hervorzuheben ist die bessere Verfügbarkeit und Transparenz von verfahrensrelevanten Informationen, sodass manuelle Doppelarbeiten und Kommunikationsaufwände erheblich reduziert werden konnten. Die insbesondere durch das Wegfallen verschiedener Listen gewonnene Zeit kann wiederum zur Steigerung der Qualität der Arbeitsergebnisse genutzt werden. Ferner ist der Prozess nun deutlich weniger fehleranfällig, wodurch sich die Abläufe nicht

nur vereinfachen, sondern darüber hinaus auch beschleunigen lassen. Zuletzt unterstützt das Blockchain-basierte Assistenzsystem eine noch konsequentere Einhaltung von Datenschutzbestimmungen und setzt einen Startpunkt für eine neuartige Zusammenarbeit auf behördeninterner und behördenübergreifender Ebene.

Ausbau der Föderalen Blockchain-Infrastruktur Asyl (FLORA)
Auf Basis der erfolgreichen Pilotierung sind nun weitere Ausbaustufen geplant. Im ersten Ausbauschritt ist eine Erweiterung des FLORA-Assistenzsystems im bereits realisierten und evaluierten fachlichen Umfang auf zusätzliche Standorte und Behörden vorgesehen. Dies umfasst zunächst eine Ausweitung auf die sächsischen funktionsgleichen Einrichtungen Chemnitz und Leipzig. Des Weiteren wurden bereits vertiefende Gespräche mit dem Ministerium für Kinder, Familie, Flüchtlinge und Integration des Landes Nordrhein-Westfalen (MKFFI) bezüglich einer Beteiligung am Projekt und der späteren Nutzung der Blockchain-Lösung aufgenommen. Auch mit dem Regierungspräsidium Karlsruhe (RPK) sowie dem Ministerium der Justiz und für Migration des Landes Baden-Württemberg (MJ BW) fanden schon Abstimmungsgespräche statt. Darüber hinaus haben die Länder Bayern und Brandenburg Interesse an der Teilnahme an weiteren Ausbaustufen geäußert.

Zusätzlich zu den angestrebten Erweiterungen auf weitere Standorte und Behörden wird auch eine Erweiterung auf fachlicher Ebene durch die Hinzunahme weiterer Anwendungsbereiche beabsichtigt.

Unterstützung des Dublin Verfahrens durch die Europäische Blockchain Services Infrastructure (EBSI)
Wie im letzten Bericht im März 2021 erläutert, hat das Bundesamt den Vorsitz einer Arbeitsgruppe übernommen, welche die Einsatzmöglichkeiten der European Blockchain Service Infrastruktur für das Dublin-Verfahren unter Spiegelung des nationalen Use Cases ausloten und erproben soll. Die Arbeitsgruppe hat mit der Konzeptionierung des Anwendungsfalls begonnen. Das Bundesamt befindet sich aktuell mit der französischen Dublin-Einheit in der Abstimmung hinsichtlich einer prototypischen Umsetzung und Erprobung, die mittels Testdaten erfolgen soll.

Für Rückfragen stehe ich Ihnen jederzeit zur Verfügung.

Mit freundlichen Grüßen

i.A.
Antje Kiss

Bundesministerium
des Innern, für Bau
und Heimat

Berlin, den 10.09.2021

Abschlussbericht des BMI

zu TOP 29 Ziffer 2 und 3

der 211. Innenministerkonferenz

vom 4. bis 6. Dezember 2019 in Lübeck

zur

„Umsetzung des Zweiten Gesetzes

zur besseren Durchsetzung der Ausreisepflicht“

Inhaltsverzeichnis

A. Einleitung

Das Zweite Gesetz zur besseren Durchsetzung der Ausreisepflicht (BGBl. I 2019, S. 1294, im Folgenden GRG) ist am 21.08.2019 in Kraft getreten.

Die IMK hat auf ihrer 211. Sitzung vom 04. bis 06.12.19 in Lübeck unter TOP 29 „Verbesserung der Durchsetzung von Ausweisungen und Abschiebungen bei straffälligen Ausländern / Flüchtlingen und Gefährdern“, Ziffer 2, beschlossen, das BMI zu bitten, ihr über den AK I bis zur Herbstsitzung 2020 einen Zwischenbericht und bis zur Herbstsitzung 2021 einen Abschlussbericht über die Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht unter Einbeziehung der AG IRM vorzulegen.

Den erbetenen Zwischenbericht hat das Bundesministerium des Innern, für Bau und Heimat zur Herbstsitzung der IMK in Weimar vom 09. bis zum 11. Dezember 2020 vorgelegt. Dieser befasst sich vorwiegend mit der geplanten Methodik des Erfahrungsberichts[1]. Hiermit legt das Bundesministerium des Innern, für Bau und Heimat den Abschlussbericht über die Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht vor.

Der Abschlussbericht hat zum Ziel, zu überprüfen, ob die gesetzgeberischen Ziele der maßgeblichen Regelungskomplexe erreicht worden sind.

Maßstäbe für die Ermittlung der Zielerreichung sind:

- Effektivität, mithin ob und in welchem Umfang die ursprünglich angestrebten Ziele der Regelung erreicht worden sind,
- Akzeptanz der Regelungskomplexe durch die mit dem Vollzug befassten Anwenderinnen und Anwender,
- Praktikabilität, also die Frage, ob die gesetzlichen Regelungen in der Vollzugspraxis handhabbar bzw. gut umsetzbar sind.

Der vorliegende Bericht beschreibt zunächst die Methodik der Berichterstellung sowie die Ziele des Gesetzes (vgl. Kapitel B. und C.).

Daraufhin werden zusammenfassend die grundsätzlichen Bewertungen der Länder zum neuen Regelwerk dargestellt (Kapitel D.I.). Anschließend beleuchtet der Bericht die einzelnen Kernbereiche des GRG, indem sich an eine Darstellung der jeweiligen gesetzgeberischen Ziele die Zusammenfassung der Praxiserfahrungen, die wichtigsten Verbesserungsvorschläge der Länder sowie eine Analyse der Rechtsprechung zu den jeweiligen maßgeblichen Regelungsteilen anschließen (Kapitel D.II. ff.). In einer Anlage sind

[1] Vgl. Anlage 1.

sämtliche von den Ländern unterbreiteten Verbesserungsvorschläge tabellarisch zusammengefasst[2].

[2] Vgl. Anlage 3.

B. Methodik

Für die dem Bericht zugrundeliegenden Daten wurde ein Erhebungszeitraum ab Inkrafttreten des GRG bis einschließlich Mai 2021 gewählt.

Die Erhebung der für den Erfahrungsbericht erforderlichen Informationen und Daten wurde auf die zentralen Regelungsmechanismen des GRG fokussiert.

Diese umfassen die nachfolgenden gesetzlichen Kernbereiche:

I. die Neustrukturierung der Regelungen zum Einreise- und Aufenthaltsverbot in § 11 AufenthG
II. der neue Duldungstatbestand für Personen mit ungeklärter Identität
III. praktikablere Ausgestaltung der Sicherungshaft
IV. Neueinführung der Mitwirkungshaft
V. praktikablere Ausgestaltung des Ausreisegewahrsams
VI. temporäre Aufhebung des Trennungsgebots
VII. Erleichterung der Voraussetzungen für die Ausweisung von Straftätern
VIII. Schaffung eines bundesgesetzlichen „Mindeststandards“ für das Betreten und Durchsuchen von Wohnungen
IX. bessere Überwachungsmöglichkeiten für (nicht abschiebbare) Intensivstraftäter
X. Reduktion des Beteiligungserfordernisses der Staatsanwaltschaft bei Ausweisung/Abschiebung von Straftätern

Die Grundlage des Erfahrungsberichts bilden folgende Komponenten:

- Eine (qualitative) Datenerhebung in Form eines am 13.01.2021 an die Länder versandten Fragebogens[3]. Dieser sollte durch einen von den Ländern zu bestimmenden Expertenkreis aus den für das Aufenthaltsrecht und dessen Vollzug zuständigen Institutionen beantwortet werden. Mit diesen teilstandardisierten Fragen sollten so deren praktische Erfahrungen bei der Umsetzung der Regelungskomplexe des GRG erhoben werden.

- Eine Erhebung der begrenzt im AZR vorhandenen Daten, sofern diese nach einer Sichtung und entsprechenden Verwertbarkeit für den Erfahrungsbericht herangezogen und ausgewertet werden konnten.

[3] Vgl. Anlage 2.

- Eine Auswertung der über Rechercheportale zugänglichen Rechtsprechung sowie weiterer seitens der Länder übersandter Urteile/Beschlüsse zu den maßgeblichen Neuregelungen des GRG.

Dieses Vorgehen wurde nach entsprechender Prüfung durch das BMI und unter Beteiligung der AG IRM gewählt, da es ermöglichte, unterschiedliche Anwendungsphasen des Gesetzes zu berücksichtigen - unabhängig von den bei einer vorwiegend quantitativen Datenerhebung bestehenden Erhebungs- und Vergleichsschwierigkeiten.

Hierbei war vor allem relevant, dass zum einen die ersten Wochen nach dem Inkrafttreten des GRG als „Anlaufphase“ gewertet werden müssen, so dass für diesen Zeitraum nicht davon ausgegangen werden konnte, dass dort bereits erkenntnisbringende praktische Erfahrungen vorlagen.

Darüber hinaus hatte ab März 2020 die COVID19-Pandemie massiven Einfluss auf den gesamten Vollzug des Aufenthaltsrechts und insbesondere das Rückkehrgeschehen. Vor allem mangelnde Flugverbindungen, fehlende persönliche Vorsprachemöglichkeiten in den Auslandsvertretungen und infektiologische Restriktionen der Herkunftsländer haben sich unmittelbar auf den Vollzug der hier maßgeblichen Regelungen ausgewirkt. Bis zum heutigen Tage kann nicht von einer völligen Normalisierung gesprochen werden.

Innerhalb des maßgeblichen Zeitfensters zwischen Inkrafttreten des GRG am 21.08.2019 und der erbetenen Vorlage des Abschlussberichts bis zur Herbstsitzung 2021 der IMK war somit festzustellen, dass von einem „regulären“ Rückkehrgeschehen nur in der Zeit zwischen September 2019 und Februar 2020 – und auch in diesem Zeitraum nur reduziert – auszugehen war.

Das durchgeführte Konzept und der entwickelte Fragebogen wurden von der AG IRM im schriftlichen Umlaufverfahren gebilligt.

Durch die zuständigen Ministerien der Länder wurden dabei – je nach landeseigenem Verwaltungsaufbau und Behördengliederung und auch je nach gewählter Erhebungsmethode - in unterschiedlicher Art und Weise die jeweils für den Vollzug des Aufenthaltsrechts zuständigen Behörden (etwa die zuständigen Landesämter, Bezirksregierungen, Regierungspräsidien, Zentralen Ausländerbehörden sowie die Ausländerbehörden der Städte und Kreise) unterbeteiligt, so dass von einer weitreichenden Basis und hohen Erfahrungswerten ausgegangen werden kann.

Auf der Grundlage dieser gesammelten Erkenntnisse wurde dieser Abschlussbericht erstellt, der neben der Darstellung des Ist-Zustandes auch Korrektur- und Verbesserungsbedarf für die Zukunft skizzieren soll.

C. Ziel des Gesetzes

Überwölbendes Ziel des GRG ist es, die Vorgaben der Regelungen zur Aufenthaltsbeendigung bzw. zur Rückkehr, vor allem in Kapitel 5 des Aufenthaltsgesetzes, so zu gestalten, dass eine effektivere Durchsetzung der vollziehbaren Ausreisepflicht erfolgen kann. Die Zuführungsquote zu Rückführungsmaßnahmen soll deutlich gesteigert werden und einer Pflicht zur Ausreise muss die tatsächliche Ausreise so schnell wie möglich folgen (Bundestagsdrucksache 19/10047).

I. Situation vor dem GRG

Die Rechtspflicht, Deutschland zu verlassen, wurde und wird nach wie vor von einer hohen Zahl vollziehbar Ausreisepflichtiger nicht befolgt. Sofern die Betroffenen innerhalb der ihnen gesetzten Frist ihrer vollziehbaren Ausreisepflicht nicht freiwillig nachkommen, muss diese daher im Wege der Abschiebung durchgesetzt werden.

Entscheidend ist hierbei die Rückkehr derer, die unter keinem rechtlichen Gesichtspunkt ein Bleiberecht in Deutschland haben.

Viele Regelungen, die in den vergangenen Jahren neu gefasst wurden, hatten in der Praxis nicht immer den gewünschten Erfolg bewirkt. Der Gesetzentwurf bezweckte daher, die rechtlichen Voraussetzungen praktikabler auszugestalten. Ziel war es, die Zuführungsquote zu Rückführungsmaßnahmen deutlich zu erhöhen.

Die Richtlinie (EG) 2008/115 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger („Rückführungsrichtlinie“) verpflichtet in Artikel 8 Abs. 1 die Mitgliedstaaten, eine Rückkehrentscheidung mit allen erforderlichen Maßnahmen zu vollstrecken. Dieses Ziel war auf wirksame und verhältnismäßige Weise zu erreichen. Der unionsrechtliche Rahmen wird dabei durch die Rückführungsrichtlinie vorgegeben.

Als einer der häufigsten Gründe dafür, dass Rückführungen nicht stattfinden konnten, wurden vor allem das Untertauchen von Abzuschiebenden vor Rückführungsmaßnahmen sowie fehlende Pass- bzw. Passersatzpapiere der Abzuschiebenden identifiziert, die in erheblichem Maße auch auf die mangelnde Mitwirkung der Abzuschiebenden bei der Beschaffung dieser Dokumente zurückzuführen sind.

II. Einführung des GRG

Das GRG[4] hat die oben beschriebenen Problembereiche im Wesentlichen wie folgt adressiert:

- Die Neustrukturierung der Regelungen zum Einreise- und Aufenthaltsverbot in § 11 AufenthG.
- Die besondere Passbeschaffungspflicht (§ 60b Abs. 2 S. 1 AufenthG) mit dem neuen Duldungstatbestand für Personen mit ungeklärter Identität (§ 60b Abs. 1 AufenthG) sowie hieran anknüpfenden Sanktionen (§ 60b Abs. 5 AufenthG).
- Die praktikablere Ausgestaltung der Sicherungshaft durch widerlegliche Vermutungen und Indizien (§ 62 Abs. 3a und 3b AufenthG).
- Die Anpassung des Ausreisegewahrsams an die Erfordernisse des praktischen Vollzugs (§ 62b AufenthG).
- Die temporäre Aufhebung des Trennungsgebots (§ 62a Abs. 1 AufenthG).
- Die Absenkung des Ausweisungsschutzes für Straftäter (§ 53 Abs. 3 bis 3b AufenthG).
- Die Neufassung des Ausweisungsinteresses bei (Intensiv-)Straftätern (§ 54 Abs. 1 Nr. 1a, 1b, Abs. 2 Nr. 1 AufenthG).
- Die Schaffung eines bundesgesetzlichen „Mindeststandards“ für das Betreten und Durchsuchen von Wohnungen zur Ergreifung des Abzuschiebenden (§ 58 Abs. 5 – 10 AufenthG).
- Erweiterte Möglichkeiten, Auflagen bzw. Überwachungsmaßnahmen gegen (Intensiv-)Straftäter zu verhängen, die nicht abgeschoben werden können (§ 12 Abs. 2 S. 3, § 56 Abs. 3 Nr. 2, Abs. 4 S. 2 AufenthG).
- Die Reduktion des Beteiligungserfordernisses der Staatsanwaltschaft bei Ausweisung/Abschiebung von Straftätern (§ 72 Abs. 4 S. 4 AufenthG).

Darüber hinaus wurden durch das Bundesministerium des Innern, für Bau und Heimat Vorläufige Anwendungshinweise zu §§ 60b, 62 und 62b AufenthG erarbeitet, um die Anwender dieser Vorschriften bei deren Vollzug zu unterstützen[5].

[4] Der Gesetzentwurf mit Begründung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht ist unter folgendem Link abrufbar: https://dserver.bundestag.de/btd/19/100/1910047.pdf

[5] Darüber hinaus enthält das Zweite Gesetz zur besseren Durchsetzung der Ausreisepflicht unter anderem Regelungen, durch welche die Befugnisse zur Zuführung zur Abschiebung bundeseinheitlich festgelegt werden und die Aufgabe der Passersatzpapierbeschaffung im Wege der Amtshilfe von der Bundespolizei auf das Bundesamt für Migration und Flüchtlinge übertragen wird. Gleichzeitig wurde eine Verlängerung der Frist für die Regelüberprüfung der Asylentscheidungen des Jahres 2015 bis

D. Die einzelnen Kernbereiche und die Bewertung ihrer Umsetzung

I. Allgemeine Beurteilung

Die Neuregelungen haben sich nach – mit einer Ausnahme - übereinstimmender Auffassung der Länder (mit unterschiedlichen Nuancierungen) als ganz überwiegend praxistauglich erwiesen. Die Erfahrungswerte waren jedoch insgesamt durch die Pandemie eingeschränkt.

Unter dem Strich haben die meisten Länder angegeben, dass der tatsächliche Arbeitsaufwand für die Ausländerbehörden im Vergleich zur vorherigen Rechtslage im Wesentlichen gleichgeblieben sei. Bei differenzierter Betrachtung sind folgende Wertungen hervorzuheben:

Einerseits habe es viele Änderungen gegeben, die für Vereinfachungen und Erleichterungen in der praktischen Anwendung und Bearbeitung und für mehr Rechtssicherheit gesorgt haben, etwa durch die Schaffung klarerer Strukturen und Normen. Als Beispiele wurden hier etwa die Neustrukturierung der Kriterien für Fluchtgefahr in widerlegliche Vermutungen und konkrete Anhaltspunkte im Rahmen der Sicherungshaft (§ 62 Abs. 3a und Abs. 3b) und die Neufassung der Ausweisungsgründe für verurteilte Straftäter in § 54 Abs. 1 Nr. 1a, 1b und § 54 Abs. 2 Nr. 1 genannt. Gleichzeitig sei durch die vorgenommenen Neuregelungen an anderen Stellen ein erhöhter Aufwand entstanden. Dieser resultiert nach Angaben einiger Länder zum Teil aus mehr Anwendungsfällen aufgrund der abgesenkten Voraussetzungen, etwa bei den o.g. Ausweisungsvorschriften. Aber auch konkret die Anwendung des neuen § 60b AufenthG führt nach nahezu einhelliger Meinung der Länder zu erheblichem Mehraufwand, v.a. aufgrund der umfänglichen Belehrungs- und Anhörungspflichten sowie des erhöhten Aufkommens an Verwaltungsstreitigkeiten.

Dennoch wurde die Einführung der Duldung für Personen mit ungeklärter Identität von besonders vielen Ländern als besonders positive Neuregelung hervorgehoben, insbesondere aufgrund der klaren Beschreibung der zumutbaren Pflichten zur Identitätsklärung, der klar geregelten Rechtsfolgen und der damit verbundenen stärkeren Fokussierung auf den Personenkreis, der seine Ausreisehindernisse selbst zu vertreten hat. Einige Länder konnten durch die getroffene Neuregelung zumindest eine leichte Steigerung

---

zum 31. Dezember 2019, der Asylentscheidungen des Jahres 2016 bis zum 31. Dezember 2020 und der Asylentscheidungen des Jahres 2017
bis zum 31. Dezember 2021 zum Zwecke der Entlastung des Bundesamtes für Migration und Flüchtlinge eingeführt. Darüber hinaus wurde unter anderem die Möglichkeit geschaffen, dass die Verletzung von Mitwirkungspflichten während des Asylverfahrenszukünftig in größerem Umfang als bisher zu Leistungseinschränkungen nach dem Asylbewerberleistungsgesetz führen kann.

der Anzahl der Identitätsklärungen – etwa durch vermehrte Vorlagen von Passpapieren und eine erhöhte Bereitschaft zur Beantragung von Passpapieren - erreichen, während andere Länder dies nicht wahrnehmen konnten (vgl. im Einzelnen Kapitel D.III).

Auch die praxisgerechtere Ausgestaltung des Ausreisegewahrsams wurde von besonders vielen Ländern als positiv und als echte Verbesserung des Vollzugs von Rückführungen wahrgenommen, da hiermit höhere Zuführungsquoten realisiert werden können (vgl. im Einzelnen Kapitel D.V). Darüber hinaus haben viele Länder die Neustrukturierung der Haftgründe aufgrund der damit verbundenen Klarheit und Rechtssicherheit als Mehrwert gesehen (s.o. und im Einzelnen Kapitel D.IV).

Ebenso wurden die Erleichterungen bei der Ausweisung von Straftätern begrüßt. So habe sich insbesondere die Neufassung bzw. -gewichtung der Gründe für ein besonders schwerwiegendes bzw. schwerwiegendes Ausweisungsinteresse als in hohem Maße praxisrelevant erwiesen, zudem sei eine Vereinfachung bei der Anwendung der Tatbestände feststellbar. Für weitere Details wird hierzu auf Kapitel D.IX verwiesen.

Die bundesrechtliche Regelung nach § 58 Abs. 5 ff. AufenthG für das Betreten und Durchsuchen von Wohnungen zur Ergreifung des Abzuschiebenden wurde von einer Reihe von Ländern als besonders wichtig und notwendig hervorgehoben, unabhängig davon, ob deren Landesrecht hierzu bereits eigene Rechtsgrundlagen vorsah.

Insbesondere Teilaspekte bestimmter Neuregelungen, die von vielen Ländern – wie vorangestellt ersichtlich – per se positiv gesehen wurden, wurden negativ bewertet.

Dies betrifft vor allem Teilaspekte der Duldung für Personen mit ungeklärter Identität (§ 60b AufenthG) sowie der Betretens- und Durchsuchungsrechte (§ 58 Abs. 5 ff. AufenthG).

Als Hauptkritikpunkt bei § 60b AufenthG wurde seitens der Länder insbesondere die Komplexität der Vorschrift und der damit verbundene Verwaltungsaufwand benannt. Vereinzelt wurde der Kosten-Nutzen-Aufwand der Duldung für Personen mit ungeklärter Identität kritisch hinterfragt; wie oben erwähnt haben nicht alle Länder substanzielle Steigerungen bei der Beschaffung von Reisedokumenten wahrgenommen bzw. sehen, dass eine tatsächliche Durchsetzung der Ausreisepflicht am Ende doch nicht erreicht werden kann. Einzelne Länder wünschen sich generell eine integrationsfreundlichere Ausgestaltung der Duldungsvorschriften (vgl. im Einzelnen Kapitel D.III).

Die Neuregelungen zum Betreten und Durchsuchen von Wohnungen wurden mehrfach in Teilaspekten als wenig praktikabel kritisiert. Dies betrifft insbesondere die s.g. Nachtzeitregelung in § 58 Abs. 7 AufenthG, da nach S. 2 organisatorische Faktoren zur Begründung der Notwendigkeit einer Durchsuchung zur Nachtzeit nicht herangezogen werden können. Dies betreffe aber wichtige, z.T. durch die Ausländerbehörden nicht

beeinflussbare Aspekte wie Abflugzeit, einzukalkulierende Wegezeiten zum Flughafen und Dienstzeiten der Vollzugskräfte. Darüber hinaus kam es in Teilen zu Anwendungsschwierigkeiten aufgrund einer uneinheitlichen Rechtsprechung in den Ländern sowohl zum einschlägigen Rechtsweg als auch zur Auslegung des o.g. Organisationsbegriffs (vgl. im Einzelnen Kapitel D.IV).

Insgesamt wurden seitens der Länder auch nach Inkrafttreten des GRG eine Reihe weiterer Rechtsänderungen für erforderlich gehalten. Diese wurden zusammengefasst und finden sich als Anlage zu diesem Bericht. Die am häufigsten genannten Änderungswünsche sind jeweils in den Kapiteln D.I bis D.X. unter 1. (Ergebnisse der Länderbefragung) ausführlicher dargestellt.

II. Neustrukturierung der Regelungen zum Einreise- und Aufenthaltsverbot in § 11 AufenthG

1. Ziel

Durch die Neufassung des § 11 AufenthG wurde der Rechtsprechung des Bundesverwaltungsgerichts (Beschlüsse vom 13. Juli 2017 – 1 BR 3.17 und 1 A 10.17 –, sowie Urteil vom 21. August 2018 – 1 C 21.17) Rechnung getragen. Das Einreise- und Aufenthaltsverbot (EAV) tritt daher nicht mehr – wie zuvor - kraft Gesetzes ein, sondern stellt einen Verwaltungsakt dar.

In Abs. 5 S. 1 ist seit der Änderung für verurteilte Straftäter bzw. Gefährder anstatt der bisherigen Staffelung (5 Jahre, „Soll-Maximum“ 10 Jahre) eine einheitliche Höchstfrist für das EAV von zehn Jahren vorgesehen.

Abs. 5a sieht eine Regelfrist von 20 Jahren für das EAV vor, wenn der Ausländer wegen eines Verbrechens gegen den Frieden, eines Kriegsverbrechens oder eines Verbrechens gegen die Menschlichkeit oder zur Abwehr einer Gefahr für die Sicherheit der Bundesrepublik Deutschland oder einer terroristischen Gefahr ausgewiesen wurde. Eine Verlängerung der Frist aus Gründen der öffentlichen Sicherheit und Ordnung ist nach Ermessen möglich, was durch den Verweis auf Abs. 4 S. 4 und 5 in Abs. 5a S. 2 klargestellt wird.

Nach Abs. 5b S. 2 kann im Einzelfall ein unbefristetes EAV in den Fallgruppen des Abs. 5a erlassen werden, wenn dies unter Berücksichtigung aller Umstände erforderlich und verhältnismäßig ist. Ebenso kann im Einzelfall ein unbefristetes EAV erlassen werden, wenn der Ausländer wegen eines in § 54 Abs. 1 Nr. 1 genannten Ausweisungsinteresses ausgewiesen worden ist; diese Fälle können im Einzelfall denjenigen nach Abs. 5a in ihrer Schwere gleichstehen. Dabei ist auch im Einzelfall die Schwere der Gefährdung zu berücksichtigen.

2. Ergebnisse der Länderbefragung

Ganz überwiegend schätzen die Länder die Neustrukturierung der Regelung, insbesondere der Fristenregelungen in Abs. 5 bis Abs. 5b AufenthG, als hilfreich ein. Von der Möglichkeit eines unbefristeten EAVs für Intensivstraftäter nach § 11 Abs. 5b S. 2 AufenthG wurde in besonders gelagerten Einzelfällen Gebrauch gemacht. Insgesamt sehen alle Länder, soweit

Erfahrungswerte vorlagen, die Neuregelung als – zumindest grundsätzlich – praxistauglich an.

Mehrere Länder wünschen sich Anwendungshinweise oder die Ergänzung von Regelbeispielen hinsichtlich der Fristanwendung zur Erleichterung der Ermessensausübung. Gemäß des Wortlauts von § 84 Abs. 1 AufenthG haben Widerspruch und Klage nur gegen die Befristung des EAV keine aufschiebende Wirkung, nicht aber gegen die Anordnung des EAVs nach § 11 Abs. 1 S. 1 AufenthG. Daher plädieren mehrere Länder für eine Anpassung von § 84 Abs. 1 S. 1 Nr. 7 AufenthG an den geänderten § 11 Abs. 1 S. 1 AufenthG.

3. Rechtsprechungsanalyse

Das OVG Lüneburg hat mit Urteil vom 06.05.2020 - 13 LB 190/19 - bestätigt: Bei einer auf der Grundlage des § 11 AufenthG in der durch das Zweite Gesetz zur besseren Durchsetzung der Ausreisepflicht geänderten Fassung getroffenen Anordnung und Befristung eines Einreise- und Aufenthaltsverbots handelt es sich um einen einheitlichen Verwaltungsakt, der nicht zwischen der Anordnung des Verbots und dessen Befristung aufgespalten werden kann (2. LS, Rdnr. 54).

Der VGH Mannheim hat mit Beschluss vom 21.01.2020 – 11 S 3477/19 - bestätigt: Das Verbot der Erteilung eines Aufenthaltstitels (Titelerteilungssperre) ist keine unmittelbare Rechtsfolge der Ausweisung, Zurückschiebung oder Abschiebung mehr, sondern eine Folge des Erlasses des Einreise- und Aufenthaltsverbots (2. LS, Rdnr. 21).

Der VGH Mannheim hat mit Beschluss vom 13.11.2019 - 11 S 2996/19 – entschieden: Widerspruch und Klage gegen ein an eine Abschiebung anknüpfendes, befristetes Einreise- und Aufenthaltsverbot nach § 11 Abs. 1 und 2 entfalten nach § 80 Abs. 2 S. 1 Nr. 3 VwGO in Verbindung mit § 84 Abs. 1 S. 1 Nummer 7 AufenthG keine aufschiebende Wirkung (LS, Rn. 41). Zwar beziehe sich § 84 Abs. 1 S. 1 Nr. 7 AufenthG seinem Wortlaut nach nur auf die Befristung des Einreise- und Aufenthaltsverbots. Ausweislich der Gesetzesbegründung wurde mit der Neufassung von § 11 AufenthG jedoch ausschließlich das Anliegen verfolgt, das deutsche Aufenthaltsrecht in Bezug auf Einreise- und Aufenthaltsverbote, die an behördliche Rückkehrentscheidungen anknüpfen, mit der Rückführungsrichtlinie 2008/115/EG und der dazu ergangenen Rechtsprechung in Einklang zu bringen. Aus den Gesetzgebungsmaterialien lasse sich hinreichend deutlich ableiten, dass das 2015 geschaffene Regelungssystem in § 84 Abs. 1 AufenthG, wonach die aufschiebende Wirkung von Widerspruch und Klage in Bezug auf sämtliche Behördenentscheidungen ausgeschlossen werden, die den Erlass und die inhaltliche

Ausgestaltung von Einreise- und Aufenthaltsverboten nach § 11 AufenthG zum Gegenstand haben, nicht geändert werden sollte (Rdnr. 42 ff).

In zwei Entscheidungen des VG Karlsruhe wurden unbefristete Einreise- und Aufenthaltsverbote nach § 11 Abs. 5b S. 2 AufenthG bestätigt:

- Im Fall einer Ausweisung eines Ausländers wegen eines in § 54 Abs. 1 Nr. 1 AufenthG genannten Ausweisungsinteresses urteilte das VG Karlsruhe, dass der Erlass eines unbefristeten Einreise- und Aufenthaltsverbots gemäß § 11 Abs. 5b S. 2 AufenthG rechtmäßig war (VG Karlsruhe, Urteil vom 27. April 2021 11 K 4211/20). Der Ausländer hatte zahlreiche strafrechtliche Verurteilungen und keinen nachhaltigen Einstellungswandel vorzuweisen.
- In einem anderen Verfahren hielt das VG Karlsruhe die Befristung des Einreise- und Aufenthaltsverbots auf 20 Jahre (§ 11 Abs. 5a AufenthG) aufrecht (VG Karlsruhe, Urteil vom 08.12.2020 12 K 6511/19). Das Gericht wies dabei darauf hin, dass der Rechtmäßigkeit der Befristungsentscheidung nicht entgegenstehe, dass der Fristbeginn gemäß § 11 Abs. 2 S. 4 AufenthG an die Ausreise des Ausländers anknüpft und dem Ausländer deshalb bei einem dauerhaft bestehenbleibenden nationalen Abschiebungsverbot im Hinblick auf sein Herkunftsland Irak eine unbefristet wirkende Titelerteilungssperre drohen könnte. Denn ein ausgewiesener Ausländer, hinsichtlich dessen Herkunftsland ein Abschiebungsverbot festgestellt worden sei, könne gleichwohl aus dem Bundesgebiet ausreisen und sei hierzu für die Dauer seiner Duldung auch verpflichtet; somit habe er es selbst in der Hand, ob er der Ausreisepflicht nachkomme und die Frist des Einreise- und Aufenthaltsverbots in Gang setze. Außerdem bestehe grundsätzlich weiterhin die Möglichkeit einer Abschiebung in ein anderes Land.

Andere Gerichte ließen unbefristete Einreise- und Aufenthaltsverbote gemäß § 11 Abs. 5b S. 2 AufenthG im Zusammenhang mit dem Milieu der organisierten Kriminalität nicht zu, weil keine Gefahr gemäß § 11 Abs. 5a AufenthG für die innere Sicherheit der Bundesrepublik Deutschland durch Verhaltensweisen und Strafrechtsverstöße im Milieu der organisierten Kriminalität vorliege bzw. das Einreise- und Aufenthaltsverbot nicht verhältnismäßig sei (VG Gießen, Beschluss vom 27.05.2020 7 L 876/20.GI; VGH Hessen Beschluss vom 02.11.2020 9 B 1553/20; VG Darmstadt, Beschluss vom 25.01.2021 6 L 566/20.DA; VGH Hessen Beschluss vom 15.04.2021 9 B 314/21).

III. Der neue Duldungstatbestand für Personen mit ungeklärter Identität

1. Ziel

Um Fehlanreize zum rechtswidrigen Verbleib im Bundesgebiet trotz vollziehbarer Ausreisepflicht zu beseitigen, wurde mit § 60b AufenthG eine besondere gesetzliche Passbeschaffungspflicht für vollziehbar ausreisepflichtige Ausländer eingeführt, an deren Verletzung sich ein neuer Duldungstatbestand „für Personen mit ungeklärter Identität“ mit gesetzlichen Sanktionen knüpft. Für vollziehbar ausreisepflichtige Ausländer statuiert § 60b Abs. 2 AufenthG die Verpflichtung, alle ihnen (näher in § 60b Abs. 3 AufenthG beschriebenen) zumutbaren Handlungen zur Beschaffung eines Passes oder Passersatzes selbst vorzunehmen. Vollziehbar ausreisepflichtigen Ausländern wird die Duldung mit dem Zusatz "Duldung für Personen mit ungeklärter Identität" erteilt, wenn die Abschiebung aus von ihnen selbst zu vertretenden Gründen nicht vollzogen werden kann, weil sie das Abschiebungshindernis durch eigene Täuschung über ihre Identität oder Staatsangehörigkeit selbst herbeiführen oder sie zumutbare Handlungen zur Erfüllung ihrer Passbeschaffungspflicht nicht vornehmen.

Die Erteilung einer Duldung nach § 60b Abs. 1 AufenthG zieht gemäß § 60b Abs. 5 AufenthG gesetzliche Sanktionen nach sich: Die Zeiten, in denen dem Ausländer die Duldung mit dem Zusatz "für Personen mit ungeklärter Identität" ausgestellt worden ist, werden für die Aufenthaltserlaubnis nach § 25a AufenthG, § 25b AufenthG oder § 25 Abs. 5 AufenthG nicht als Vorduldungszeiten angerechnet (§ 60b Abs. 5 S. 1 AufenthG). Dem Inhaber der Duldung darf die Ausübung einer Erwerbstätigkeit nicht erlaubt werden (§ 60b Abs. 5 S. 2). Darüber hinaus unterliegt er einer Wohnsitzauflage nach § 61 Abs. 1d AufenthG (§ 60b Abs. 5 S. 3). Die Nichtvornahme der zumutbaren Handlungen zur Erfüllung der besonderen Passbeschaffungspflicht kann darüber hinaus nach § 98 Abs. 3 Nr. 5b AufenthG mit einer Geldbuße von bis 5 000 Euro geahndet werden.

Hintergrund der Einführung war die praktische Erfahrung der Vollzugsbehörden, dass vollziehbar Ausreisepflichtige ohne Identitätspapiere vielfach nicht kooperationsbereit waren und die geltenden Regelungen zur Passbeschaffung oftmals nicht befolgten.

Ziel der Regelung ist es darüber hinaus, besser danach differenzieren zu können, ob und inwieweit die Abschiebung aus von dem vollziehbar Ausreisepflichtigen selbst zu vertretenden Gründen nicht vollzogen werden kann.

2. Ergebnisse der Länderbefragung

Die Länder machen in der Praxis durchweg – in unterschiedlichem Ausmaß - Gebrauch von den neuen Regelungen[6], wobei nicht alle die Möglichkeit der Bußgeldverhängung nutzen.

Die Vorschrift hat sich nach Einschätzung aller Länder mit Ausnahme eines Bundeslandes als praxistauglich erwiesen.

Die mit den Regelungen gemachten Erfahrungen sind gemischt:

Als negativ sehen viele Länder den mit der Anwendung verbundenen Verwaltungsaufwand an, insbesondere die weitgehenden Anhörungs- und Belehrungspflichten, die hohen Anforderungen an die Dokumentation der jeweiligen Verfahrensschritte, die komplexen Erteilungsvoraussetzungen und die Bearbeitung der vielfältigen Klageverfahren. Eine größere Anzahl von Ländern hebt auf der anderen Seite positiv hervor, dass nach Feststellung der Voraussetzungen klare Rechtsfolgen einträten, die das Verfahren (z.B. Bearbeitung von Anträgen auf Beschäftigungserlaubnisse) im Vergleich zur alten Rechtslage deutlich erleichterten.

Mit vereinzelten Ausnahmen durchweg positiv wird die durch die Vorschriften erreichte bessere Differenzierbarkeit zwischen kooperativen und nicht kooperativen Ausreisepflichtigen bewertet.

Die mit der Duldung verbundenen Nachteile bzw. Sanktionen werden vielfach als zu wenig weitgehend empfunden, um tatsächlich spürbare Verhaltensänderungen bei (insbesondere langjährig) nicht kooperierenden Ausreisepflichtigen zu erreichen.

Überwiegend wird berichtet, dass sich die Bereitschaft der Ausreisepflichtigen zur Beschaffung von Dokumenten infolge der Neuregelung (zwischen geringfügig und merklich) gesteigert habe, oftmals wird dies insbesondere für die Gruppe der Personen mit Beschäftigungserlaubnis oder mit Ausblick auf eine Aufenthaltserlaubnis gesehen, vereinzelt auch mit Blick auf bestimmte Nationalitäten (AFG, PAK), auch würden Überlegungen zur freiwilligen Ausreise gestärkt. Die schon lange andauernden pandemiebedingten Einschränkungen der Botschaftskontakte machten hier allerdings definitive Aussagen schwierig. Einzelne Länder nehmen hingegen keinerlei Verbesserungen wahr.

Viele Länder weisen darauf hin, dass die Aussichten auf eine tatsächliche Durchsetzung der Ausreisepflicht dadurch konterkariert würden, dass sich vorwiegend diejenigen Personen verstärkt um Dokumente bemühten, die auch aus anderen Gründen nicht unmittelbar abgeschoben werden könnten bzw. für eine Rückführung ungeeignete Dokumente vorgelegt

[6] Vgl. zur Erteilung der Duldung für Personen mit ungeklärter Identität AZR-Auswertung in Anlage 4.

würden. Z.T. weisen die Länder darauf hin, dass die Restriktionen bei vielen beharrlichen Mitwirkungsverweigerern und auch langzeitig Geduldeten keinen Eindruck machten. Positiv wird teilweise gewertet, dass zumindest ein Hineinwachsen in eine Aufenthaltserlaubnis durch die Duldung nach § 60b AufenthG verhindert werde.

Am häufigsten wurden folgende Änderungs- und Verbesserungsvorschläge genannt:

- Wunsch nach gesetzlicher Klarstellung, dass der Verstoß gegen die Passbeschaffungspflicht lediglich mitursächlich für das Unterbleiben der Abschiebung sein muss (keine Monokausalität). Dies ist zwar in den Vorläufigen Anwendungshinweisen des BMI zu § 60b AufenthG grundsätzlich klargestellt, es liegt jedoch hierzu gegenläufige Rechtsprechung der Verwaltungs- und Oberverwaltungsgerichte vor (vgl. OVG Niedersachsen, Beschluss vom 09. Juni 2021, 13 ME 587/20, Rn. 49; sowie Beschluss vom 23. Juni 2021, 13 PA 96/21, Rn. 6; VG Cottbus, Beschluss vom 28.05.2020, 9 L 134/20, Rn. 9; VG Dresden, Beschluss vom 26. Mai 2021, Az. 3 L 339/21, unveröffentlicht).
- Abkehr von der Aussetzung der besonderen Passbeschaffungspflicht nach § 60b Abs. 2 S. 2 AufenthG für bestimmte Personengruppen. Die Vorschläge sind hier unterschiedlich weitgehend: Zum Teil wird vorgeschlagen, die Pflichten auf alle vollziehbar Ausreisepflichtigen bzw. zumindest Personen mit subsidiärem Schutz zu erstrecken bzw. unmittelbar nach Erlöschen der Aufenthaltsgestattung anzusetzen. Zum Teil wird nur vorgeschlagen, offensichtlich unbegründete Asylanträge von der Aussetzung auszunehmen.
- Erweiterung des Katalogs sanktionierender Rechtswirkungen; konkret schlagen einzelne Länder z.B. vor, an die Erteilung automatisch Leistungskürzungen nach § 1a AsylbLG, Titelerteilungssperren oder räumliche Beschränkungen zu knüpfen.
- Verzicht auf die Möglichkeit, die Erfüllung erforderlicher Handlungen zur Passbeschaffung mittels Versicherung an Eides statt glaubhaft zu machen (§ 60b Abs. 3 S. 4). Dies sei nach den gesammelten Erfahrungen kein verlässliches Mittel der Glaubhaftmachung.
- Genauere Definition der ausreichenden/zumutbaren Handlungen zur Mitwirkung/Glaubhaftmachung (ggf. in Vorläufigen Anwendungshinweisen/VwV).
- Z.T. wird vorgeschlagen, die missverständliche Bezeichnung der Duldung (die auch bei Personen mit geklärter Identität, aber ohne Dokumente greift) zu ändern, die bei den Betroffenen zu falschen Erwartungen bzw. Verwirrung führe.
- Einzelne Länder stehen der Konzeption des § 60b AufenthG insgesamt kritisch gegenüber, weil sie sich weitergehende Integrationsmöglichkeiten für Geduldete wünschen.

3. Rechtsprechungsanalyse

Mehrere Entscheidungen befassen sich mit dem Verhältnis der besonderen Passbeschaffungspflicht nach § 60 b Abs. 2 S. 1 AufenthG zur allgemeinen Mitwirkungspflicht nach § 48 Abs. 3 S. 1 AufenthG:

- Das OVG Lüneburg (Beschluss vom 01. September 2020 – 13 ME 312/20, Rn. 6) hat dazu festgestellt, dass die allgemeine Mitwirkungspflicht des § 48 Abs. 3 S. 1 AufenthG durch § 60b Abs. 2 S. 1 AufenthG nicht ausgeschlossen wird.
- Eine im wesentlichen gleichlautende Entscheidung ist durch das OVG Berlin-Brandenburg ergangen (Beschluss vom 19. April 2021 – OVG 3 S 19/21, Rn. 3): § 60b Abs. 2 S. 2 AufenthG sei eine Ausnahmeregelung von der in § 60b Abs. 2 S. 1 AufenthG bestimmten besonderen Passbeschaffungspflicht. Dieser speziellen Vorschrift, die lediglich eine Duldung für Personen mit ungeklärter Identität betrifft, könne nicht entnommen werden, dass eine Anordnung zur Mitwirkung an der Passbeschaffung außerhalb dieses Regelungszusammenhangs generell unzulässig ist.

Wie unter 1. bereits dargestellt, haben mehrere Gerichte Aussagen zur notwendigen Kausalität zwischen verletzter Passbeschaffungspflicht und mangelnder Abschiebungsaussicht getroffen:

- Das VG Cottbus hat mit Beschluss vom 28. Mai 2020 – 9 L 134/20 (dort Rn. 9) entschieden, dass die Erteilung einer „Duldung für Personen mit ungeklärter Identität“ eine Kausalität zwischen der Unmöglichkeit der Abschiebung und einer vom Ausländer zu vertretenen ungeklärten Identität bzw. der Nichterfüllung von Mitwirkungspflichten bei der Passbeschaffung fordere. Diese fehle, wenn neben der ungeklärten Identität bzw. dem Nichtvorhandensein eines die Rückführung ermöglichenden Passes oder sonstigen Rückreisedokuments ein weiterer selbständiger Grund tritt, dass die Abschiebung aus tatsächlichen oder rechtlichen Gründen nicht vollzogen werden kann.
- Dieser Auffassung ist auch das VG Dresden mit Beschluss vom 26. Mai 2021 - 3 L 339/21 (unveröffentlicht) gefolgt. Dies folge aus dem Wortlaut der Norm. Da der Halbsatz "wenn die Abschiebung aus von ihm selbst zu vertretenden Gründen nicht vollzogen werden kann" vor den mit "weil" beginnenden Satz gestellt ist, ergebe sich, dass sich die geforderte Kausalität auf alle in den selbstständig nebeneinanderstehenden Fallgruppen beschriebenen Verhaltensweisen des Ausländers bezieht.

- Diese Auffassung vertritt auch das OVG Lüneburg erstmals in einem obiter dictum seines Beschlusses vom 09. Juni 2021, Az. 13 ME 587/20, Rn. 49.
- Seine Auffassung bestätigt das OVG Lüneburg in einem weiteren Beschluss vom 23. Juni 2021 (Az. 13 PA 96/21, dort Rn. 6 ff.). An der notwendigen Kausalität fehle es in den hier beschriebenen „Mischfällen“, schon weil der damit beabsichtigte Druck auf den vollziehbar ausreisepflichtigen Ausländer, im Interesse der Aufenthaltsbeendigung durch Abgabe einer Identitäts- oder Staatsangehörigkeitstäuschung oder durch Vornahme von Mitwirkungshandlungen die Beschaffung von Rückreisedokumenten zu ermöglichen, jeden Sinn verlöre. Die Kausalität im o.g. Sinne wird nach Ansicht des OVG Lüneburg auch durch die Annahme einer Härtefalleingabe zur Beratung in der Niedersächsischen Härtefallkommission und die damit verbundene Aussetzung aufenthaltsbeendender Maßnahmen bis zu einer Entscheidung unterbrochen.

Das VG Minden hat mit Beschluss vom 13. Januar 2020 (7 L 1317/19) entschieden, dass die Liste der regelmäßig zumutbaren Mitwirkungshandlungen in § 60b Abs. 3 S. 1 AufenthG nicht abschließend ist. Für die Beurteilung der Zumutbarkeit der Passbeschaffungshandlungen seien alle Umstände des Einzelfalles entscheidend (3. LS und Rn. 18f.).

IV. Praktikablere Ausgestaltung der Sicherungshaft durch neue Tatbestände und Indizien

1. Ziel

Die Voraussetzungen für Sicherungshaft nach § 62 Abs. 3 des Aufenthaltsgesetzes wurden durch das 2. Gesetz zur Verbesserung der Ausreisepflicht systematischer gefasst und die Haftgründe ausgeweitet.

Dabei wurden insbesondere Fallgruppen normiert, bei deren Vorliegen Fluchtgefahr widerleglich vermutet wird (§ 62 Abs. 3a AufenthG), während es in anderen Fallgruppen bei konkreten Anhaltspunkten („Indizien“) für Fluchtgefahr bleibt (§ 62b Abs. 3b AufenthG). Dadurch sollte die Sicherungshaft für die jeweiligen Anwender praktikabler gestaltet werden. Insbesondere sollte so der Aufwand für die Überprüfung und Abfassung von Haftanträgen merklich reduziert und insgesamt der Vollzug von Abschiebungen verbessert werden.

Aufgrund der verfassungsrechtlich begründeten Vorgaben des § 62 Abs. 1 S. 1 AufenthG ist jedoch in jedem Fall weiterhin eine Einzelfallentscheidung unter Berücksichtigung sämtlicher Umstände erforderlich.

2. Ergebnisse der Länderbefragung

Fast alle Länder haben positive Erfahrungen mit den mit den neuen Vermutungstatbeständen (§ 62 Abs. 3a AufenthG) und Indizien (§ 62b Abs. 3b AufenthG) gemacht. Einzelne Länder geben an, nur eingeschränkt Erfahrungswerte zu haben, bzw. ein Land macht von der Möglichkeit der Sicherungshaft nur zurückhaltend Gebrauch.

Soweit die Länder von der Möglichkeit der Sicherungshaft nicht nur zurückhaltend Gebrauch machen, halten sie die neu eingebrachte Vermutungsregelung übereinstimmend für praktikabel.

Als positiv werde u.a. die systematische Gesetzgebungstechnik empfunden, insbesondere die klarere Regelung des Haftgrunds „Fluchtgefahr“, die die Darlegung bei Haftanträgen vereinfache. Die systematische Auflistung der konkreten Anhaltspunkte als objektive Kriterien für eine Fluchtgefahr in Abs. 3b erleichterten die Erstellung von Haftanträgen ebenso wie die Vermutungstatbestände des Abs. 3a.

Einige Länder sehen zwar in der Aufnahme der Vermutungsregelungen einen erleichterten Begründungsaufwand für einen Haftantrag, die Mehrzahl der Länder gibt jedoch an, dass

dieser im Verhältnis zur Vorgängerregelung im Wesentlichen gleichgeblieben sei. Als Ursache wird z.T. auf die weiterhin hohen formalen Anforderungen an Haftanträge nach den Vorgaben des FamFG und entsprechend hohe Vorgaben der Gerichte mit Blick auf Darlegung und Interessenabwägung hingewiesen. Als positiv wird jedoch zum Teil empfunden, dass eine eigene Definition der Fluchtgefahr nicht mehr erforderlich sei und die gesetzlichen Vermutungsregelungen mehr Sicherheit für die Ausländerbehörde bei der Begründung von Fluchtgefahr schafften (s.o. 2. Abs.).

In Bezug auf die Frage, von welchen Tatbeständen des § 62 Abs. 3a häufiger Gebrauch gemacht wird, wurden am häufigsten Nr. 3 und Nr. 5 genannt, gefolgt von Nr. 6 und Nr. 1. Ursächlich hierfür sei, dass die angeführten Nummern Lebenssachverhalte erfassten, die häufig vorkämen und faktenbasierte Fallkonstellationen darstellen.

Von den Tatbeständen des § 62 Abs. 3a, die seltener einschlägig sind, wird vor allem § 62 Abs. 3a Nr. 2 genannt, aber auch Nr. 4. Als Grund hierfür wird u.a. aufgeführt, dass die Konstellation selten einschlägig sei, erheblicher Verwaltungsaufwand durch Belehrungspflichten entstehe bzw. regelmäßig bereits ein anderer Haftgrund erfüllt sei.

In Bezug auf die Frage, von welchen Tatbeständen des § 62 Abs. 3b häufiger Gebrauch gemacht wird, wurden am häufigsten Nr. 1 und Nr. 4 genannt, mehrere Länder nannten auch Nr. 5 und Nr. 7. Diese Sachverhalte seien häufig und gut nachweisbar, da faktenbasiert.

Von den Tatbeständen des § 62 Abs. 3b, die seltener einschlägig sind, wurde am häufigsten § 62 Abs. 3b Nr. 2 genannt. Diese Sachverhalte würden weniger häufig auftreten, bzw. seien schwieriger nachzuweisen.

Fast alle Länder konnten Angaben zur (geschätzten) relativen Erfolgsquote der beantragten Fälle von Sicherungshaft machen; diese sei hoch bis sehr hoch (genannt werden 75% - 98%). Die relative Erfolgsquote bleibt nach Einschätzung der meisten Länder im Vergleich zur alten Rechtslage unverändert, einige Länder sehen aber auch (z.T. deutliche) Steigerungstendenzen. Ergänzend weisen einige Länder darauf hin, dass in absoluten Zahlen in mehr Fällen als zuvor erfolgreich Abschiebungshaft beantragt werden bzw. mehr Haftanträge durch die Behörden gestellt werden könnten.

Zahlreiche Länder sind der Auffassung, dass durch die Neuregelung eine Verbesserung im Vollzug der Abschiebungen erreicht werden konnte, da eine Inhaftierung in mehr Fällen in Betracht kommt und Abschiebungen aus der Haft heraus eine höhere Erfolgsquote haben. Einige Länder weisen darauf hin, dass aufgrund der coronabedingt eingeschränkten Vollzugsmöglichkeiten noch keine Aussage getroffen werden könne bzw. verweisen auf zusätzliche Vollzugshindernisse unabhängig von den Haftvorschriften.

In Bezug auf Verbesserungsmöglichkeiten nennen zahlreiche Länder die hohen (formalen) Anforderungen an die Darlegung der Haftvoraussetzungen und wünschen sich, dass der Anspruch an die Nachweis- bzw. Begründungspflicht gesenkt werde. Darüber hinaus setzen sich einzelne Länder dafür ein, dass das FamFG im Falle einer Erledigung des Freiheitsentziehungsverfahrens auch der beteiligten Behörde ein Beschwerderecht einräumt.

Mehrere Länder empfehlen statt des Verweises des § 2 Abs. 14 AufenthG auf § 62 AufenthG einen eigenen Katalog an Tatbeständen für Fluchtgefahr im Dublinverfahren aufzunehmen, um eine Vermischung der Dublinhaft (§ 2 Abs. 14 AufenthG) mit § 62 AufenthG zu vermeiden.

Einzelne Länder nennen allgemeinen praktischen Verbesserungsbedarf. So wünschen sich einige Länder mehr verfügbare Haftplätze und eine Beschleunigung des Asylverfahrens bzw. von Rechtsmittelverfahren.

3. Rechtsprechungsanalyse

Der BGH hat mit Beschluss vom 20. April 2021 – XIII ZB 47/20 – entschieden, dass der Vermutungstatbestand des § 62 Abs. 3a Nr. 5 AufenthG voraussetzt, dass der Ausländer eine konkrete, auf seine Abschiebung gerichtete Maßnahme der Behörde vereitelt hat (LS.).

Der BGH hat mit Beschluss vom 26.01.2021 – XIII ZB 20/20 - entschieden, dass eine die widerlegliche Vermutung der Fluchtgefahr begründende Identitätstäuschung gemäß § 62 Abs. 3a Nummer 1 AufenthG vorliegt, wenn der Betroffene seine wahre Identität nicht preisgibt, etwa durch die Angabe diverser Aliaspersonalien oder durch falsche Angaben zu seiner Person, wofür bereits geringe Abweichungen bei den Personalien wie ein anderer Vorname und ein verändertes Geburtsdatum genügen (Rn. 9).

Der BGH hat mit Beschluss vom 24.06.2020 – XIII ZB 33/19 - entschieden, dass die in § 62 Abs. 3a und 3b AufenthG bestimmten Anhaltspunkte für (erhebliche) Fluchtgefahr abschließend sind (Rn. 15).

V. Neueinführung der Mitwirkungshaft

1. Ziel

In § 62 Abs. 6 AufenthGs wurde das Institut der Mitwirkungshaft neu geschaffen. Hintergrund der Neueinführung waren Erfahrungen aus der Vollzugspraxis, dass Anordnungen nach § 82 Abs. 4 S. 1 AufenthG, insbesondere die Anordnung, bei der Vertretung des Herkunftsstaates zum Zwecke der Identitätsklärung zu erscheinen, vielfach ins Leere liefen und die Erscheinensquote bei entsprechenden Terminen sehr niedrig war. Die Betreffenden waren, sofern diese zu einem Termin vorgeführt werden sollten, vielfach nicht auffindbar. Es bestand daher das Bedürfnis nach einer Möglichkeit, Personen, die bereits in der Vergangenheit entsprechende Mitwirkungspflichten verletzt haben, zum Zwecke der Durchführung der o.g. Anordnungen kurzfristig in Haft nehmen zu können.

2. Beurteilung durch die Länder

Zahlreiche Länder haben keine Erfahrungswerte im Zusammenhang mit der Mitwirkungshaft.

Dies liegt nach Auffassung einiger Länder u.a. daran, dass es aufgrund der Pandemiesituation im Laufe des letzten Jahres weniger Vorführungsmöglichkeiten gab.

Die Länder, die die Mitwirkungshaft einsetzen, geben allerdings an, bisher gute Erfahrungen damit gemacht zu haben. So erwähnen mehrere Länder, dass bereits die alleinige Androhung von Mitwirkungshaft zum gewünschten Erfolg geführt habe. Ein Land begrüßt die klaren gesetzlich geregelten Voraussetzungen und sieht im längeren Zeitraum gegenüber der Vorführhaft nach § 82 Abs. 4 Sätze 2 und 3 AufenthG eine Verbesserung.

Die relative Erfolgsquote der Mitwirkungshaft wird von mehreren Ländern als hoch eingeschätzt. Als Grund wird z.T. eine gute Nachweisbarkeit aufgeführt.

Bei der Einschätzung des Arbeitsaufwands für die Abfassung eines entsprechenden Haftantrags gehen die Meinungen auseinander. Zum Teil wird dieser als geringer eingeschätzt, zum Teil aber auch als vergleichbar mit Anträgen für die Sicherungshaft.

Von den Ländern, die bereits Erfahrungen mit der Mitwirkungshaft gesammelt haben, gaben mehrere an, dass durch die Mitwirkungshaft eine Verbesserung mit Blick auf die Durchführung von Mitwirkungshandlungen erreicht werden konnte bzw. sehen die Mitwirkungshaft als geeignetes Druckmittel an. Ein Land konnte keine gesteigerte Mitwirkung der Betroffenen verzeichnen, ein anderes bezweifelte aufgrund der Erfahrung mit

mangelnder Mitwirkung von Inhaftierten bei der Passbeschaffung, dass eine Kooperationsbereitschaft durch die Mitwirkungshaft erreicht werden könne.

3. Rechtsprechungsanalyse

Es ist keine Rechtsprechung zur Mitwirkungshaft bekannt geworden.

VI. Praktikablere Ausgestaltung des Ausreisegewahrsams

1. Ziel

Mit der Neuregelung des Ausreisegewahrsams sollte dieser praxisgerecht fortentwickelt werden. Im Rahmen der Neufassung des § 62b AufenthG wurde daher klargestellt, dass für die Anordnung des Ausreisegewahrsams das Bestehen von Fluchtgefahr nicht Voraussetzung ist, da in diesem Punkt einige Gerichte die gesetzlichen Voraussetzungen enger interpretiert haben als vorgesehen.

Zudem wird nunmehr in bestimmten gesetzlich angeführten Fällen (widerleglich) vermutet, der Ausländer werde die Abschiebung erschweren oder vereiteln (§ 62b Abs. 1 S. 1 Nr. 3 lit. a) – d) AufenthG).

Durch Neufassung des Tatbestandsmerkmals in Abs. 2 „im Transitbereich eines Flughafens oder in einer Unterkunft, von der aus die Ausreise des Ausländers ohne Zurücklegen einer größeren Entfernung zu einer Grenzübergangsstelle möglich ist“ wurde klargestellt, dass die Unterbringung in einer Unterkunft, die sich im weiteren Umfeld eines Flughafens oder einer Grenzübergangstelle befindet, möglich ist. Dabei ist eine übliche Fahrzeit von etwa einer Stunde von Unterkunft bis Flughafen oder Grenzübergang als „ohne Zurücklegen einer größeren Entfernung“ zu bewerten.

2. Beurteilung durch die Länder

Mit Ausnahme eines Landes berichten alle Länder, die über Erfahrungswerte zur Neufassung des Ausreisegewahrsams verfügen, über positive Erfahrungen mit der Regelung.

U.a. wird in der Regelung eine sinnvolle und praktikable Möglichkeit gesehen, Rückführungen zu sichern, bei denen Abschiebungshaft nicht in Betracht kommt. Aufgrund der relativ niedrigschwelligen gesetzlichen Anforderungen und den leicht anzuwenden Voraussetzungen an den Ausreisegewahrsam werde von der Regelung häufig Gebrauch gemacht.

Fast alle Länder sehen in der Klarstellung in § 62b AufenthG, dass Fluchtgefahr nicht für die Ingewahrsamnahme erforderlich ist, eine Erleichterung der praktischen Arbeit der Ausländerbehörden, zum Teil sogar eine deutliche Erleichterung.

Fast einhellig bestätigen die Länder, dass die Vermutungsregelungen des § 62b Abs. 1 S. 1 Nr. 3 lit. a) bis d) AufenthG die praktische Arbeit der Ausländerbehörden erleichtern. Die Vermutungsregelungen mit ihrer Beweislastumkehr seien auf eine Vielzahl von Fällen anwendbar.

Am häufigsten wird auf die Vermutungsregelung des § 62b Abs. 1 S. 1 Nr. 3d) (Überschreitung der Ausreisefrist um mehr als 30 Tage) abgestellt. Die Fallkonstellation komme sehr häufig vor und das Vorliegen sei gut darlegbar und beweisbar, da faktenbasiert. Am zweithäufigsten wurde die Alternative § 62b Abs. 1 S. 1 Nr. 3c) (Verurteilung wegen einer im Bundesgebiet begangenen vorsätzlichen Straftat) genannt. Auch dieser Tatbestand lasse sich gut darlegen. Einige Länder weisen darauf hin, dass häufig mehr als nur eine Vermutungsregelung einschlägig sei.

Einige Länder geben an, dass seltener von § 62b Abs. 1 S. 1 Nr. 3b AufenthG (Täuschung über Identität oder Staatsangehörigkeit) Gebrauch gemacht wird. Als Begründung wird zum einen genannt, dass eine Identitätstäuschung grundsätzlich zwar häufiger vorkomme, jedoch die Falschangabe im Verlauf des Verfahrens oft von den Betroffenen selbst korrigiert werde, sodass die Vermutungsregel nicht mehr greife, zum anderen, dass die Beweisführung diesbezüglich schwieriger sei und häufig auch andere Vermutungstatbestände vorlägen.

Alle Länder geben an, dass sich die Neufassung des Ausreisegewahrsams als praxistauglich erwiesen habe; nur ein Land gab an, mangels Ausreisegewahrsamseinrichtung keine belastbaren Aussagen treffen zu können.

Die Länder schätzen die relative Erfolgsquote bei der Beantragung des Ausreisegewahrsams insgesamt als hoch bis sehr hoch ein, eine Steigerung gegenüber der alten Rechtslage (bzw. eine Steigerung der Anzahl der gestellten Anträge) wird wahrgenommen.

Mehrere Länder gehen von einem geringeren Aufwand für die Abfassung eines entsprechenden Haftantrags im Vergleich zur alten Rechtslage aus, andere sehen den Aufwand als gleichbleibend an. Einzelne Länder konnten die Frage noch nicht abschließend beurteilen.

Fast alle Länder sind der Auffassung, dass die Zuführung zur Abschiebung durch die Neufassung des Ausreisegewahrsams insgesamt verbessert werden konnte.

Am häufigsten wurden folgende Änderungs- und Verbesserungsvorschläge genannt:

- Mehrere Länder schlagen als Verbesserung der Regelung eine Verlängerung der maximalen Dauer des Ausreisegewahrsams vor, da ein Vorlauf zur Abschiebung von

zehn Tagen oftmals sehr knapp sei. Hierbei wird eine maximale Dauer von 14 Tagen, 28 Tagen oder einem Monat genannt.

- Mehrere Länder schlagen eine Klarstellung der Voraussetzungen, die für die Gewahrsamseinrichtung in § 62b AufenthG gelten, vor, z.B. wird vorgeschlagen, auch eine Abschiebungshafteinrichtung explizit als Unterbringungsmöglichkeit in § 62b Abs. 2 zu benennen.

3. Rechtsprechungsanalyse

Der BGH hat mit Beschluss vom 10.11.2020 – XIII ZB 25/20 - entschieden, dass sich nach der Entfernung der Unterkunft zu einer Grenzübergangsstelle, von der aus der Ausländer jederzeit ausreisen kann, bestimmt, ob dem Betroffenen eine Ausreise ohne Zurücklegen einer größeren Entfernung i.S.v. § 62 b Abs. 2 AufenthG möglich ist. In die Betrachtung sind sämtliche Grenzübergangsstellen einzubeziehen, die sich in der Nähe der Unterkunft befinden. Das Tatbestandsmerkmal ist erfüllt, wenn die übliche Fahrzeit von der Unterkunft bis zum Flughafen oder der Grenzübergangsstelle etwa eine Stunde beträgt (Rn. 18 f.).

Der BGH hat mit Beschluss vom 23.02.2021 – XIII ZB 50/20 entschieden, dass die Ausübung des Ermessens bei der Anordnung des Ausreisegewahrsams nach § 62b AufenthG eine Berücksichtigung der relevanten persönlichen Umstände des Betroffenen erfordert. Hat das Amtsgericht nicht erkannt, dass es ein Ermessen hat, und den Betroffenen nicht zu seinen für die Ermessensausübung relevanten persönlichen Umständen - z.B. seiner Arbeitsstelle - befragt, kann der Ermessensfehler nur nach erneuter Anhörung des Betroffenen und nur für die Zukunft geheilt werden (LSe; Rn. 26).

Einzelne Gerichte stellen hohe Anforderungen an die Voraussetzungen für Ausreisegewahrsam. So lehnt das LG Limburg a.d. Lahn Ausreisegewahrsam zur Durchführung eines Corona-Tests als Voraussetzung für eine anstehende Abschiebung ab (LG Limburg a.d. Lahn Beschluss vom 06.04.2021 7 T 47/21; LG Limburg a.d. Lahn Beschluss vom 10.02.2021 7 T 22/21). Für die Anordnung von Ausreisegewahrsam müsse sicher sein, dass die Abschiebung innerhalb der Frist vollziehbar ist. Es stehe aber gerade nicht zwingend fest, dass die Abschiebung durchgeführt werden könne, denn vor der Ausreise sei ein negatives Testergebnis zwingend erforderlich und der Test sei nicht durchgeführt worden. Auch sei die Anordnung von Ausreisegewahrsam unverhältnismäßig, da zunächst eine Inhaftierung des Betroffenen nach § 62 Abs. 6 AufenthG lediglich für die Durchführung des PCR Tests nach § 82 Abs. 4 S. 1 AufenthG zu beantragen sei.

VII. Temporäre Aufhebung des Trennungsgebots

1. Ziel

In Deutschland besteht nur eine begrenzte Kapazität an Abschiebungshaftplätzen (etwa 487 zum Stand 27. März 2019 sowie etwa 613 zum Stand 31. Juli 2021). Aufgrund des Missverhältnisses von vollziehbar Ausreisepflichtigen und Abschiebungshaftplätzen war diese bestehende Kapazität deutlich überlastet.

Damit konnten in der Praxis trotz Vorliegens der Tatbestandsvoraussetzungen zahlreiche Haftanträge nicht gestellt werden.

Dem Mangel an speziellen Abschiebungshaftplätzen wurde durch die – bis zum 30.06.2022 befristete - Aussetzung des Trennungsgebots nach § 62a Abs. 1 des Aufenthaltsgesetzes begegnet, um bis zu 500 weitere Haftplätze in Justizvollzugsanstalten bereitstellen zu können. Wie und ob die Länder diese Möglichkeit im Einzelnen ausschöpfen, bleibt ihnen überlassen.

2. Ergebnisse der Länderbefragung

Ganz überwiegend machen die Länder nicht von der Neuregelung Gebrauch.

Niedersachsen gab an, von der Regelung nur in Ausnahmefällen bei Straftätern Gebrauch gemacht zu haben. Thüringen brachte im Jahr 2019 einen Gefährder in einer JVA unter (Anm.: bei Gefährdern war auch nach der alten und wieder ab dem 01.07.2022 geltenden Fassung des § 62a Abs. 1 AufenthG eine Unterbringung in Haftanstalten möglich).

Sachsen-Anhalt gab an, die Regelung des neuen § 62a Abs. 1 AufenthG zu nutzen, wodurch sich grundsätzlich die Haftplatzsituation entspannt habe.

3. Rechtsprechungsanalyse

Das AG Hannover hat mit Beschluss vom 12.10.2020 - 44 XIV 43/20 B – dem Gerichtshof der Europäischen Union gemäß Art. 267 AEUV die Frage zur Vorabentscheidung vorgelegt, ob ein nationales Gericht das Vorliegen einer Notlage nach Art. 18 der Rückführungsrichtlinie überprüfen muss, auch wenn der nationale Gesetzgeber eine entsprechende gesetzliche Grundlage im Aufenthaltsrecht vorsieht.

Eine Entscheidung des EuGH hierzu ist noch nicht ergangen.

VIII. Absenkung des Ausweisungsschutzes für Straftäter

1. Ziel

Das Ausweisungsrecht wurde dahingehend überarbeitet, dass der besondere Ausweisungsschutz für bestimmte Personengruppen stärker ausdifferenziert wurde. Darüber hinaus wurden jeweils spezifische Ausweisungsschutzvorschriften für Asylberechtigte und anerkannte Flüchtlinge auf den Kern der europa- und völkerrechtlichen Vorgaben zurückgeführt. Damit sollten die Möglichkeiten, bei schutzberechtigten Intensivstraftätern im Einzelfall ein Überwiegen des öffentlichen Ausreiseinteresses zu begründen, erleichtert werden.

2. Ergebnisse der Länderbefragung

Überdurchschnittlich viele Länder geben an, noch keine oder wenige Erfahrungen mit der Regelung gesammelt zu haben. Soweit solche vorliegen, schätzen die Länder die Absenkung des Ausweisungsschutzes für Straftäter mit Schutzstatus weit überwiegend als praxistauglich ein.

Die Erfahrung mit der Regelung wird überwiegend als positiv beschrieben. Einige Länder sehen Erleichterungen etwa beim Begründungsaufwand. Mehrere Länder geben allerdings an, faktisch sei der Prüfungsmaßstab unverändert geblieben, der Aufwand bei den Ausländerbehörden sei unverändert.

Mehrere Länder sehen für bestimmte Fallkonstellationen einen fehlenden Gleichlauf zu unionsrechtlichen Vorgaben. Bei anerkannten Asylberechtigten und Flüchtlingen seien weiterhin die Schutzbestimmungen des Kapitels VII der Richtlinie 2011/95/EU heranzuziehen.

Es wird auch von mehreren Ländern vorgetragen, dass die unionsrechtlichen Möglichkeiten, den Ausweisungsschutz abzusenken, nicht ausgeschöpft seien. Art. 24 Abs. 1 der Richtlinie 2011/95/EU sehe weitergehende Möglichkeiten vor.

Dem entsprechend wurde am häufigsten als Verbesserungsvorschlag genannt, die Vorschrift stringenter an den unionsrechtlichen Vorgaben auszurichten, u.a. um eine weitere Absenkung des Ausweisungsschutzes für Straftäter zu erreichen. Darüber hinaus soll der Rechtsbegriff „schwere Straftat“ in § 53 Abs. 3b AufenthG nach Wunsch vieler Länder definiert werden.

3. Rechtsprechungsanalyse

Der VGH Baden-Württemberg hat mit Urteil vom 15. April 2021 - VGH 12 S 2505/20 - entschieden: Der Begriff „schwere Straftat“ im Sinne des § 53 Abs. 3a Variante 3 AufenthG ist nicht im Lichte der Begründung des Gesetzesentwurfs zu § 53 Abs. 3a AufenthG dahingehend zu bestimmen, dass es sich um eine „besonders schwere Straftat“ gemäß Art. 14 Abs. 4 lit. b) Richtlinie 2011/95/EU handeln muss. Vielmehr ergibt sich aus der Gesamtschau des Wortlauts und der Absicht, die der Gesetzgeber mit der Einführung des § 53 Abs. 3a AufenthG verfolgt, dass die Anforderungen des § 53 Abs. 3a Variante 3 AufenthG kohärent mit denen nach Art. 24 Abs. 1 Richtlinie 2011/95/EU sind, nach welchem zwingende Gründe der nationalen Sicherheit oder der öffentlichen Ordnung eine Ausweisung gestatten (LSe; Rn. 110).

Das OVG Magdeburg hat mit Beschluss vom 27.01.2021 – 2 M 101/20 – entschieden: Das Tatbestandsmerkmal „Gefahr für die Allgemeinheit“ im Sinne des § 53 Abs. 3a AufenthG setzt nicht nur voraus, dass der Flüchtling wegen einer schweren Straftat verurteilt worden ist, sondern auch die Feststellung einer Verbindung zwischen der Straftat, für die er verurteilt wurde, und der Gefahr, die von ihm ausgeht. Da dem Wortlaut nach die Gefahr von dem Ausländer selbst ausgehen muss („er“), ist klargestellt, dass eine Ausweisung nur aus spezialpräventiven, nicht aber aus generalpräventiven Gründen möglich ist (LSe; Rn. 30).

IX. Ausweisungsinteresse bei (Intensiv-)Straftätern

1. Ziel

Die Neufassung des § 54 Abs. 1 Nr. 1a inkorporiert anstelle der bislang genannten Tatmittel Gewalt, Drohung mit Gefahr für Leib oder Leben oder List einen abschließenden Straftatenkatalog, der den im Normcharakter angelegten, die Annahme eines besonders schwerwiegenden Ausweisungsinteresses rechtfertigenden Rechtsgüterschutz abbildet. Durch die Neufassung sollten die Ausländerbehörden davon entlastet werden, umfangreiche Strafurteile auf die Voraussetzung durchzusehen, ob die abgeurteilten Straftaten unter Anwendung der genannten Tatmittel begangen wurden. Dies ergab sich in der Regel nicht aus dem Tenor des Urteils, sondern erforderte ein ausführliches Studium der Urteilsgründe.

Nach dem neuen § 54 Abs. 1 Nr. 1b begründen Verurteilungen zu mindestens einjährigen Freiheitsstrafen wegen Sozialleistungsbetrugs und nach dem BtMG ein besonders schwerwiegendes Ausweisungsinteresse.

In § 54 Abs. 2 Nr. 1 wurde die Mindestschwelle für ein schwerwiegendes Ausweisungsinteresse von einem Jahr auf sechs Monate Freiheitsstrafe gesenkt.

2. Ergebnisse der Länderbefragung

Nahezu alle Länder konnten durch die Neufassung des § 54 Abs. 1 Nr. 1a AufenthG – z.T. in graduell unterschiedlichem Ausmaß - eine Entlastung bei der Bearbeitung und dem Erlass von Ausweisungsverfügungen feststellen. Ein Land hebt hierbei hervor, dass die Begehungsweise nicht mehr von der Behörde aufwändig durch Urteilsauswertungen ermittelt werden muss, ein anderes, dass Ausweisungsverfügungen so auch im Klageverfahren leichter Bestand hätten. Vielfach wird von erweiterten Ausweisungsmöglichkeiten aufgrund der Novellierung berichtet.

Betreffend § 54 Abs. 1 Nr. 1b AufenthG liegen nicht in allen Ländern ausreichende Erfahrungswerte vor. Sofern dies der Fall ist, werden häufig positive Erfahrungen berichtet. Viele Länder begrüßen die ausdrückliche Normierung von BtM-Delikten; es wird ein großer Anwendungsbereich und eine Vereinfachung der Rechtsanwendung gesehen. Einzelne Länder weisen allerdings darauf hin, dass BtM-Delikte mit Freiheitsstrafe zwischen ein und zwei Jahren selten vorkämen.

Die Mehrzahl der Länder berichtet, dass durch Absenkung des Regelausweisungstatbestands des § 54 Abs. 2 Nr. 1 AufenthG von einem Jahr auf sechs

Monate Freiheitsstrafe eine Erhöhung der Zahl von Ausweisungen erreicht werden konnte. Teilweise wird berichtet, dass Ausweisungen aufgrund der unveränderten Normierung der Bleibeinteressen des Betroffenen dennoch schwer bleiben. Zwei Länder weisen darauf hin, dass bereits nach alter Rechtslage bei Verurteilungen zu Freiheitsstrafen von weniger als einem Jahr ein schwerwiegendes Ausweisungsinteresse nach § 54 Abs. 2 Nr. 9 AufenthG bestand und insofern die Absenkung des § 54 Abs. 2 Nr. 1 AufenthG für sich zu keiner Erhöhung der Ausweisungen geführt hat.

Befragt nach Problemen bei der Anwendung weisen einige Bundesländer auf schwierige Schnittstellen zum Straf- bzw. Strafprozessrecht hin. So wird etwa ausgeführt, dass nach § 31 JGG stets eine einheitliche Jugendstrafe gebildet wird (abweichend von der Gesamtstrafenbildung nach StGB). Es erfolge keine gesonderte Auswertung der einzelnen Strafmaße, so dass es nicht immer möglich sei zu erkennen, ob für den relevanten Teil der Taten eine Jugendstrafe von mindestens einem Jahr verhängt wurde.

Ferner wurde bemängelt, es bestünden Unklarheiten bei der Subsumtion unter die Voraussetzung „gegen das Eigentum“ und „serienmäßig“ (§ 54 Abs. 1 Nr. 1a lit. d)). Das Tatbestandsmerkmal „serienmäßig“ entspreche nicht der Terminologie des StGB.

Bei Gesamtstrafenbildung wegen vorsätzlicher und fahrlässiger Straftaten sei es darüber hinaus schwierig, das Strafmaß für die Vorsatztat (isoliert) festzustellen (betrifft § 54 Abs. 1 Nr. 1, 1a, Abs. 2 Nr. 1, Nr. 2 AufenthG).

Dem entsprechend wurde am häufigsten der Vorschlag unterbreitet, § 54 Abs. 1 Nr. 1a lit. d) AufenthG an die strafrechtliche Terminologie anzupassen oder das Tatbestandsmerkmal „serienmäßig“ zu definieren. Ferner sollten nach Einschätzung einiger Länder mit Blick auf § 54 Abs. 1 Nr. 1, 1a, 1b, Abs. 2 Nr. 1, 2 AufenthG Probleme bei Gesamtstrafenbildung bzw. Einheitsjugendstrafe gelöst werden.

3. Rechtsprechungsanalyse

Rechtsprechung betreffend die Änderung des § 54 AufenthG ist nicht bekannt geworden.

X. Betretens und Durchsuchungsrechte

1. Ziel

Die Absätze 5 bis 10 des § 58 AufenthG wurden auf Vorschlag der Fraktionen der CDU/CSU und SPD im parlamentarischen Verfahren eingeführt (BT-Drs. 19/10047 - Änderungsantrag S. 6).

Mit dieser Neuregelung sollte eine spezielle bundesgesetzliche Regelung für die Verwaltungsvollstreckung eingeführt werden, da es in einigen Bundesländern an einer eindeutigen Rechtsgrundlage für das Betreten und Durchsuchen von Wohnungen zum Zwecke des Auffindens des Abzuschiebenden fehlte. Entsprechende Betretens- und Durchsuchungsrechte sind vor allem bei so genannten Sofortabschiebungen (d.h. Abschiebungen ohne vorherige Haft oder Gewahrsam) bedeutsam, um eine Zuführung des Abzuschiebenden sicherstellen zu können.

Die Regelung enthält u.a. eine Ermächtigungsgrundlage zum Betreten von Wohnungen (Abs. 5) und für die Durchsuchung der Wohnung des abzuschiebenden Ausländers sowie sonstiger Personen, in deren Wohnung sich der Ausländer aufhält (Abs. 6). Darüber hinaus wird u.a. die bei Eingriffen in Art. 13 GG übliche Nachtzeitenregelung (Abs. 7) normiert.

Weitergehende Regelungen der Länder, die den Regelungsgehalt der Absätze 5 bis 9 betreffen, blieben hierbei unberührt (Abs. 10). Damit bilden die bundesrechtlichen Regelungen einen „Mindeststandard“ bei fehlenden bzw. weniger weitgehenden landesrechtlichen Regelungen.

2. Beurteilung durch die Länder

Mit Ausnahme von BE, BB, und TH liegen in allen Ländern neben der neuen bundesrechtlichen Regelung landesrechtliche Regelungen vor.

Mehrere Länder berichten, dass in bestimmten Konstellationen die landesrechtliche Regelung weitergehende Befugnisse vorsieht, etwa zur Nachtzeit. In einem Land ist nach Landesrecht die Durchsuchung auch zur Identitätsklärung erlaubt. Folglich greifen die betreffenden Länder mit Blick auf § 58 Abs. 10 AufenthG kaum auf die bundesrechtliche Regelung zurück, in vielen Fällen wird jedoch die nach Landesrecht nicht bestehende Möglichkeit der Durchsuchung bei Dritten (§ 58 Abs. 6 S. 2 AufenthG) genutzt.

Mehrere andere Länder berichten wiederum, dass die bundesrechtliche Regelung weitergehende Befugnisse einräumt als das Landesrecht. Diese Länder machen von der bundesrechtlichen Regelung umfassender Gebrauch. Diese Länder beurteilen die Anwendbarkeit der Regelung in der Praxis tendenziell positiv.

Unabhängig von Art und Umfang der landesrechtlichen Regelung kritisieren sehr viele Länder die Vorgaben des § 58 Abs. 7 S. 2 AufenthG (Durchsuchungen zur Nachtzeit) als unpraktikabel bzw. aufgrund divergierender Rechtsprechung (s.u. 2.) rechtsunsicher. Der Begriff der „Organisation der Abschiebung“ sei zu unbestimmt. Probleme ergäben sich insbesondere bei feststehenden Abflugzeiten, die nicht behördlich beeinflussbar sind. Hier sei hoher Aufwand notwendig um zu begründen, dass dies nicht unter den Begriff „Organisation der Abschiebung“ falle.

Bemängelt werden ferner Probleme bei der Rechtswegzuweisung für die Anordnung der Durchsuchung. In manchen Ländern bestehen Unklarheiten, ob die Verwaltungsgerichtsbarkeit oder die ordentliche Gerichtsbarkeit für die Anordnung zuständig ist. Das liege daran, dass die bundesrechtliche Norm keine Rechtswegzuweisung vorsieht und demnach die Anwendbarkeit ggf. bestehender landesrechtlicher Rechtswegzuweisungen problematisch sei. In der Frage, ob eine Rechtswegzuweisung an die Verwaltungsgerichtsbarkeit oder die ordentliche Gerichtsbarkeit vorzugswürdig ist, sind die Länder jedoch gespalten.

Die relative Erfolgsquote bei der Beantragung von Wohnungsdurchsuchungen nach § 58 Abs. 6, Abs. 8 S. 1 AufenthG wird von den Ländern, die die Regelung anwenden, grundsätzlich als hoch bis sehr hoch eingeschätzt. Ein gänzlich anderes Bild ergibt sich bei entsprechenden Durchsuchungsanträgen zur Nachtzeit (§ 58 Abs. 7 AufenthG). Hier wird von der weit überwiegenden Mehrzahl der rückmeldenden Länder eine geringe Erfolgsquote berichtet.

Der Aufwand für die Abfassung eines Durchsuchungsantrags auf Grundlage der neuen Regelung wird von einer Mehrzahl der Länder als erheblich eingeschätzt, abhängig von der Fallkonstellation. Die Regelung erfordere eine detaillierte Darlegung, insbesondere wenn eine Maßnahme zur Nachtzeit erforderlich ist.

Gleichwohl sehen mehrere Länder durch die Einführung eines bundeseinheitlichen Mindeststandards grundsätzlich eine Erleichterung des Auffindens des Abzuschiebenden zur Sicherstellung der Durchführbarkeit von Abschiebungsmaßnahmen. Dies betrifft insbesondere die Länder, die über keine (ausreichende) landesrechtliche Regelung verfügen.

Am häufigsten wurden folgende Änderungs- und Verbesserungsvorschläge genannt:

- Ausschluss oder Modifizierung der Nachzeitregelung des § 58 Abs. 7 S. 2 AufenthG.
- Aufnahme einer Regelung, wonach eine Durchsuchung der Wohnung des Ausländers auch zu anderen Zwecken (Identitätsklärung, Durchsuchung von Sachen des Betroffenen) möglich ist.
- Viele Länder sprachen sich ausdrücklich für die Aufnahme einer Rechtswegzuweisung in der Norm auf.

3. Rechtsprechungsanalyse

Gegenstand von Rechtsprechung ist vornehmlich die Auslegung von § 58 Abs. 7 S. 2 AufenthG. § 58 Abs. 7 S. 1 AufenthG statuiert ein grundsätzliches Verbot des Betretens und Durchsuchens zur Nachtzeit. S. 2 regelt, dass jedenfalls die Organisation der Abschiebung keine Ausnahme von diesem grundsätzlichen Verbot rechtfertigt.

In der Rechtsprechung ist eine Tendenz erkennbar, dass externe organisatorische Rahmenbedingungen, die weder durch die zuständige Behörde noch durch bei der Abschiebung beteiligte sonstige deutsche Behörden beeinflusst werden können (etwa feststehende Abflugzeiten) und damit deren Organisationsspielraum begrenzen, keine organisatorischen Gründe im Sinne der einschränkenden Regelung des § 58 Abs. 7 S. 2 AufenthG sind (so etwa Beschluss des OVG Nordrhein-Westfalen vom 24. Februar 2021 - 18 E 920/20 (Rdnr. 45); VG Trier, Beschluss vom 17. September 2019 - 11 N 4019/19.TR, VG Hamburg, Beschluss vom 1. September 2020 - 5 V 3671/20 (Rdnr. 14 ff.), VG Berlin, Beschluss vom 23. März 2021 – VG 10 M 120/21).

Gegenläufige Entscheidungen sind ergangen durch das VG Ansbach, Beschluss vom 3. Februar 2021 – AN 5X 21.00207 sowie Beschluss vom 19. Februar 2021 – AN 5X 21.00285. Diese Beschlüsse stellten darauf ab, dass die Behörde in diesem Fall die Möglichkeit gehabt habe, einen späteren Linienflug zu buchen bzw. bewerten Flugzeiten grundsätzlich als organisatorischen Aspekt der Abschiebung.

Es ist eine gerichtliche Entscheidung bekannt geworden (VG Arnsberg, Beschluss vom 11. November 2019 – 3 I 24/19), die Unklarheiten betreffend die Zuständigkeit für die gerichtliche Anordnung bestätigt. Das Verwaltungsgericht hat den Antrag auf Erlass eines Durchsuchungsbeschlusses an das zuständige Amtsgericht verwiesen. Zwar sei der Verwaltungsrechtsweg gemäß § 40 Abs. 1 S. 1 VwGO grundsätzlich eröffnet. Aus § 58 Abs. 10 AufenthG folge jedoch, dass die landesrechtliche abdrängende Sonderzuweisung zur ordentlichen Gerichtsbarkeit fortgelte (Rdnr. 43).

XI. Bessere Überwachungsmöglichkeiten für (nicht abschiebbare) Intensivstraftäter

1. Ziel

Um bessere Überwachungsmöglichkeiten für (nicht abschiebbare) Intensivstraftäter zu schaffen, wurde unter anderem § 12 Abs. 2 S. 3 AufenthG eingeführt. Dadurch kann die Aufenthaltserlaubnis insbesondere mit einer räumlichen Beschränkung versehen werden, wenn ein Ausweisungsinteresse nach § 54 Abs. 1 Nr. 1 oder 1a AufenthG besteht und dies erforderlich ist, um den Ausländer aus einem Umfeld zu lösen, welches die wiederholte Begehung erheblicher Straftaten begünstigt.

Zudem wurde mit § 56 Abs. 3 Nr. 2 AufenthG die Möglichkeit zu Verpflichtungen zur Wohnsitznahme geschaffen, wenn dies geboten erscheint, um die wiederholte Begehung erheblicher Straftaten, die zu einer Ausweisung nach § 54 Abs. 1 Nr. 1 Aufenthaltsgesetz geführt haben, zu unterbinden.

Der neue § 56 Abs. 4 S. 2 sieht die Möglichkeit vor, bislang ausdrücklich lediglich aus Gründen der inneren Sicherheit vorgesehene kontakt- und kommunikationsbeschränkende Verpflichtungen auf Intensivstraftäter zu erstrecken. Aufgrund der Eingriffstiefe dieser Maßnahmen sind diese jedoch nur zur Abwehr von Gefahren für die innere Sicherheit oder für Leib und Leben Dritter möglich.

2. Ergebnisse der Länderbefragung

Etwa die Hälfte der Länder gibt an, von den Regelungen in der Praxis Gebrauch gemacht zu haben. Häufiger zur Anwendung kommen insbesondere Maßnahmen nach § 56 Abs. 3 Nr. 2 AufenthG (Wohnsitzauflage). Einzelne Länder haben von der Möglichkeit des § 12 Abs. 2 S. 3 AufenthG (räumliche Beschränkung) und nach § 56 Abs. 4 S. 2 AufenthG (Kontaktbeschränkungen/-verbote) Gebrauch gemacht.

Die Rückmeldungen durch die Länder zu Erfahrungen und Anwendbarkeit der Regelungen fallen knapp und divergierend aus. Teilweise wird von erheblichen Defiziten bei der Befolgung der Maßnahmen durch den Betroffenen und fehlende Möglichkeiten zur Kontrolle bzw. Sanktionierung berichtet.

Mehrere Länder berichteten, dass durch die Neufassungen das Ziel der gezielten Kontrolle und Überwachung gefährlicher Ausländer grundsätzlich verbessert werden konnte. Ein Land

berichtete über eine Ausländerbehörde, die mittels der Maßnahmen den BtM-Handel eindämmen konnte.

Den Rückmeldungen von zwei Ländern ist zu entnehmen, dass Änderungs- und Verbesserungspotenzial insbesondere in der Ermöglichung von Sanktionen bei Verstößen, etwa straf- und leistungsrechtlicher Art, gesehen werden.

3. Rechtsprechungsanalyse

Rechtsprechung zur Auslegung der o.g. Vorschriften ist nicht bekannt geworden.

XII. Reduktion des Beteiligungserfordernisses der Staatsanwaltschaft bei Ausweisung/Abschiebung von Straftätern

I. Ziel

Um die Ausweisung und Abschiebung bei Ausländern, gegen die öffentliche Klage erhoben oder ein strafrechtliches Ermittlungsverfahren eingeleitet wurde, praktikabler zu gestalten, wurden die Beteiligungserfordernisse der Staatsanwaltschaft bei Ausweisung/Abschiebung von Straftätern reduziert.

Hierzu wurde der Katalog der Straftaten nach § 72 Abs. 4 S. 5, bei denen ein „geringer Unrechtsgehalt“ i.S.d.§ 72 Abs. 4 S. 3 vorliegt und ein Einvernehmen der Staatsanwaltschaft unter den weiteren gesetzlichen Voraussetzungen nicht erforderlich ist, um Straftatbestände erweitert, die mit den bislang erfassten Tatbeständen mit geringem Unrechtsgehalt vergleichbar sind und gehäuft Gegenstand von Ermittlungsverfahren oder öffentlichen Klagen sind.

Die Straftaten mit geringem Unrechtsgehalt müssen zudem nicht mehr eine begleitende Straftat im Zusammenhang mit einer aufenthaltsrechtlichen Straftat sein. Für den Verzicht auf das Einvernehmen kommt es allein auf den geringeren Unrechtsgehalt an.

2. Ergebnisse der Länderbefragung

Während ein Teil der Länder eine Erleichterung bzw. Beschleunigung der Verfahren aufgrund der Neuregelung bejaht, kann ein anderer Teil der Länder keinen spürbaren Entlastungseffekt feststellen. Dies ist teilweise bedingt durch geringe praktische Erfahrungen, zum Teil fällt die Erleichterung aufgrund der bereits bestehenden guten Zusammenarbeit mit den Staatsanwaltschaften nicht merklich ins Gewicht, zum Teil werden die Änderungen als zu wenig weitgehend angesehen (s.u.).

Die allermeisten Länder plädieren dafür, das Einvernehmenserfordernis in Ausweisungsfällen zu streichen

Ein sehr großer Teil der Länder fordert darüber hinaus auch bei Abschiebungen weitergehende Erleichterungen; der größte Teil favorisiert hierbei eine Widerspruchs- bzw. Fristenlösung, vereinzelt wird auch vorgeschlagen, das Einvernehmenserfordernis nur noch bei schweren Straftaten vorzusehen oder dieses ganz abzuschaffen.

Manche Länder schlagen operative Verfahrenserleichterungen wie einen Zugriff auf das bzw. die Einsicht in das Staatsanwaltschaftliche Verfahrensverzeichnis (ZStV) oder die Schaffung einer zentralen Ansprechstelle bei der Staatsanwaltschaft vor.

Einige Länder schlagen vor, einzelne bzw. beide Rückausnahmen in § 72 Abs. 4 S. 5 a.E. zu streichen, da diese die durch die Neuregelung gewonnene Erleichterung deutlich relativierten. Da in der ausländerbehördlichen Praxis gerade Personen vielfach in kurzer Zeit mehrfach einschlägig strafrechtlich in Erscheinung treten würden, plädieren diese Länder insbesondere für eine Ausweitung der Erleichterungen auf mehrfach begangene einschlägige Straftaten.

3. Rechtsprechungsanalyse

Der BGH hat mit Beschluss vom 12.02.2020 – XIII ZB 15/19 – entschieden, dass allein das Fehlen eines nach § 72 Abs. 4 S. 1 AufenthG erforderlichen Einvernehmens der Staatsanwaltschaft nicht zur Rechtswidrigkeit einer Abschiebungshaftanordnung führt.

Soweit der Bundesgerichtshof in bisher ständiger Rechtsprechung unter Verweis auf Art. 104 Abs. 1 S. 1 GG angenommen hat, das Einvernehmen der Staatsanwaltschaft stelle eine essentielle Haftvoraussetzung dar und es komme insoweit allein auf die objektive Rechtslage an, hält der nunmehr zuständige XIII. Zivilsenat daran nicht fest.

Bei dem Beteiligungserfordernis nach § 72 Abs. 4 S. 1 AufenthG handele es sich nicht um eine freiheitsschützende Verfahrensvorschrift in diesem Sinne. Dies ergebe sich aus der Gesetzgebungsgeschichte, aus dem Wortlaut der Norm und aus ihrer systematischen Stellung im Aufenthaltsgesetz.

XIII. Vorläufige Anwendungshinweise des BMI

1. Ziel

Die Vorläufigen Anwendungshinweise dienen der sachgerechten Anwendung des Aufenthaltsgesetzes. Sie sollen insbesondere Hinweise zum Umgang mit komplexen Regelungen bieten und dadurch eine Hilfestellung für die mit dem Vollzug des Aufenthaltsrechts betrauten Behörden sein.

2. Ergebnisse der Länderbefragung

Die Vorläufigen Anwendungshinweise des BMI zu § 60b, 62 und 62b AufenthG werden in allen Ländern verwendet. Während etwa ein Drittel Länder sogar auf eigene Anwendungshinweise verzichtet, hat der Großteil der Länder darüber hinaus noch eigene Anwendungshinweise oder Handreichungen erarbeitet oder ergänzende Weisungen erlassen.

Insgesamt fließen die Anwendungshinweise als Hilfsmittel in die tägliche Arbeit der Ausländerbehörden mit ein und haben sich insoweit bewährt.

In einem Land wird gänzlich darauf verzichtet, die Anwendungshinweise zu § 60b AufenthG den Ausländerbehörden zur Verfügung zu stellen. Begründet wird dies damit, dass man dort – anders als das BMI in Nr. 1.9 der Vorläufigen Anwendungshinweise - § 60b Abs. 1 S. 2 AufenthG so lese, dass die Abschiebung allein aus vom Ausländer selbst zu vertretenden Gründen nicht möglich sein dürfe.

Ergänzungsbedarf wird insbesondere in Bezug auf die Anwendungshinweise zu § 60b AufenthG gesehen. So sind aus Sicht einzelner Länder etwa Hinweise zum notwendigen Umfang von Mitwirkungshandlungen bzw. zu den Folgen von lediglich kurzfristigen Mitwirkungshandlungen wünschenswert. Darüber hinaus wünschen sich einzelne Länder Konkretisierungen zur Mitwirkung in bestimmten familiären Konstellationen sowie zur Frage der konkret zumutbaren Mitwirkungshandlungen. Darüber hinaus wird um Klarstellung gebeten, dass § 72 Abs. 1 Nr. 1 AsylG der Aufforderung zur Passpapierbeschaffung bei einer Person, die vollziehbar ausreisepflichtig in einem Asylstreitverfahren ist, nicht entgegensteht.

XIV. Weitere Erfahrungen beim Vollzug des Aufenthaltsrechts

Die Länder wurden auch gefragt, ob sie Erfahrungen und Erkenntnisse beim Vollzug der einschlägigen Vorschriften des Aufenthaltsrechts (§ 11, §§ 50 – 62b AufenthG) gesammelt haben, die im Übrigen zu berücksichtigen wären. Rund die Hälfte der Länder hat hierzu Anregungen gemacht.

Befragt zu weiterem Verbesserungsbedarf in diesem Bereich, haben drei Viertel der Länder entsprechende Anregungen übermittelt.

Die von den Ländern übermittelten Angaben sind in der Anlage 3 zu diesem Bericht beigefügt.

Anlagen

Anlage 1: Zwischenbericht des BMI zu TOP 29 Ziffer 2 und 3 der 211. Innenministerkonferenz vom 4. bis 6. Dezember 2019 in Lübeck zu dem Thema „Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht“

Anlage 2: Fragebogen anlässlich des Erfahrungsberichts zum Zweiten Gesetz zur verbesserten Durchsetzung der Ausreisepflicht

Anlage 3: Änderungs- und Verbesserungsvorschläge der Länder

Anlage 4: Zahlen zur Erteilung der Duldung für Personen mit ungeklärter Identität

Anlage 1: Zwischenbericht – Auszug aus dem Gesamtbericht des BMI zu TOP 29 Ziffer 2 und 3 der 211. Innenministerkonferenz vom 4. bis 6. Dezember 2019 in Lübeck

Gesamtbericht des BMI zu TOP 29 Ziffer 2 und 3
der 211. Innenministerkonferenz vom 4. bis 6. Dezember 2019 in Lübeck
zu den Themen
„Umsetzung des Zweiten
Gesetzes zur besseren Durchsetzung der Ausreisepflicht - Zwischenbericht“,
„Personalaufwuchs bei den Sicherheitsbegleitern der BPol“,
„Sachstand bei der Übernahme der Dublin-Überstellungen durch den Bund“
und
„Pass-/Passersatzpapierbeschaffung durch den Bund“

Die Innenministerkonferenz hat das Bundesministerium des Innern, für Bau und Heimat gebeten, zu den Themen „*Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht - Zwischenbericht*“, „*Personalaufwuchs bei den Sicherheitsbegleitern der BPol*“, „*Sachstand bei der Übernahme der Dublin-Überstellungen durch den Bund*“ und „*Pass-/Passersatzpapierbeschaffung durch den Bund*“ zu berichten.

Hierzu nimmt das Bundesministerium des Innern, für Bau und Heimat wie folgt Stellung:

Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht - Zwischenbericht

Die IMK hat auf ihrer 211. Sitzung vom 04. bis 06.12.19 in Lübeck unter TOP 29 „Verbesserung der Durchsetzung von Ausweisungen und Abschiebungen bei straffälligen Ausländern / Flüchtlingen und Gefährdern“, Ziffer 2, beschlossen, das BMI zu bitten, ihr über den AK I bis zur Herbstsitzung 2020 einen Zwischenbericht und bis zur Herbstsitzung 2021 einen Abschlussbericht über die Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht unter Einbeziehung der AG IRM vorzulegen.

Das Zweite Gesetz zur besseren Durchsetzung der Ausreisepflicht trat am 21.08.2019 in Kraft. Seine Regelungen sollen den für die Rückführung zuständigen Behörden eine effektivere Durchsetzung der Ausreisepflicht ermöglichen. Das Bundesministerium des Innern, für Bau und Heimat hat den für den Vollzug der entsprechenden Regelungen im Wesentlichen zuständigen Ländern in der Folge nähere Hinweise zur Umsetzung der Kernvorschriften des Gesetzes in Form von Vorläufigen Anwendungshinweisen an die Hand gegeben. So wurden entsprechende Anwendungshinweise für die Haftregelungen (§§ 62 und 62b AufenthG) und die neue Duldung für Personen mit ungeklärter Identität (§ 60b AufenthG, § 105 AufenthG) erstellt und am 17.12.2019 und 14.04.2020 an die Länder übermittelt. Darüber hinaus wurden zentrale Fragen der Anwendung des Gesetzes, beispielsweise zu Durchsuchungsrechten in der Wohnung des Abzuschiebenden zur Nachtzeit und zur Dauer der Ausnahme von Asylantragstellern von der Passbeschaffungspflicht, unter anderem in der 5. Sitzung der AG IRM am 17./18. September 2019 erörtert.

Das BMI hat, dem Berichtsauftrag entsprechend, ein Konzept (Anlage I) sowie einen Fragebogen (Anlage II) zur Erhebung der für die Bewertung der Umsetzung des Zweiten Gesetzes zur besseren Durchsetzung der Ausreisepflicht erforderlichen Informationen erstellt. Konzept und Fragebogen wurden bereits im Vorfeld von der AG IRM im schriftlichen Umlaufverfahren gebilligt.

Die Erhebung der erforderlichen Informationen und Daten soll sich auf die Kernpunkte des Geordnete-Rückkehr-Gesetzes beziehen und insbesondere die nachfolgenden Regelungen umfassen:

- die Neustrukturierung der Regelungen zum Einreise- und Aufenthaltsverbot in § 11 AufenthG
- der neue Duldungstatbestand für Personen mit ungeklärter Identität
- praktikablere Ausgestaltung der Sicherungshaft
- Neueinführung der Mitwirkungshaft
- praktikablere Ausgestaltung des Ausreisegewahrsams
- temporäre Aufhebung des Trennungsgebots
- Erleichterung der Voraussetzungen für die Ausweisung von Straftätern

- Schaffung eines bundesgesetzlichen „Mindeststandards“ für das Betreten und Durchsuchen von Wohnungen
- bessere Überwachungsmöglichkeiten für (nicht abschiebbare) Intensivstraftäter
- Reduktion des Beteiligungserfordernisses der Staatsanwaltschaft bei Ausweisung/Abschiebung von Straftätern

Die Datenerhebung bei der Erstellung des Berichts soll allein anhand qualitativer Daten (Expertenbefragungen, Rechtsprechungsauswertung) – ergänzt durch begrenzt im AZR abrufbare Daten - erfolgen. Dieses Vorgehen wurde nach entsprechender Prüfung durch das BMI und unter Beteiligung der AG IRM gewählt, da es ermöglicht, unterschiedliche Anwendungsphasen des Gesetzes zu berücksichtigen - unabhängig von den bei einer quantitativen Datenerhebung bestehenden Erhebungs- und Vergleichsschwierigkeiten.

Hierbei auschlaggebend war vor allem die einhellige Feststellung, dass von einem „regulären“ Rückkehrgeschehen innerhalb des zu untersuchenden Zeitraums nur in der Zeit zwischen September 2019 und Februar 2020 ausgegangen werden kann. Die ersten Wochen nach dem Inkrafttreten des GRG müssen hierbei als „Anlaufphase“ gewertet werden, so dass für diesen Zeitraum nicht davon ausgegangen werden kann, dass dort bereits praktische Erfahrungen erkenntnisbringend gesammelt werden konnten.
Darüber hinaus ist in der Folgezeit der massive Einfluss der COVID19-Pandemie auf den gesamten Vollzug des Aufenthaltsrechts und insbesondere das Rückkehrgeschehen zu berücksichtigen, das im Laufe der Monate März und in Folge mangels Flugverbindungen, persönlicher Vorsprachemöglichkeiten in den Auslandsvertretungen und aufgrund infektiologischer Restriktionen der Herkunftsländer massiv beeinträchtigt wurde. So kann bis heute von einer Normalisierung der Lage noch nicht annähernd gesprochen werden. Auch sind die anhaltenden Auswirkungen der COVID19-Pandemie auf das gesamte Rückkehrgeschehen nach wie vor nicht absehbar.

Vor diesem Hintergrund ist eine quantitative retrospektive Erhebung der abzubildenden Anwendungsfälle innerhalb dieses stark eingeschränkten Zeitfensters

nur mit erheblichem Aufwand, der bis hin zu händischen Nacherfassungen reichen würde, verbunden. Darüber hinaus sind auch vergleichbare Daten nicht realistisch zu generieren, da u.a. die zur Bewertung der Neuregelungen notwendigen Daten in den seltensten Fällen zentral abrufbar vorliegen und auch das Ausländerzentralregister zu entscheidenden Neuregelungen keine Informationen zur Häufigkeit der Anwendung der o.g. Regelungen vorhält.

Aus den vorgenannten Gründen soll daher der Erhebungszeitraum die Zeit seit Inkrafttreten des GRG bis einschließlich Mai 2021 umfassen. Grundsätzlich soll eine Auswertung der vorhandenen und zugänglichen Rechtsprechung und Literatur zu den Neuregelungen des GRG erfolgen. Die im AZR vorhandenen Daten sollen gesichtet und im Falle einer Verwertbarkeit für den Erfahrungsbericht herangezogen und ausgewertet werden. Parallel dazu soll der eingangs erwähnte Fragebogen an einen durch die Länder zu bestimmenden Expertenkreis aus den für das Aufenthaltsrecht und dessen Vollzug zuständigen Behörden versandt werden. Dieser soll anhand teilstandardisierter Fragen die Erfahrungen mit dem GRG abfragen.
Auf der Grundlage dieser gesammelten Erkenntnisse soll der erbetene Erfahrungsbericht erstellt werden, der neben der Darstellung des Ist-Zustandes auch Korrektur- und Verbesserungsbedarf für die Zukunft skizzieren soll.

[…]

Bundesministerium des Innern, für Bau und Heimat

AZ: R1-20010/5#32 Berlin, den 13.01.2021

Fragebogen anlässlich des Erfahrungsberichts zum Zweiten Gesetz zur verbesserten Durchsetzung der Ausreisepflicht

Mit dem vorliegenden Fragebogen sollen die bisher mit den Regelungen des Zweiten Gesetzes zur verbesserten Durchsetzung der Ausreisepflicht gemachten Erfahrungen erfragt werden.

In die Beantwortung der Fragen sollte der Zeitraum vom 21.08.2019 bis 31.05.2021 einbezogen werden. Die Antworten können in elektronischer Form direkt in den Fragebogen eingetragen werden.

Um Beantwortung des Fragebogens bis zum 30.06.2021 wird gebeten.

Ausfüllende Stelle: **Klicken oder tippen Sie hier, um Text einzugeben.**

Durch das Geordnete-Rückkehr-Gesetz soll der Vollzug der Ausreisepflicht insbesondere abgelehnter Asylbewerber und Asylbewerberinnen verbessert werden; Ziel war es vor allem, gesetzliche Erleichterungen zu schaffen, um Ausländerbehörden von ausufernden Vorgaben zu entlasten und somit auch auf der operativen Ebene Fortschritte zu ermöglichen.

Daher wurden u.a. folgende Neuerungen geschaffen, deren Rezeption und Umsetzung in den Ländern nachfolgend erfragt werden soll:

- die Neustrukturierung der Regelungen zum Einreise- und Aufenthaltsverbot in § 11 AufenthG
- der neue Duldungstatbestand für Personen mit ungeklärter Identität
- Praktikablere Ausgestaltung der Sicherungshaft
- Neueinführung der Mitwirkungshaft
- Praktikablere Ausgestaltung des Ausreisegewahrsams

- Temporäre Aufhebung des Trennungsgebots
- Erleichterung der Voraussetzungen für die Ausweisung von Straftätern
- Schaffung eines bundesgesetzlichen „Mindeststandards“ für das Betreten und Durchsuchen von Wohnungen
- Bessere Überwachungsmöglichkeiten für (nicht abschiebbare) Intensivstraftäter
- Praktikablere Reduktion des Beteiligungserfordernisses der Staatsanwaltschaft bei Ausweisung/Abschiebung von Straftätern

Über die Umsetzung dieser Neuerungen soll anhand Ihrer Beantwortung der nachfolgenden Fragen im Rahmen eines Erfahrungsberichtes an die Innenministerkonferenz berichtet werden.

I. Allgemeine Fragen

a) Das Zweite Gesetz zur Verbesserung der Ausreisepflicht brachte für die Ausländerbehörden in der Umstellungsphase naturgemäß zunächst viel Mehrarbeit. Wurde nach dieser Umstellung Ihrer Einschätzung nach die Arbeit der Ausländerbehörden durch die Neuregelungen vereinfacht, erschwert oder ist sie gleichgeblieben?
Können Sie dies kurz begründen?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Welche Neuregelungen schätzen Sie als besonders positiv ein? Können Sie dies kurz begründen?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Welche Neuregelungen schätzen Sie als besonders negativ ein? Können Sie dies kurz begründen?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Halten Sie weitere Rechtsänderungen für erforderlich?
☐ Nein ☐ Ja
Falls ja, welche?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Haben sich die Neuregelungen insgesamt als in der Praxis anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

II. Einreise- und Aufenthaltsverbot (§ 11 AufenthG)

a) Hat die Neustrukturierung der Regelung, insbesondere der Fristenregelungen in Abs. 5 bis Abs. 5b, die Anwendungspraxis erleichtert?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Wird von der Möglichkeit eines unbefristeten Einreise- und Aufenthaltsverbots für Intensivstraftäter nach § 11 Abs. 5b S. 2 AufenthG Ihrer Erfahrung nach Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Hat sich die Neuregelung als in der Praxis anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

III. Duldung für Personen mit ungeklärter Identität (§ 60b AufenthG)/Besondere Passbeschaffungspflicht (§ 60 b Abs. 2 S. 1 AufenthG)/Sanktionen (§ 60b Abs. 5 AufenthG)

a) Wird von der Regelung des § 60b AufenthG in der Praxis Gebrauch gemacht?
Wenn zurückhaltend: aus welchen Gründen?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Welche Erfahrungen haben Sie bisher mit der Regelung gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Hat sich genannte Regelung als in der Praxis anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Konnte aus Ihrer Sicht eine Steigerung der Fälle, in denen sich Ausländer aufgrund der Rechtsänderung selbst um Reisedokument bemühen, festgestellt werden?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Haben Sie von der Möglichkeit der Verhängung von Bußgeldern bei fehlender Mitwirkung Gebrauch gemacht?
☐ Nein ☐ Ja

f) Hat sich die sanktionierende Rechtswirkung der eingeschränkten Duldung als geeignet zur Verbesserung der Kooperationsbereitschaft der Ausländer bei der Beschaffung von Pässen oder Passersatzpapieren erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

g) Hat sich die sanktionierende Rechtswirkung der eingeschränkten Duldung als insgesamt geeignet zur Effektivierung des Rückführungsverfahrens erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

h) Sehen Sie das Ziel des Gesetzgebers, durch die „Duldung für Personen mit ungeklärter Identität “ zwischen regulären Duldungsinhabern und solchen Ausländern, die ihre Mitwirkung verweigern, besser differenzieren zu können, verwirklicht?
Klicken oder tippen Sie hier, um Text einzugeben.

i) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

IV. Sicherungshaft – neue Tatbestände und Indizien (§ 62 Abs. 3a und 3b AufenthG)

a) Welche Erfahrungen haben Sie bisher mit den neuen Vermutungstatbeständen (§ 62 Abs. 3a AufenthG) und Indizien (§ 62b Abs. 3b AufenthG) gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Hat sich die neu eingebrachte Vermutungsregelung als in der Praxis anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Konnte durch die Vermutungsregelung eine Entlastung für die Ausländerbehörden aufgrund des verringerten Prüfaufwandes herbeigeführt werden?
Können Sie dies kurz begründen?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Von welchen Tatbeständen des § 62 Abs. 3a wird häufiger Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.
Was ist aus Ihrer Sicht hierfür ursächlich?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Von welchen Tatbeständen des § 62 Abs. 3a wird weniger häufig Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.
Was ist aus Ihrer Sicht hierfür ursächlich?
Klicken oder tippen Sie hier, um Text einzugeben.

f) Von welchen Tatbeständen des § 62 Abs. 3b wird häufiger Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.
Was ist aus Ihrer Sicht hierfür ursächlich?
Klicken oder tippen Sie hier, um Text einzugeben.

g) Von welchen Tatbeständen des § 62 Abs. 3b wird weniger häufig Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.
Was ist aus Ihrer Sicht hierfür ursächlich?
Klicken oder tippen Sie hier, um Text einzugeben.

h) Wie hoch schätzen Sie anhand Ihrer Erfahrungen die die relative Erfolgsquote der beantragten Fälle von Sicherungshaft? Hat sich diese nach Ihren Erfahrungen im Vergleich zur alten Rechtslage gesteigert?
Klicken oder tippen Sie hier, um Text einzugeben.

i) Wie schätzen Sie den Aufwand für die Abfassung eines Haftantrags nach der neuen Rechtslage im Vergleich zur alten Rechtslage ein?
Klicken oder tippen Sie hier, um Text einzugeben.

j) Konnte durch die Neuregelung eine Verbesserung im Vollzug der Abschiebungen erreicht werden?

Klicken oder tippen Sie hier, um Text einzugeben.

k) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

V. Mitwirkungshaft (§ 62 Abs. 6 AufenthG)

a) Wird von der Regelung in der Praxis Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Welche Erfahrungen haben Sie bisher mit der Regelung gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Hat sich die Einführung der Mitwirkungshaft in der Praxis als anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Wie hoch schätzen Sie anhand Ihrer Erfahrungen die die relative Erfolgsquote der Mitwirkungshaft?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Wie schätzen Sie den Aufwand für die Abfassung eines entsprechenden Haftantrags?
Klicken oder tippen Sie hier, um Text einzugeben.

f) Konnte durch diese Neuregelung eine Verbesserung mit Blick auf die Durchführung von Mitwirkungshandlungen erreicht werden?
Klicken oder tippen Sie hier, um Text einzugeben.

g) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

VI. Ausreisegewahrsam (§ 62b AufenthG)

a) Konnte durch die Klarstellung, dass Fluchtgefahr nicht erforderlich ist, die praktische Arbeit der Ausländerbehörden erleichtert werden?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Konnte durch Vermutungsregelungen des § 62b Abs. 1 S. 1 Nr. 3 AufenthG die praktische Arbeit der Ausländerbehörden erleichtert werden?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Von welcher Vermutungsregelung wird häufig Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

Was ist aus Ihrer Sicht hierfür ursächlich?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Von welcher Vermutungsregelung wird selten Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

Was ist aus Ihrer Sicht hierfür ursächlich?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Welche Erfahrungen haben Sie insgesamt bisher mit der Regelung gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

f) Hat sich die Neufassung des Ausreisegewahrsams in der Praxis als anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

g) Wie hoch schätzen Sie anhand Ihrer Erfahrungen die relative Erfolgsquote bei der Beantragung des Ausreisegewahrsams ein? Hat sich diese im Vergleich zur alten Rechtslage nach Ihren Erfahrungen gesteigert?
Klicken oder tippen Sie hier, um Text einzugeben.

h) Wie schätzen Sie den Aufwand für die Abfassung eines entsprechenden Haftantrags im Vergleich zur alten Rechtslage ein?
Klicken oder tippen Sie hier, um Text einzugeben.

i) Konnte durch die Neufassung des Ausreisegewahrsams die Zuführung zur Abschiebung insgesamt verbessert werden?
Klicken oder tippen Sie hier, um Text einzugeben.

j) Wo sehen Sie noch einen Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

VII. Aussetzen des Trennungsgebots (§ 62a Absatz 1 AufenthG)

a) Wird von dieser Regelung in Ihrem Bundesland Gebrauch gemacht?
☐ Ja ☐ Nein

b) Welche Erfahrungen haben Sie bisher mit der Regelung gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Konnte durch diese Neuregelung eine Entspannung der Haftplatzsituation erreicht werden?
Klicken oder tippen Sie hier, um Text einzugeben.

VIII. Absenkung Ausweisungsschutz für Straftäter (§ 53 AufenthG)

a) Hat sich die Absenkung des Ausweisungsschutzes für Straftäter mit Schutzstatus gem. § 53 AufenthG als in der Praxis anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Welche Erfahrungen haben Sie bisher mit der Regelung gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

IX Ausweisungsinteresse bei (Intensiv-)Straftätern (§ 54 Abs. 1 Nr. 1a, 1b, Abs. 2 Nr. 1 AufenthG)

a) Konnten durch die Neufassung des § 54 Abs. 1 Nr. 1 a AufenthG die Ausländerbehörden bei der Bearbeitung und dem Erlass von Ausweisungsverfügungen entlastet werden?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Welche Erfahrungen haben Sie bei der Feststellung eines besonders schwerwiegenden Ausweisungsinteresses nach § 54 Abs. 1 Nr. 1b AufenthG gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Konnte durch die Absenkung des Regelausweisungstatbestands des § 54 Abs. 2 Nr. 1 AufenthG von einem Jahr auf sechs Monate eine Erhöhung der Zahl von Ausweisungen herbeigeführt werden?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Welche Probleme sind aufgetreten?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

X. Betretens- und Durchsuchungsrechte nach § 58 Abs. 5-10 AufenthG

a) Liegen in Ihrem Bundeland neben den speziellen bundesgesetzlichen Regelungen landesrechtliche Regelungen vor?
☐ Ja ☐ Nein

Falls ja, welche?
Klicken oder tippen Sie hier, um Text einzugeben.

Sind diese (z.T.) weitergehend als der bundesrechtliche Mindeststandard? Wenn zum Teil, welche Regelungen?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Wird von der bundesrechtlichen Regelung in der Praxis Gebrauch gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Hat sich die Regelung insgesamt in der Praxis als anwendbar erwiesen?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Welche Erfahrungen haben Sie bisher mit der Regelung gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Wie hoch schätzen Sie anhand Ihrer Erfahrungen die relative Erfolgsquote bei der Beantragung von Wohnungsdurchsuchungen (§ 58 Abs. 6, Abs. 8 S. 1 AufenthG) ein?
Klicken oder tippen Sie hier, um Text einzugeben.

f) Wie hoch schätzen Sie anhand Ihrer Erfahrungen die Erfolgsquote bei entsprechenden Durchsuchungsanträgen zur Nachtzeit (§ 58 Abs. 7 AufenthG) ein?
Klicken oder tippen Sie hier, um Text einzugeben.

g) Wie schätzen Sie den Aufwand für die Abfassung eines entsprechenden Durchsuchungsantrages ein?
Klicken oder tippen Sie hier, um Text einzugeben.

h) Konnte durch diese Regelung das Ziel des erleichterten Auffindens des Abzuschiebenden zur Sicherstellung der Durchführbarkeit von Abschiebungsmaßnahmen verbessert werden?
Klicken oder tippen Sie hier, um Text einzugeben.

i) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

XI. Maßnahmen gegen (Intensiv-)Straftäter, die nicht abgeschoben werden können (§ 12 Abs. 2 S. 3, § 56 Abs. 3 Nr. 2, Abs. 4 S. 2 AufenthG)

a) Wird von den Regelungen in der Praxis Gebrauch gemacht? Wenn in unterschiedlicher Weise: von welcher mehr, von welcher weniger?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Welche Erfahrungen haben Sie bisher mit den Regelungen gemacht?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Haben sich die Maßnahmen gegen (Intensiv-)Straftäter, die nicht abgeschoben werden können, in der Praxis als anwendbar erwiesen?
Wenn in unterschiedlicher Weise: welche mehr, welche weniger?
Klicken oder tippen Sie hier, um Text einzugeben.

d) Konnte durch diese Neufassungen das Ziel der gezielten Kontrolle und Überwachung gefährlicher Ausländer verbessert werden?
Klicken oder tippen Sie hier, um Text einzugeben.

e) Wo sehen Sie noch einen Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

XII. Beteiligungserfordernis der Staatsanwaltschaft (§ 72 Abs. 4 S. 4 AufenthG)

a) Inwieweit konnte durch die Änderung, dass die Straftaten nach dem Strafgesetzbuch nunmehr keine begleitende Straftat mehr sein müssen und der Katalog der Straftaten "mit

geringem Unrechtsgehalt" erweitert wurde, die Arbeit der Ausländerbehörden erleichtert und der Vollzug von Abschiebungen beschleunigt werden?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Wo sehen Sie noch Änderungs- oder Verbesserungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

XIII. Vorläufige Anwendungshinweise des BMI zu § 60b, 62 und 62b AufenthG

a) Inwieweit arbeiten die Ausländerbehörden mit den Vorläufigen Anwendungshinweisen des BMI?

b) Wurden von den Ländern eigene Anwendungshinweise erstellt?
☐ Ja ☐ Nein

Wenn ja, welche?
Klicken oder tippen Sie hier, um Text einzugeben.

c) Haben sich die Vorläufigen Anwendungshinweise des BMI bewährt oder sehen Sie noch weiteren Ergänzungsbedarf?
Klicken oder tippen Sie hier, um Text einzugeben.

XIV. Weitere Erfahrungen beim Vollzug des Aufenthaltsrechts

a) Haben Sie weitere Erfahrungen und Erkenntnisse zum Vollzug der einschlägigen Vorschriften des Aufenthaltsrechts (§ 11, §§ 50 – 62b AufenthG) im Hinblick auf Rückkehr- und aufenthaltsbeendende Aspekte, die Ihrer Meinung nach zukünftig zu berücksichtigen sind?
Klicken oder tippen Sie hier, um Text einzugeben.

b) Sehen Sie in anderen Bereichen des Vollzugs des Aufenthaltsrechts (§ 11, §§ 50 – 62b AufenthG) im Hinblick auf Rückkehr- und aufenthaltsbeendende Aspekte weiteren Verbesserungsbedarf?
☐ Ja ☐ Nein

Wenn ja, welchen?
Klicken oder tippen Sie hier, um Text einzugeben.

Änderungs- und Verbesserungsvorschläge der Länder

Einreise- und Aufenthaltsverbot, § 11 AufenthG

- Anpassung von § 84 Abs. 1 Satz 1 Nr. 7 AufenthG an den geänderten § 11 Abs. 1 Satz 1 AufenthG
- Klarstellung in § 11 Abs. 5a S. 4 AufenthG, ob das Einvernehmen der obersten Landesbehörde nur für den Fall einer nachträglichen Verkürzung der Soll-Frist einzuholen ist, oder auch wenn bereits beim erstmaligen Erlass von der Soll-Frist abgewichen werden soll
- Anpassung des § 11 Abs. 5b S. 2 AufenthG dahingehend, dass der gesamte § 54 Abs. 1 AufenthG erfasst wird, aber auch nicht nur unbefristete EAVs zugelassen werden, sondern z.B. auch ein solches zwischen 10 und 20 Jahren (ähnlich der Rechtsprechung zum alten Ausweisungssystem (§ 53 a.F.=15 Jahre, §54 a.F.=10 Jahre, § 55 a.F.=5 Jahre)
- Beweislastumkehr ab einer gewissen Strafhöhe (5 Jahre analog § 6 Abs. 5 FreizügG/EU), so dass der Betroffene zu gegebener Zeit nachweisen muss, dass von seiner Person keine Gefahr ausgeht
- Schaffung eines § 54 Abs. 1 Nr. 2 AufenthG vergleichbaren Ausweisungstatbestands für der organisierten und Clan-Kriminalität angehörige, nicht notwendig vorbestrafte Ausländer und Aufnahme dieses Tatbestands in § 11 Abs. 5b AufenthG, um ein entsprechend langes EAV verfügen zu können
- Klarstellung in § 11 Abs. 4 S. 2 AufenthG, ob die Aufhebung des EAVs unter der Bedingung "nur für Titel nach Kap. 2 Abschn. 5 des AufenthG" erfolgen soll/darf
- Regelung der örtlichen Zuständigkeit für Anträge auf nachträgliche Befristung eines EAVs, welche im Kontext eines erneuten Visumantrags stehen, um die Beteiligung der sachnahen Ausländerbehörde sicherzustellen
- Einführung von Regelbeispielen für Fristen, die sich nach Straftatbeständen bzw. gestaffeltem Ausweisungsinteresse richten
- Grobe Orientierung des Aufenthaltsverbots am Strafmaß

- Leitfaden, der die Bestimmung der Dauer der Verbote erleichtert bzw. Anwendungshinweise des BMI hinsichtlich der Fristanwendung
- Bezugnehmend auf § 11 AufenthG sollte keine Zuweisung mehr in den Zuständigkeitsbereich der ABH erfolgen, die die Ausreise vollzogen hat.

Duldung für Personen mit ungeklärter Identität, 60b AufenthG

- Umbenennung des § 60b AufenthG, da auch identifizierte Personen die Passbeschaffungspflicht verletzten können
- Erstreckung der besonderen Passbeschaffungspflicht nach § 60b Abs. 2 AufenthG
    - auf Asylbewerber, deren Antrag als oU abgelehnt wurde, um beschleunigte Aufenthaltsbeendigung zu fördern.
    - auf Ausländer mit Abschiebungsverboten nach § 60 Abs. 5 AufenthG (subsidiär Schutzberechtigte), da nach Rechtsprechung Beantragung von Dokumenten bei Heimatbotschaft nicht per se unzumutbar.
    - auf alle vollziehbar Ausreisepflichtigen, da Identifizierungspflicht bereits im Asylverfahren besteht und um Kohärenz zu § 60a Abs. 6 Nr. 2 AufenthG zu schaffen.
    - auf Personen, deren Aufenthaltsgestattung nach § 67 AsylG erloschen ist.
- Erweiterung des § 60b AufenthG auf Fälle passiver Renitenz.
- Gesetzliche Klarstellung, dass die fehlende Kooperation nicht allein kausal für die mangelnde Rückkehraussicht sein muss.
- Präzisierung Verhältnis von § 48 AufenthG zu § 60b AufenthG.
- Genauere Definition, welche Handlungen im Rahmen von § 60b Abs. 3 AufenthG als zureichend zur Erfüllung der Passbeschaffungspflicht angesehen werden (oft auch HKL-spezifisch unterschiedlich), ggf. in Vorläufigen Anwendungshinweisen.
- Kriterienkatalog des § 60b Abs. 3 AufenthG weiter fassen.
- Zurechnung der Verletzung von Mitwirkungspflichten durch Erziehungsberechtigte ermöglichen.
- Abschaffung der Möglichkeit der eidesstattlichen Erklärung als Mittel der Glaubhaftmachung/Änderung von § 60b Abs. 3 S. 4 AufenthG.

- Zentrale Anlaufstelle/konkrete Vermittlung von herkunftslandspezifischen Besonderheiten.
- Erweiterung des Katalogs der sanktionierenden Rechtswirkungen in § 60b Abs. 5 AufenthG. Im Einzelnen:
    - Automatismus zu Leistungskürzungen nach § 1a AsylbLG,
    - stärkere Leistungseinschränkungen,
    - automatische räumliche Beschränkungen,
    - Titelerteilungssperren.
- Verweis in § 98 Abs. 3 Nr. 5b AufenthG auf § 60b Abs. 1 S. 2 AufenthG korrigieren (korrekt: § 60b Abs. 2 S. 1).
- Abschaffung des Widerspruchsverfahrens.
- Bessere und zügigere Kooperation mit den Herkunftsländern.
- Regelung einer generellen Beschäftigungsmöglichkeit für Ausreisepflichtige.
- Integrationsperspektiven nicht (zu schnell) abschneiden.
- Weitere Möglichkeiten für Ausreisepflichtige, die bereits Integrationserfolge vorweisen können, Wege in das Bleiberecht zu eröffnen, v.a. über Ausbildungs- und Beschäftigungsduldung.
- Gesondertes Dokument für die Duldung nach § 60b AufenthG.

Sicherungshaft, § 62 Abs. 3a und 3b AufenthG

- Verstöße gegen Einreise- und Aufenthaltsverbote sollten als eigenständiger Haftgrund normiert werden
- Abschiebungshaft soll auch ermöglicht werden, wenn die Aufenthaltsbeendigung erst innerhalb von sechs Monaten möglich ist
- Senkung der Nachweis-/Begründungspflicht für Abschiebungshaftanträge; insbesondere hinsichtlich des Gefahrenbegriffs
- Erweiterte Vermutungsregelungen i.V.m. mit einer Ist-Vorschrift zur Reduzierung des Prüfaufwands
- Eindeutigere Formulierung der Voraussetzungen für die Haft, um zu verhindern, dass sie z.B. durch unhaltbare Aussagen des Betroffenen im Rahmen der Anhörung [wie etwa die Bereitschaft zur (freiwilligen) Ausreise] widerlegt werden können.

- Schaffung eines neuen Haftgrunds „erhebliche Gefahr für sexuelle Selbstbestimmung“ in § 62 Abs. 3b Nr. 3 AufenthG
- Änderung des § 62 Abs. 3 b Nr. 4 AufenthG dahingehend, dass auch Geldstrafen von mehr als 50 Tagessätzen als Anhaltspunkt für eine Fluchtgefahr ausreichen
- Aufnahme eines eigenen Katalogs an Tatbeständen betreffend die Fluchtgefahr im Dublinverfahren, um eine Vermischung der Dublinhaft (§ 2 AufenthG Abs. 14 AufenthG) mit § 62 AufenthG zu vermeiden (HE) bzw. Entzerrung des § 2 Abs. 14 AufenthG und Einordnung in § 62 AufenthG
- Änderung des § 2 Abs. 14 Nr. 2 AufenthG dahingehend, dass eine mehrfache Asylantragstellung ausreichend ist, unabhängig davon, ob der Staat vorher verlassen wurde, um Nr. 1 und Nr. 2 klar zu unterscheiden
- Einführung einer automatischen Verlängerung der Abschiebungshaft um 48 Stunden, wenn eine Abschiebung wegen Verhinderungshandlungen des Betroffenen scheitert (z.B. Randale im Flugzeug)
- Ausweitung der Regelung des § 62 Abs. 3 S. 3 AufenthG auf einen längeren Zeitraum
- Beibehaltung der Ausnahmeregelung des § 62a AufenthG.
- Erweiterung des Anwendungsbereichs des § 14 Abs. 3 AsylG auf Folgeanträge (insofern Verweis in § 71 Abs. 8 AsylG)
- Zustellungserleichterungen in Anlehnung an § 10 AsylG, insbesondere zur Vermeidung der Notwendigkeit, den Sicherungshaftantrag gegen Unterschrift bzw. nach dem jeweiligen Verwaltungszustellungsgesetz aushändigen zu müssen
- Einführung eines wirksamen Rechtsbeschwerderechts der Behörde im FamFG
- Einführung einer Regelung im FamFG, wonach der konkrete Abschiebungstermin nicht im Haftbeschluss genannt werden darf (analog § 59 Abs. 1 S. 8 AufenthG)
- Schaffung der Möglichkeit für eine planbare Haft durch einstweilige Anordnung ohne vorherige Anhörung (§ 427 FamFG)
- Schaffung einer einheitlichen Regelung zur Hafttauglichkeit
- Schaffung besserer Informationsflüsse
- Verkürzung der Asylverfahren bzw. Beschleunigung des Rechtsbehelfsverfahrens
- Erhöhung der Anzahl bzw. Bereitstellung von Abschiebungshaftplätzen
- Vereinfachung hinsichtlich der vorzunehmenden Übersetzungen der wichtigsten Passagen in die jeweilige Muttersprache des betroffenen Ausländers
- Herausgabe von standardisierten Belehrungsmustern und Übersetzungen

Mitwirkungshaft, § 62 Abs. 6 AufenthG

- Unterbringung der von der Mitwirkungshaft Betroffenen in der - gemessen am Vorführungsort - räumlich nächsten JVA
- Regelung der Problematik, dass die von der Mitwirkungshaft betroffene Person schon bei Vorladung gem. § 82 Abs. 4 S. 1 AufenthG in der jeweiligen Muttersprache zur Möglichkeit der Inhaftnahme belehrt werden muss (problematisch insb. bei Altfällen, in denen keine Belehrung, aber eine Vorladung erfolgte)
- Schaffung der Möglichkeit der Mitwirkungshaft auch ohne zuvor gescheiterte Vorführung bei der Botschaft aufgrund langer Wartezeiten für Botschaftsvorführungen
- Bereitstellung von Muster-Formulierungsvorschlägen für Mitwirkungshaftanträge zur Vereinheitlichung der Verfahrensweise

Ausreisegewahrsam, 62b AufenthG

- Streichung des § 62b Abs. 1 S. 2 AufenthG
- Klarstellung der Voraussetzungen in § 62b Abs. 2 AufenthG, die für die Gewahrsamseinrichtung gelten, z.B. hinsichtlich der Formulierung „ohne Zurücklegen einer größeren Entfernung“, explizite Auflistung einer Abschiebungshafteinrichtung als Unterbringungsmöglichkeit, oder Klarstellung, dass eine direkte Ausreisemöglichkeit in den Zielstaat von dem Flughafen nicht erforderlich ist
- Verlängerung der maximalen Dauer für Ausreisegewahrsam nach § 62b AufenthG auf 28 Tage (Zeitraum, für den gemäß § 14 Abs. 3 S. 3 AsylG die Abschiebungshaft nach Stellung eines Asylantrages weiter aufrecht gehalten werden darf), bzw. auf 14 Tage, 1 Monat
- Einführung eines wirksamen Rechtsbeschwerderechts der Behörde (trotz § 70 Abs. 3 S. 3 FamFG wegen BGH-Beschluss vom 22.10.2015 –V ZB 169/14 - keine Möglichkeit der Fortsetzung eines in der Hauptsache erledigten Freiheitsentziehungsverfahrens)

- Beschleunigung der Rechtsmittelverfahren und bessere Abstimmung mit den Herkunftsstaaten zur Rücknahme von abgelehnten Asylbewerbern zur Förderung der freiwilligen Ausreise
- Verbesserung der Verfügbarkeit von Haftplätzen

Absenkung Ausweisungsschutz für Straftäter (§ 53 AufenthG)

- Stringentere Orientierung an den unionsrechtlichen Vorgaben (BY, BW, SN)
- Der Rechtsbegriff „schwere Straftat“ in § 53 Abs. 3b AufenthG soll definiert werden
- Korrektur des Redaktionsversehens in § 53 Abs. 4 S. 2 Nr. 1 AufenthG: bestehender Verweis auf Abs. 3 wurde nicht angepasst
- Absenkung des Ausweisungsschutzes auch in § 53 Abs. 3 AufenthG
- Ausweisung als unmittelbare Rechtsfolge des Widerrufs des Schutzstatus
- gesetzliche Festlegung des entscheidungserheblichen Zeitpunks für den Bestand einer Ausweisungsverfügung bei gerichtlicher Überprüfung auf den Zeitpunkt der letzten behördlichen Entscheidung

Ausweisungsinteresse bei (Intensiv-)Straftätern, § 54 Abs. 1 Nr. 1a, 1b, Abs. 2 Nr. 1 AufenthG

- In § 54 Abs. 1 Nr. 1 AufenthG sollte auch die Maßregel der Unterbringung in einem psychiatrischen Krankenhaus nach § 63 StGB aufgenommen werden
- Normierung der Ausweisungsinteressen bei Einheitsjugendstrafe (betrifft § 54 Abs. 1 Nr. 1, 1a, 1b, Abs. 2 Nr. 2 AufenthG)
- Anpassung des § 54 Abs. 1 Nr. 1a lit. d) AufenthG an strafrechtliche Terminologie oder Orientierung an § 54 Abs. 1 Nr. 1a lit. c) AufenthG oder Begriffsdefinition „serienmäßig“
- Ergänzung des § 54 Abs. 1 Nr. 1a lit. d) um Straftaten gegen das Vermögen
- § 54 Abs. 2 Nr. 2 AufenthG: Reduzierung auf rechtskräftige Verurteilung zu mindestens 6 Monaten Jugendstrafe ohne Bewährung (vgl. § 54 Abs. 2 Nr. 1 AufenthG)
- Regelung für nachträgliche gebildete Gesamtfreiheitsstrafen (betrifft § 54 Abs. § 54 Abs. 1 Nr. 1, 1a, 1b, Abs. 2 Nr. 1, 2 AufenthG)

Betretens- und Durchsuchungsrechte, § 58 Abs. 5-10 AufenthG

- Schaffung einer eindeutigen Rechtsgrundlage für die Durchsuchung der Wohnräume, um das Auffinden von identitätsklärenden Dokumenten zu ermöglichen
- Klarstellende Rechtsnorm zur Durchsuchung von Wohnungen zum Auffinden von Datenträgern
- Ausschluss oder Modifizierung der Nachzeitregelung
- Aufnahme einer Regelung, wonach eine Durchsuchung der Wohnung des Ausländers auch zu anderen Zwecken (Identitätsklärung, Durchsuchung von Sachen des Betroffenen) möglich ist
- Klarstellende Regelung, dass eine Duldung der Durchsuchung nicht entgegensteht
- Konkretisierung in § 58 Abs. 8 S. 2 AufenthG, dass die Annahme von Gefahr im Verzug nicht „allein“ darauf gestützt werden kann, dass der Ausländer nicht angetroffen wurde
- Votum der Länder für Rechtswegzuweisung
    - An ordentliche Gerichtsbarkeit (entsprechend BRat-Drs. 504/20 und 665/20): BE, HE, NW, SL, SN, SH, TH
    - An Verwaltungsgerichtsbarkeit: BW, BB, HB

Maßnahmen gegen (Intensiv-)Straftäter, die nicht abgeschoben werden können (§ 12 Abs. 2 S. 3, § 56 Abs. 3 Nr. 2, Abs. 4 S. 2 AufenthG)

- Beseitigung von Unklarheiten bei Maßnahmen bei bedingten Ausweisungen nach § 53 Abs. 4 AufenthG
- Gesetzliche Definition des Tatbestandsmerkmals „Bezirk der Ausländerbehörde“ in § 56 Abs. 2 AufenthG
- Die abweichende Bestimmung in § 56 Abs. 1 S. 1 Hs 2 AufenthG sowie die abweichende Festlegung in § 56 Abs. 2 Hs 2 AufenthG sollten gesetzlich für sofort vollziehbar erklärt werden
- Eindeutige Zuständigkeitsregelung für verwaltungsrechtliche Anordnungen bei Manipulationen an Fußfesseln
- Sanktionen straf- und leistungsrechtlicher Art bei Verstoß gegen Maßnahmen

Beteiligungserfordernisse der Staatsanwaltschaft, §72 Abs. 4 S.4 AufenthG

- Schaffung einer Widerspruchs-/„Fristenlösung“ bei bestimmten Straftaten, bei der das Einvernehmen der Staatsanwaltschaft als erteilt gilt, wenn nicht innerhalb einer Frist Widerspruch erhoben wird.
- Abschiebungsinteresse sollte das Strafverfolgungsinteresse grundsätzlich überwiegen
- Das Einvernehmen der Staatsanwaltschaft sollte nur noch bei schweren Straftaten erforderlich sein
- Abschaffung des Einvernehmenserfordernisses der Staatsanwaltschaft vor einer Ausweisung
- Streichung der Rückausnahmen in § 72 Abs. 4 S. 5 AufenthG a. E.
- Wegfall des Beteiligungserfordernisses der Staatsanwalt, wenn mehrere Ermittlungsverfahren bzw. Klagen wegen gleicher Straftaten mit geringem Unrechtgehalt (Beispiel: Ladendiebstahl § 242 StGB) begangen wurden
- Schaffung einer bundeseinheitlichen Leitlinie, in welchen Fällen von Einstellungen nach der StPO das Einvernehmenserfordernis besteht
- Schaffung einer Zentralstelle in der Justiz für die Erteilung des Einvernehmens
- Normierung einer Schnittstelle bzw. eines zentralen Ansprechpartners bei der Staatsanwaltschaft für ausländerrechtliche Fragestellungen
- Eindeutige örtliche Zuordnung zu Staatsanwaltschaften und Gerichten bei orts- bzw. länderübergreifenden Fällen

Sonstige Vorschläge zur Verbesserung rückkehrbezogener Aspekte des Aufenthaltsgesetzes

- Allgemein sollten die Vorschriften des Aufenthaltsrechts übersichtlicher gestaltet werden
- Abschiebungen bei nicht geklärter Identität und Nichtmitwirkung bei der Passbeschaffung sollten ermöglicht werden
- Schaffung des Rechtsinstituts einer „ausländerrechtlichen Verwarnung“
- Gesetzliche Regelung der Verbandskompetenz in Bezug auf Sachentscheidungen
- Schaffung einer gesetzlichen Regelung zur Datenübermittlungsbefugnis von Leistungsbehörden und Ärzten/Kliniken an Ausländerbehörden hinsichtlich

Behandlungen und Befundberichten zur Planung der Abschiebung bzw. zur Feststellung inlandsbezogener Abschiebungshindernisse

- Normierung des Vorrangs der freiwilligen Rückkehr im AufenthG
- Für ausländerbehördliche Verfügungen ist nach § 48 Abs. 3 AufenthG ein gesetzlicher Sofortvollzug vorzusehen, um eine rasche Aufenthaltsbeendigung vorantreiben zu können
- Schaffung einer Rechtsgrundlage zur Durchsuchung von Personen nach monetären Mitteln zur Begleichung von Abschiebungskosten
- Klarstellung in § 48 Abs. 3a, dass die dort gewährte Befugnis auch das Auslesen von Daten einer Cloud umfasst und Erweiterung der Auswertungsbefugnis auf Bedienstete auch ohne Befähigung zum Richteramt
- Schaffung von Sanktionsmöglichkeiten bei Missachtung des § 50 Abs. 4 AufenthG.
- Ergänzung des § 50 Abs. 6 S. 1 AufenthG um den Zusatz „…oder solange ein die Freiheit entziehender richterlicher Beschluss besteht.“, um Personen bei einer einstweiligen Anordnung von Abschiebehaft bzw. Ausreisegewahrsam in den Fahndungspool der Polizei aufnehmen zu können
- Gesetzliche Anordnung des Sofortvollzugs auch für Abs. 1 und Abs. 2 in § 56 Abs. 5 S. 2 AufenthG.
- Klarstellung im Rahmen des § 58 Abs. 4 AufenthG dahingehend, welcher Zeitraum der Ingewahrsamnahme bei Abschiebungen zulässig ist
- § 59 Abs. 3 S. 2 AufenthG sollte durch folgenden Regelung ersetzt werden: „Sofern ein Abschiebungsverbot vorliegt, ist die Abschiebung nach § 60a Abs. 2 S. 3 AufenthG auszusetzen, solange dieses Abschiebungsverbot vorliegt.“
- Klarstellung, dass bei Wiederaufgreifensanträgen nach § 60 Abs. 5 und 7 AufenthG keine aufschiebende Wirkung hinsichtlich Vollzugsmaßnahmen eintritt
- Überarbeitung des § 60a Abs. 2c und 2d.
- Reform des § 60a Abs. 5 S. 4 AufenthG
- Im Hinblick auf die Kostenpflicht des Ausländers nach § 66 AufenthG und um jegliche finanzielle Anreize für Abzuschiebende zu minimieren, sollte die Höhe des Überbrückungsgeldes – vordringlich bei ausgewiesenen Straftätern – an dem zu erwartenden Bedarf im Heimatland angepasst werden können

- Änderung des § 84 Abs. 1 S. 1 Nr. 2, 2a oder Nr. 3 AufenthG in der Form, dass Widerspruch und Klage auch gegen andere „Nebenbestimmungen“ zur Duldung keine aufschiebende Wirkung zukommt
- Streichung des Wortes „wiederholt“ in § 95 Abs.1 Nr. 6a AufenthG
- gesetzliche Klärung, auf welcher Rechtsgrundlage die Ausländerbehörden bei Beantragung von Abschiebungshaft die Untersuchung der Gewahrsamsfähigkeit oder eine Corona-Testung anordnen darf (§ 46 Abs. 1 AufenthG?)

Vorschläge zur Änderung rückkehrbezogener Bestimmungen des Asylgesetzes

- Ergänzungsbedarf in § 14 Abs. 3 AsylG
    - Abschaffung der systemwidrigen Privilegierung von Folgeantragstellern, da Asylerstantragsteller nach Stellung eines Asylantrags gemäß § 14 Abs. 3 AsylG in Abschiebungshaft verbleiben, aber Asylfolgeantragsteller gemäß § 71 Abs. 3 AsylG aus der Abschiebungshaft entlassen werden müssen, wenn ein weiteres Folgeverfahren durchgeführt wird.
    - Klarstellung, dass ein Antrag nach § 33 Abs. 5 S. 2 AsylG dem Erstantrag in § 14 Abs. 3 AsylG gleichgestellt ist.
- Ergänzung des § 14 Abs. 3 AsylG um Polizeigewahrsam und behördlichen Gewahrsam im Sinne des § 62 Abs. 5 S. 1 AufenthG. Anpassung des § 15 AsylG, so dass die Identitätstäuschung als Straftat verfolgt werden kann
- Anpassung des § 71 Abs. 5 AsylG an die RL 2013/32/EU
- Redaktionelle Korrektur des § 34a Abs. 2 Satz 3 AsylG (Ersetzung des Wortes „Befristung“ durch „Anordnung“)

Vorschläge zur Verbesserung des operativen Vollzugs des Aufenthaltsgesetzes

- Einführung eines nationalen Visahebels für unkooperative Staaten
- Die Möglichkeit, die europäischen Passersatzdokumente für Rückführungen anzuwenden, sollte erweitert werden
- Schaffung eines schnelleren Verfahrens bei der Passersatzbeschaffung sowie einer besseren Kontrolle des Einreise- bzw. Aufenthaltsverbots im Rahmen des Dublin-III-Abkommens.

- Sicherheitsbegleitung bei jeder Abschiebung
- Berücksichtigung der Vorschläge der Unterarbeitsgruppe Vollzugsdefizite der AG Rück, u.a. Fortsetzung der zentralisierten Unterstützung von Rückkehrmaßnahmen durch das ZUR

Anlage 4: Zahlen zur Erteilung der Duldung für Personen mit ungeklärter Identität

Entwicklung der erfassten Inhaber einer Duldung für Personen mit ungeklärter Identität		
Stichtag	**Erfasste Personen zum Stichtag**	**Erstmalige Erteilung im jeweiligen Monat**
31.08.2020	108	97
30.09.2020	2708	2004
31.10.2020	6286	3158
30.11.2020	9530	3073
31.12.2020	12697	2799
31.01.2021	14903	2388
28.02.2021	16653	2117
31.03.2021	17988	1986
30. 04.2021	19319	1905
31.05.2021	20646	1876
30.06.2021	21683	1683

Erteilte Duldung für Personen mit ungeklärter Identität zum 30.06.2021 nach Bundesländern	
Gesamt	**21.683**
davon:	
Baden-Württemberg	1.345
Bayern	4.712
Berlin	434
Brandenburg	629
Bremen	62
Hamburg	81
Hessen	1.888
Mecklenburg-Vorpommern	809
Niedersachsen	1.608
Nordrhein-Westfalen	4.339
Rheinland-Pfalz	885
Saarland	42
Sachsen	2.087
Sachsen-Anhalt	2.220
Schleswig-Holstein	305
Thüringen	237

Erteilte Duldung für Personen mit ungeklärter Identität zum 30.06.2021 nach Staatsangehörigkeiten	
Staatsangehörigkeiten gesamt	21.683
darunter:	
Nigeria	1.915
Indien	1.635
Pakistan	1.561
Iran, Islamische Republik	1.421
Libanon	1.149
Äthiopien	1.101
Ungeklärt	986
Russische Föderation	956
Afghanistan	699

Bundesministerium
des Innern, für Bau
und Heimat

Cybersicherheitsstrategie für Deutschland 2021

Bundesministerium
des Innern, für Bau
und Heimat

Impressum

Herausgeber
Bundesministerium des Innern, für Bau und Heimat

Kontaktinformationen
Bundesministerium des Innern, für Bau und Heimat
Alt-Moabit 140
10557 Berlin
Tel.: +49 (0)30 18 681-0
E-Mail: CSS2021@bmi.bund.de

Stand
August 2021

1 Inhaltsverzeichnis

2 Zusammenfassung (Management Summary)

Die „Cybersicherheitsstrategie für Deutschland 2021“ bildet vorbehaltlich der Verfügbarkeit entsprechender Haushaltsmittel den strategischen Rahmen für das Handeln der Bundesregierung im Bereich der Cybersicherheit für die nächsten fünf Jahre.

Ausgangspunkt der Strategie ist eine Analyse der Bedrohungslage. Diese ist gekennzeichnet durch eine deutliche sowohl qualitative als auch quantitative Zunahme von Cyberangriffen, eine wachsende Angriffsfläche und neuartige Bedrohungsszenarien. Zudem steigt die potenzielle Schadenshöhe.

Sodann wird ein Überblick über die Institutionen gegeben, die in Deutschland einen Beitrag zur Cybersicherheit leisten. Die Cybersicherheitslandschaft umfasst zivilgesellschaftliche, wissenschaftliche, wirtschaftliche und staatliche Initiativen und Akteure.

Auf Grundlage der Analyse der Ausgangslage werden für die Cybersicherheitsstrategie 2021 vier übergreifende Leitlinien definiert:

1. „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“,
2. „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken“,
3. „Digitalisierung sicher gestalten“ und
4. „Ziele messbar und transparent ausgestalten“.

Diese Leitlinien beschreiben Aspekte, die alle vier folgenden Handlungsfelder der Cybersicherheitsstrategie betreffen. Die Ausrichtung der strategischen Ziele der Handlungsfelder anhand der Leitlinien gewährleistet ihr kohärentes Ineinandergreifen.

In Handlungsfeld 1, „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“, werden die Bürgerinnen und Bürger beziehungsweise die Gesellschaft in den Mittelpunkt der Betrachtung gerückt. Die zehn strategischen Ziele des Handlungsfeldes sollen dazu beitragen, dass Bürgerinnen und Bürger die Chancen digitaler Technologien nutzen und sich hierbei sicher und selbstbestimmt in einer digitalisierten Umgebung bewegen können. Hierfür sehen die strategischen Ziele vor, Bürgerinnen und Bürger zu sensibilisieren, deren Cyberkompetenz zu steigern und den Verbraucherschutz in der digitalen Welt zu stärken. Zudem werden Regulierungsvorhaben beschrieben, die den Rahmen für selbstbestimmtes Handeln verbessern sollen.

Das Handlungsfeld 2 trägt die Überschrift „Gemeinsamer Auftrag von Staat und Wirtschaft“. Die 13 dort verorteten strategischen Ziele sollen die Cybersicherheit in der Wirtschaft insgesamt stärken, legen aber auch einen Fokus auf Kritische Infrastrukturen (KRITIS). Daneben werden insbesondere kleine und mittlere Unternehmen (KMU) in den Blick genommen. Die Ziele sehen vor, die vertrauensvolle und enge Zusammenarbeit zwischen Staat und Wirtschaft weiter auszubauen und die regulatorischen Rahmenbedingungen für die Wirtschaft fortzuentwickeln. Ziele, die die Förderung von Schlüssel- und Zukunftstechnologien zum Inhalt haben, sollen die Digitale Souveränität und die Wettbewerbsfähigkeit der Unternehmen im Bereich Cybersicherheit ausbauen.

Die staatlichen Akteure der Cybersicherheit und die notwendigen Entwicklungen in diesem Bereich werden in Handlungsfeld 3, „Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“, in den Blick genommen. Die Ziele in diesem Handlungsfeld lassen sich drei Bereichen zuordnen: 1. Kompetenzverteilung und Zusammenarbeit zwischen den Behörden, 2. Fortentwicklung von Fähigkeiten und Befugnissen der Behörden und 3. neue Herausforderungen für staatliche Akteure im Cyberraum. Die 14 strategischen Ziele des Handlungsfeldes sollen insbesondere Barrieren einer effektiven Zusammenarbeit zwischen den Behörden abbauen und die sich stetig wandelnden Anforderungen im Cyberraum aufzeigen, für deren Erfüllung die Behörden mit ausreichenden Fähigkeiten und Befugnissen ausgestattet sein müssen.

Die Gewährleistung eines hohen Cybersicherheitsniveaus in Deutschland erfordert auch eine „aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik“. Dies wird in Handlungsfeld 4 mit insgesamt sieben strategischen Zielen adressiert. Zentral ist dabei das Engagement Deutschlands in der Europäischen Union (EU) und in der Organisation des Nordatlantikvertrages (NATO). Während Fragen der Harmonisierung von Regelungen im Rahmen des Gemeinschaftsrechts in allen Handlungsfeldern zu finden sind, befassen sich die Ziele dieses Handlungsfeldes mit der Weiterentwicklung der Grundlagen und Instrumentarien der Cybersicherheitspolitik dieser Organisationen. Darüber hinaus sollen das internationale Regelwerk für Staaten im Cyberraum und die internationale Bekämpfung von Cyberkriminalität gestärkt werden. Auch Ziele der bilateralen Zusammenarbeit und vertrauensbildende Maßnahmen sind Gegenstand von Handlungsfeld 4.

Die Cybersicherheitsstrategie schließt mit der Darstellung eines transparenten Ansatzes für Umsetzung, Berichtwesen und Controlling der Strategie. Die Wirksamkeit der Umsetzung soll kontinuierlich verfolgt und überprüft werden. Zukünftige Evaluierungen werden systematisch vorbereitet.

3 Einleitung

Unsere Zeit ist geprägt von den neuen Möglichkeiten einer digitalisierten Welt. Technologien wie Künstliche Intelligenz (KI), vernetzte elektronische Geräte und neue innovative Kommunikationskanäle bringen große Veränderungen mit sich. Viele unserer alltäglichen Aufgaben, unabhängig ob im privaten, beruflichen oder behördlichen Kontext, werden durch neue Technologien erleichtert und beschleunigt. Immer mehr Prozesse verlagern sich in den Cyberraum. Die COVID-19-Pandemie hat dieser Entwicklung einen weiteren Schub gegeben.

Mit den zunehmenden Möglichkeiten können sich jedoch auch die Risiken im Cyberraum ändern oder vermehren. Um alle Chancen, Vorteile und Notwendigkeiten der Digitalisierung vollumfänglich ausschöpfen zu können, ist es zwingend erforderlich, sich vor diesen Risiken zu schützen. Der Staat hat die Pflicht, die rasanten Entwicklungen der Digitalisierung so im Interesse der Bürgerinnen und Bürger gemeinsam mit Wirtschaft, Wissenschaft und Zivilgesellschaft zu bewerten und aktiv zu gestalten, dass die erforderlichen Rahmenbedingungen für ein hohes Maß an Sicherheit und Schutz im Cyberraum gewährleistet werden.

Die Bürgerinnen und Bürger müssen Technologien auch zukünftig stets sicher, frei und selbstbestimmt nutzen können. Die Cyber- und Informationssicherheit ist kein notwendiges Übel, sondern Garant dafür, dass Digitalisierung nachhaltig erfolgreich ist.

Die von der Bundesregierung beschlossenen Cybersicherheitsstrategien für Deutschland aus den Jahren 2011[1] und 2016[2] bildeten wesentliche Weichenstellungen für eine zukunftsgerichtete Cybersicherheitspolitik.

So wurden beispielsweise für den Nationalen Cybersicherheitsrat (NCSR), das Nationale Cyber-Abwehrzentrum (Cyber-AZ) oder die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) in den Strategien die Grundlagen gelegt. Die Umsetzung von Zielen wie „Digitale Kompetenz bei allen Anwendern fördern“, „Kritische Infrastrukturen sichern“, „Strafverfolgung im Cyberraum intensivieren“ oder „Cybersicherheit international aktiv mitgestalten“ hat in den Strategien ihren Ausgangspunkt.

An diese Entwicklung knüpft die Cybersicherheitsstrategie 2021 an. Die darin beschriebenen Leitlinien, Maßnahmen und Ziele bilden die Grundlage für ein sicheres Deutschland im Cyberraum in den kommenden Jahren.

Cyber- und Informationssicherheit betrifft Staat, Wirtschaft, Wissenschaft und Gesellschaft gleichermaßen. Deshalb adressiert die Strategie alle Akteure und bindet sie ein.

---

[1] Abrufbar unter: https://www.cio.bund.de/Web/DE/Strategische-Themen/IT-und-Cybersicherheit/Cyber-Sicherheitsstrategie-fuer-Deutschland/cyber_sicherheitsstrategie_node.html

[2] Abrufbar unter: https://www.bmi.bund.de/cybersicherheitsstrategie/

Die Cybersicherheit ist eine Aufgabe der Gegenwart, aber auch eine der wichtigsten Aufgaben für die Zukunft. Verstärkt werden deshalb Schwerpunkte auf Zukunfts- und Schlüsseltechnologien gelegt.

Die deutsche Wirtschaft ist zukünftig noch stärker darauf angewiesen, im Cyberraum zu agieren. Transformationen sind in vollem Gange, beispielhaft seien hier Industrie 4.0 und Arbeiten 4.0 genannt. Diese müssen nachhaltig durch die Cyber- und Informationssicherheit abgesichert werden. Hierzu führt die Strategie die bewährte enge Zusammenarbeit von Staat und Wirtschaft fort und intensiviert diese in Form eines noch engeren Austauschs, eines verbesserten Schutzes und der Förderung sicherer Produkte und Dienstleistungen.

Aber auch die staatliche Cybersicherheitsarchitektur ist auf den Prüfstand zu stellen und zeitgemäß fortzuentwickeln.

Außerdem beabsichtigt die Bundesregierung, ihr Engagement auf europäischer und internationaler Ebene noch weiter auszubauen, und setzt verstärkt auf die Zusammenarbeit sowie ein koordiniertes Handeln mit ihren Partnern.

Nicht nur thematisch, auch strukturell wurde die Cybersicherheitsstrategie weiterentwickelt. Im Rahmen einer umfassenden Evaluierung unter Einbindung der Bundesministerien und ihrer Geschäftsbereichsbehörden, der Länder, von Wirtschaftsvertretern und von Vertretern der Zivilgesellschaft wurde festgestellt, dass sich die bisher definierten vier Handlungsziele „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“, „Gemeinsamer Auftrag Cybersicherheit von Staat und Wirtschaft“, „Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“ sowie „Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik“ bewährt haben und sie weiterhin Bestand haben. Sie haben Querschnittscharakter und betreffen alle gesellschaftlichen Bereiche, unter die sich alle erforderlichen Maßnahmen subsumieren lassen. Gleichzeitig wurden Themen wie „Digitale Souveränität“ identifiziert, die neu als Querschnittsthemen in allen Handlungsfeldern berücksichtigt werden müssen. Leitlinien führen durch die Fortschreibung der vorliegenden Cybersicherheitsstrategie, um ein Ineinandergreifen der einzelnen strategischen Ziele und Maßnahmen zu gewährleisten.

Als weitere wesentliche Neuerung gegenüber der letzten Cybersicherheitsstrategie soll die Umsetzung der Strategie kontinuierlich verfolgt und überprüft werden. Hierzu sind alle strategischen Ziele mit definierten Indikatoren hinterlegt, anhand derer der Erfolg der Strategie nachvollziehbar kontrolliert werden kann.

4 Zielstellung der Cybersicherheitsstrategie 2021

Die „Cybersicherheitsstrategie für Deutschland 2021“ ersetzt die „Cybersicherheitsstrategie für Deutschland 2016“. Sie bildet den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung im Bereich Cybersicherheit für die nächsten fünf Jahre. Sie ist eine Fortschreibung, die inhaltlich auf Bewährtem der Strategien aus den Jahren 2011 und 2016 aufbaut und gleichzeitig neue Schwerpunkte setzt.

Die Strategie beschreibt die grundsätzliche, langfristige Ausrichtung der Cybersicherheitspolitik der Bundesregierung in Form von Leitlinien, Handlungsfeldern sowie strategischen Zielen. Sie hat einen aktiven gestaltenden Charakter und soll ein zielgerichtetes und abgestimmtes Zusammenwirken aller Akteure ermöglichen und fördern. Die Cybersicherheitsstrategie für Deutschland und die Cybersicherheitsstrategien der Länder ergänzen sich dabei gegenseitig und intensivieren damit die föderale Zusammenarbeit. Eingebettet in die Europäische Cybersicherheitsstrategie[3] trägt die Cybersicherheitsstrategie für Deutschland zudem auch zur Gestaltung der digitalen Zukunft Europas bei.

Der Steuerungsrahmen gemäß der NIS-Richtlinie[4] ist Bestandteil der Strategie. Wie in der Richtlinie gefordert, bilden die strategischen Ziele die Prioritätensetzungen der Bundesregierung ab, zudem werden in Kapitel 6 „Die Cybersicherheitslandschaft in Deutschland“ die Akteure der Cybersicherheitslandschaft benannt.

Die Cybersicherheitsstrategie

- beschreibt den Rahmen, in dem die Bundesregierung ihre Aktivitäten entfalten wird;
- schafft Transparenz und Nachvollziehbarkeit für alle Akteure aus Staat, Wirtschaft, Wissenschaft und Gesellschaft,
- fördert das aktive, zielgerichtete Zusammenwirken dieser Akteure,
- berücksichtigt die Vorgaben der EU,
- verankert ein Berichtswesen und Controlling auf strategischer Ebene und
- bereitet zukünftige Evaluierungen und eine kontinuierliche Weiterentwicklung systematisch vor.

Die Umsetzung der Ziele der Cybersicherheitsstrategie steht unter dem Vorbehalt der Verfügbarkeit entsprechender im Haushaltsplan veranschlagter Haushaltsmittel. Das Prinzip der Wirt-

[3] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020JC0018

4 Die NIS-Richtlinie gibt den Mitgliedstaaten vor, dass sie in der Strategie einen Steuerungsrahmen schaffen müssen (siehe Art. 7 Abs. 1 lit. b Richtlinie (EU) 2016/1148). Dieser muss eine Bestimmung enthalten, (i) wie die Ziele und Prioritäten der Strategie zu erreichen sind und (ii) welche staatliche Institution oder Private für deren Erreichung verantwortlich sind. Die Richtlinie ist abrufbar unter: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:32016L1148

schaftlichkeit und Sparsamkeit (vergleiche § 7 Bundeshaushaltsordnung für den nationalen Haushalt) gilt entsprechend für den Haushalt der EU, soweit dieser in Anspruch genommen werden sollte.

Die Cyber- und Informationssicherheit grenzt an zahlreiche weitere Themen an und überschneidet sich teilweise mit diesen. Zu einigen dieser Themenstellungen hat die Bundesregierung eigene Strategien veröffentlicht. Diese werden in der Cybersicherheitsstrategie referenziert und überblicksartig erläutert, um ein Gesamtverständnis zu ermöglichen.

Die Themen hybride Bedrohungen und Datenschutz haben besonders große Schnittmengen mit der Cyber- und Informationssicherheit und müssen daher stets mitberücksichtigt werden. Der Themenbereich der hybriden Bedrohungen wird im Kapitel 5 „Cyberbedrohungslage“ einer genauen Betrachtung unterzogen.

Die Überschneidungen von Datenschutz und Cyber- und Informationssicherheit werden dadurch deutlich, dass zahlreiche Schutzziele des Datenschutzes auch für die Cyber- und Informationssicherheit Bedeutung haben. Seit dem Jahr 2018 stellen die Datenschutz-Grundverordnung[5] und die Richtlinie für den Datenschutz in den Bereichen Polizei und Justiz[6] auf europäischer Ebene sowie das Bundesdatenschutzgesetz[7] die zentralen datenschutzrechtlichen Regelungen dar. Dabei sind die datenschutzrechtlichen Schutzziele und die der Cyber- und Informationssicherheit weitgehend kohärent und teilweise sogar deckungsgleich (zum Beispiel bei den Schutzzielen der Integrität und Vertraulichkeit), können im Einzelfall aber auch in einem Spannungsverhältnis zueinander stehen (zum Beispiel die datenschutzrechtliche Datenminimierung und das Sicherheitsinteresse an einer Protokollierung von Datenzugriffen). In diesen Fällen muss ein Ausgleich der widerstreitenden Interessen erfolgen, der beiden Schutzzielen zur weitestgehenden Wirksamkeit verhilft.

[5] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

[6] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680

[7] Abrufbar unter: http://www.gesetze-im-internet.de/bdsg_2018/

5 Cyberbedrohungslage

Informationstechnik (IT) ist ein integraler Bestandteil unseres gesellschaftlichen Lebens geworden. Kaum ein technisches Produkt kommt ohne IT aus. Während Anfang des 21. Jahrhunderts um die Jahrtausendwende die Prozessautomatisierung mittels IT im Vordergrund stand, erfolgt die Wertschöpfung bei heutigen IT-Systemen insbesondere durch deren Vernetzung und durch „intelligente“ Algorithmen.

Vernetzte IT-Systeme haben allerdings auch eine deutlich größere Angriffsfläche, insbesondere da diese zumeist aus aller Welt über das Internet erreichbar sind. Gleichzeitig führt die wachsende Komplexität der IT-Systeme und Algorithmen häufiger zu ungewolltem Systemverhalten und Sicherheitslücken in Systemen, sogenannten Schwachstellen. Angreifer nutzen daher die weltweite Erreichbarkeit der Systeme in Verbindung mit den Schwachstellen, um ihre kriminellen Absichten umzusetzen.

Dem Bestreben, die Sicherheit von IT-Systemen zu gewährleisten und zu verbessern, steht eine marktgetriebene dynamische Weiterentwicklung der IT gegenüber. In diesem Wettlauf treten daher nach wie vor regelmäßig Schwachstellen auf. Auch werden Vorgaben beziehungsweise etablierte Standards zum sicheren Betrieb von IT nicht immer hinreichend beachtet. Dafür tragen die Hersteller eine besondere Verantwortung, aber auch das Verhalten der Nutzer, Betreiber und Administratoren trägt einen wesentlichen Anteil zu sicheren IT-Systemen bei. Nur wenn alle beteiligten Akteure gut zusammenwirken, lassen sich Cyberangriffe zuverlässig erkennen und deren Wirkung erfolgreich verhindern oder abschwächen.

Dem Staat kommt dabei die Rolle zu, geeignete Rahmenbedingungen für sichere IT-Systeme zu schaffen. Beratungsangebote unter anderem des Bundesamts für Sicherheit in der Informationstechnik (BSI), staatlich geförderte Forschung und präventive Maßnahmen verschiedener Sicherheitsbehörden tragen dafür Sorge, dass Mindestanforderungen für die Gewährleistung von IT-Sicherheit geschaffen und eingehalten, Cyberangriffe erkannt und aufgeklärt sowie die Täterinnen oder Täter durch Sicherheits- und Strafverfolgungsbehörden ermittelt und zur Verantwortung gezogen werden - dies ist aufgrund von deren weltweitem Wirken oftmals eine besondere Herausforderung.

Trotz intensiver Bemühungen zur Gewährleistung von Cybersicherheit sehen wir heute eine deutliche Zunahme von Cyberangriffen. Dabei vermischt sich der klassische Cyberangriff im Sinne der Definition dieser Strategie zunehmend mit anderen Phänomenbereichen wie Erpressung, Desinformation, Betrug oder Beleidigung. Das Vorgehen der Täterinnen und Täter wird zudem immer ausgefeilter. Arbeitsteiliges Vorgehen bei der Durchführung von Cyberangriffen und der Entwicklung von Schadsoftware ist zwischenzeitlich der Regelfall. Dem kann nur geeignet begegnet werden, wenn alle Maßnahmen zur Gewährleistung von Cybersicherheit regelmäßig geprüft und angepasst werden. Diese Strategie ist einer der Bausteine dafür.

Deutschland setzt sich für ein freies, offenes, sicheres und globales Internet ein, in dem grundrechtlich verbürgte Freiheiten geschützt werden. Cybersicherheit ist auch ein Baustein, diese Werte zu gewährleisten.

5.1 Angriffsvektoren – welche Einfallstore ermöglichen den Angriff?

Unsichere IT-Systeme – sowohl Hard- als auch Software – stellen ein zentrales Einfallstor für Cyberangriffe dar. Je größer und komplexer Softwareprojekte werden und je mehr Personen dabei in die Erstellung eingebunden sind, desto häufiger entstehen Fehler in der Software, die als Schwachstellen durch Angreifer ausgenutzt werden können. Zwar sorgen zahlreiche Hersteller mittlerweile mit regelmäßigen oder kurzfristigen Updates dafür, festgestellte Schwachstellen zu schließen (Patchen). Jedoch lassen sich nicht immer alle Schwachstellen schließen und auch die schiere Anzahl an Schwachstellen verdeutlich den Bedarf, durch verbesserte Qualitätssicherungsprozesse das Aufkommen von Schwachstellen bereits vor Veröffentlichung zumindest zu reduzieren.

Weitere Ursachen für unsichere IT-Systeme sind fehlerhafte Konfiguration, mangelnde Schutzmechanismen oder Fehlbedienungen der Nutzerinnen und Nutzer. Auch diese Ursachen ermöglichen es unberechtigten Dritten, in fremde Systeme einzudringen und diese zu kompromittieren.

Zusätzlich erweitert die schnell anwachsende Zahl von mit dem Internet verbundenen Geräten (Internet of Things - IoT), wie beispielsweise Lautsprecher, Kühlschränke, Türklingeln, Fahrstühle und Werkzeugmaschinen sowie Medizingeräte, die Möglichkeit potenzieller Cyberangriffsszenarien. Dies wiegt umso schwerer, als viele IoT-Geräte oftmals nur über ein geringes Cybersicherheitsniveau verfügen. Die Schnelllebigkeit dieses Marktes führt häufig zu schlechter Qualität der Software mit großen Sicherheitslücken. Zudem sind Patches nicht oder nicht über entsprechend lange Zeiträume oder nur stark verzögert verfügbar und gegebenenfalls in Ermangelung entsprechender Funktionen beziehungsweise Schnittstellen gar nicht erst einspielbar.

Für die Ausnutzung der Mehrzahl der Schwachstellen bedarf es zumeist auch eines aktiven Zutuns der Nutzenden. Für Angriffe über Schwachstellen wird teilweise auch fehlende Information von Nutzenden ausgenutzt. Der schnelle Klick auf einen unsicheren, schadhaften Link, die Installation von Software aus unbekannten Quellen oder das unbedachte Öffnen eines E-Mail-Anhangs sind typische Alltagsfälle für die Kompromittierung eines IT-Gerätes. Ohne sensibilisierte Nutzende wird ein hohes Niveau an Cybersicherheit daher kaum gelingen.

Zu beobachten ist zudem ein sich verstärkender Trend zu Supply-Chain-Angriffen. Hier wird durch den Angreifer eine Soft- oder Hardware während des Herstellungs- oder Pflegeprozesses verändert. Die Manipulation des Angreifers wird dann unmittelbar vom Hersteller mit dem Produkt ausgeliefert. Zum Beispiel wurde im Dezember 2020 bekannt, dass Angreifer ein Update eines Softwareherstellers manipuliert hatten. Die Installation des Updates erfolgte automatisiert. Da die Nutzenden regelmäßig den Updatemechanismen vertrauen, können typischerweise zahlreiche Systeme betroffen sein. Derartige Angriffe stellen ein besonderes Risiko dar, da die manipulierte Software häufig mit Administratorrechten installiert oder betrieben wird und Schutzmechanismen wie Virenscanner zumeist nicht ansprechen. Kundinnen und Kunden sowie Verbraucherinnen und Verbraucher sind regelmäßig arg- und schutzlos.

Insbesondere bewusst herbeigeführte Schwachstellen der Hardware zeigen, dass Cybersicherheit auch eine Frage Digitaler Souveränität ist, da ein nationaler Fertigungsprozess besser beaufsichtigt oder reguliert werden kann. Die Abhängigkeit von Systemen, deren Vertrauenswürdigkeit nicht kontrolliert werden kann, eröffnet potenzielle Einfallstore für Cyberakteure.

Die Chancen neuer Technologien wie KI oder Quantencomputing sind unbestritten. Damit verbunden sind aber auch neue Risiken. Beispielsweise basieren KI-basierte Verfahren häufig auf einem Trainingsprozess und lassen sich in ihrem Verhalten oftmals nicht vollständig nachvollziehen. Aus diesem Grund kann die Integrität dieser Algorithmen gegebenenfalls durch geschickte Auswahl der Eingabemuster oder Trainingsdaten beeinträchtigt werden. Bei einer Verkehrszeichenerkennung führten beispielsweise geschickte Manipulationen der Verkehrszeichen zu fehlerhaften Ausgaben. Um Risiken bei neuen Informationstechnologien zu begegnen, bedarf es jedoch weiterer Forschung und neu zu entwickelnder Technologien.

5.2 Bedrohungen – welche Entwicklungen werden bei Cyberangriffen festgestellt?

Die Durchdringung des gesellschaftlichen Lebens durch die IT hat zu verschiedensten neuen Bedrohungen geführt. Die Bereitstellung von Medien über das Internet lässt neue Wege zur Manipulation von Meinungen zu. Einfache Nutzung und weitgehende Anonymität haben unter anderem Falschmeldungen und Hassreden in Sozialen Medien ansteigen lassen. Auch die Verbreitung illegaler Inhalte wie Kinderpornographie und urheberrechtlich geschützter Inhalte über das Internet nimmt – insbesondere unter Ausnutzung von Anonymisierungsdiensten und Verschlüsselungsangeboten – nach wie vor zu.

Der eigentliche Fokus dieser Strategie liegt jedoch nicht auf Bedrohungen, bei denen die IT dazu genutzt wird, illegale Inhalte zu verbreiten oder auf Betrugsversuchen (Phishing), sondern auf Cyberangriffen, die die Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen unmittelbar und maßgeblich beeinträchtigen. Damit einher gehen auch regelmäßig Verstöße gegen den Datenschutz durch Abschöpfung personenbezogener Daten. Cyberangriffe können auch als Mittel hybrider Bedrohungen zum Einsatz kommen. Typisch sind Cyberangriffe auch in den Phänomenbereichen Cyberkriminalität, Cyberterrorismus, Cyberspionage und Cybersabotage, deren Wirkungen zum Beispiel auf Kritische Infrastrukturen erhebliche wirtschaftliche und gesellschaftliche Folgen haben können.

5.2.1 Cyberkriminalität

Im Bereich der Cyberkriminalität ist der Einsatz von Ransomware, die den Zugang zu Daten oder Systemen blockiert, derzeit eine der größten Bedrohungen. Die Akteure greifen dort an, wo sie ungeschützte Schwachstellen finden, egal ob es sich um Unternehmen, Behörden oder private Nutzende handelt. Dem eigentlichen Cyberangriff folgen dann Erpressungsversuche, wie die Drohung der Veröffentlichung von Kundendaten im Netz, bis zur Androhung der Weitergabe sensibler Informationen an Konkurrenten. Ransomware verursacht zwischenzeitlich erhebliche Schäden, insbesondere auch, weil die betroffenen Stellen oftmals weltweit vernetzt sind und so große Bereiche von Unternehmen oder ganze Infrastrukturbereiche bei einem solchen Angriff ausfallen können. Eine ernstzunehmende Gefahr geht außerdem vom sogenannten „Big Game Hunting“ aus. Dabei fokussieren sich die Angreifer auf besonders zahlungskräftige beziehungsweise lukrative Ziele, so dass die Aussicht auf hohe Lösegeldzahlungen besteht.

Sogenannte Distributed-Denial-of-Service (DDoS)-Angriffe überlasten IT-Systeme in der Regel durch Netzwerkverkehr und werden ebenfalls häufig für Erpressungsversuche genutzt. Oftmals finden diese Angriffe mittels Bot-Netzen statt. Dazu kapern Angreifer zuvor eine Vielzahl von IT-Systemen, die dann ferngesteuert genutzt werden, oder sie zweckentfremden teils fehlkonfigu-

rierte, teils nicht absicherbare, aber öffentlich erreichbare Systeme, um das Zielsystem zu überlasten. Die dafür genutzte Schadsoftware hat sich über die Jahre deutlich fortentwickelt, so dass neben der Durchführung von DDoS-Angriffen häufig auch Zugriffe auf die Daten der Bots möglich sind, mittels derer vertrauliche Daten der Betroffenen gewonnen werden können. Dies ist ein typisches Einfallstor für die Erlangung von Zugangsdaten. Ein weiteres Feld für DDoS-Angriffe sind unliebsame Inhalte im Internet. So werden diese beispielsweise zur Behinderung von Parteiveranstaltungen genutzt. Dabei verschwimmen die Motive wie Hacktivismus oder staatliche Einflussnahme zunehmend.

5.2.2 Staatlich motivierte Cyberangriffe

Auf dem Gebiet staatlich motivierter Cyberangriffe wie Cyberspionage und Cybersabotage sehen sich staatliche und nichtstaatliche Einrichtungen sowie Wirtschaftsunternehmen zunehmend strategisch agierenden Cyberakteuren gegenüber. Die in diesen Bereichen zumeist tätigen Akteure – sogenannte Advanced Persistent Threat (APT)-Gruppen – zeichnen sich durch einen teils sehr hohen Ressourceneinsatz, eine hohe Durchhaltefähigkeit und umfassende technische Fähigkeiten aus. Dementsprechend werden deren Aktivitäten oftmals nachrichtendienstlichen Akteuren oder in ihrem Auftrag handelnden Gruppen zugerechnet.

Mit komplexen und langfristig angelegten Strategien versuchen diese Gruppen, unerkannt in IT-Systemen Fuß zu fassen. Neben der Nutzung solcher „Zugänge“ zum Zweck der Cyberspionage, um beispielsweise sensible Informationen zu stehlen, wurden zuletzt häufiger Aktivitäten zur Vorbereitung von Cybersabotagemaßnahmen festgestellt (sogenanntes Pre-Positioning). Da immer mehr Staaten entsprechende Cyberfähigkeiten entwickeln, werden Cyberangriffe von APT-Gruppen auf absehbare Zeit eine große Bedrohung bleiben. Erkennbar ist auch, dass teils eine Symbiose der Akteure im Bereich Cyberkriminalität und Cyberspionage beziehungsweise Cybersabotage vollzogen wird. Auch militärische Akteure arbeiten kontinuierlich am Aufbau eigener Cyberfähigkeiten; der Blick auf die Cyberbedrohungslage muss daher auch die militärische Komponente beinhalten.

5.2.3 Cyberangriffe im Rahmen hybrider Bedrohungen

Unter hybriden Bedrohungen wird das zielgerichtete Vorgehen staatlicher Akteure und ihrer nicht-staatlichen vorgelagerten Stellen (Proxies) verstanden, das eine große Bandbreite an verdeckten und offenen Mitteln umfassen kann. So können Angriffe im Cyberraum in weiteren Bereichen (zum Beispiel im Informationsraum) Wirkung entfalten, mit Aktivitäten in weiteren Bereichen konzertiert erfolgen oder der Vorbereitung weiterer Aktivitäten der illegitimen Einflussnahme dienen.

Gerade zwischen den Bereichen Cyber- und Informationsraum besteht ein enger Zusammenhang, da der Informationsraum zunehmend durch Informationstechnik gestaltet wird und sich durch einen hohen Grad der Vernetzung auszeichnet. Ein Beispiel für Angriffe im Sinne hybrider Bedrohungen sind Cyberspionageangriffe, die sensible Informationen rechtswidrig aus IT-Systemen abgreifen, um diese in einem zweiten Schritt manipulativ zu verbreiten und so im Informationsraum mittels Diskreditierung oder Desinformation schädliche Wirkung zu entfalten.

Cybersabotageangriffe können auch das Ziel verfolgen, in weiteren Bereichen, zum Beispiel in der Wirtschaft, insbesondere auch auf Kritische Infrastrukturen schädlich einzuwirken und die daraus folgenden Auswirkungen im Informationsraum manipulativ auszunutzen. Kritische Infrastrukturen sind für die Versorgung essenziell. Ein Ausfall führt zu großer Verunsicherung und liegt somit im potenziellen Fokus der Angreifer. Kritische Infrastrukturen bedürfen daher eines hohen

Schutzniveaus. Die im Rahmen hybrider Bedrohungen eingesetzten Mittel ermöglichen es den jeweiligen Akteuren oft verhältnismäßig einfach, die Täterschaft und die dahinterliegenden Motivationen zu verschleiern beziehungsweise abzustreiten. Als ein Beispiel kann der mutmaßlich staatliche Cyberangriff mit einem als Ransomware getarnten Sabotagetool (NotPetya) im Jahr 2017 angesehen werden.

Propaganda und Desinformation können besonders dann zu einer großen Gefahr werden, wenn diese durch Cyberangriffe auf glaubwürdigen Plattformen verbreitet werden. Web-Angebote von Medienunternehmen bedürfen daher eines hohen Schutzes vor Cyberangriffen.

Cyberangriffe im Rahmen hybrider Bedrohungen unterscheiden sich technisch zunächst nicht von anderen Cyberangriffen, zu denen diese Strategie Aussagen trifft. Die reguläre Nutzung digitaler Medien für Desinformation oder anderweitige illegitime Zwecke ist hingegen keine Frage der Cybersicherheit.

5.3 Assets – welche Güter sind bedroht?

Da unser Leben in nahezu allen Aspekten mit der IT verknüpft ist, können Cyberangriffe alle Lebensbereiche treffen. Der Ausfall der IT durch einen Cyberangriff kann beispielsweise zu Versorgungsengpässen führen. Daten werden zunehmend zu einem wertvollen Gut, etwa, wenn durch Cyberangriffe auf sensible Finanz- oder Gesundheitsdaten zugegriffen wird, um sie anschließend zum Gegenstand von Erpressung oder Verkäufen im Darknet werden zu lassen. Die weite Verbreitung und die Vielzahl von Informationsportalen im Internet ermöglichen die Verbreitung falscher Informationen auf scheinbar legitimen Angeboten, die erhebliche Unsicherheit in der Bevölkerung schüren können. Letztlich können Cyberangriffe zentrale Güter und Werte unserer Gesellschaft beeinträchtigen, wie Sicherheit, Wohlstand, Selbstbestimmung und Demokratie.

Ob Kommunikation mit Familie und Freunden, Online-Shopping und Online-Banking, Bezug staatlicher Leistungen oder demokratische Willensbildung: Die Digitalisierung prägt den Alltag der Menschen. Cyberangriffe, wie beispielsweise zum Zwecke des Identitäts- und Datendiebstahls oder zur Verbreitung von Desinformation, beeinträchtigen daher die Möglichkeiten, sich sicher und selbstbestimmt im Cyberraum zu bewegen.

Die Wirtschaft hängt in hohem Maße von funktionierenden, verlässlichen und integren IT-Infrastrukturen ab. Cyberangriffe auf Unternehmen sowohl in Deutschland als auch in aller Welt können in der eng verzahnten Produktionswelt mit komplexen Lieferverbindungen beziehungsweise Lieferketten enorme Dominoeffekte erzeugen, die massive wirtschaftliche Schäden mit sich bringen. Digitale Wirtschaftsspionage gefährdet unmittelbar den wirtschaftlichen Erfolg unserer Unternehmen, aber auch mittelbar die Wettbewerbsfähigkeit und Stabilität unserer Volkswirtschaft als Ganzes.

Kritische Infrastrukturen wie beispielsweise Strom- und Telekommunikationsnetze, Klinikverbünde oder Finanzsysteme sind für das Funktionieren des privaten, wirtschaftlichen und öffentlichen Lebens unerlässlich. Sie sind zunehmend von einer störungsfrei arbeitenden und integren IT-Infrastruktur abhängig. Eine Störung oder auch ein Ausfall durch einen IT-Sicherheitsvorfall kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Beeinträchtigungen der öffentlichen Sicherheit und Ordnung oder anderen dramatischen Folgen führen.

Angesichts der zunehmenden Digitalisierung der öffentlichen Verwaltung stellen Cyberangriffe auf staatliche Institutionen – neben den Gefährdungen durch eine Ausspähung sensibler Daten – unter anderem eine elementare Gefahr für die Funktionsfähigkeit und Integrität der staatlichen

Leistungserbringung dar. Angriffe auf das parlamentarische System sind auch Angriffe auf die demokratische Willensbildung und die freiheitliche demokratische Grundordnung.

5.4 Fazit

Ob sich die Bedrohungslage im Cyberraum insgesamt erhöht hat oder ob die Bedrohungslage nur relativ zur zunehmenden Verbreitung der IT in allen Lebensbereichen gestiegen ist, ist schwer zu beantworten. Die hohe und stetig wachsende Durchdringung aller Lebensbereiche durch IT, verbunden mit der Schnelllebigkeit des Marktes, fehlenden Standards und teilweise auch schlechtem Design, hat jedoch das Risiko erhöht, dass Cyberangriffe größere Schäden oder Störungen bewirken und deren Auswirkungen über die eigentlich betroffene IT hinaus spürbar sein können. Dies gilt es zu verhindern. Auch ist die absolute Zahl der erfassten Cyberangriffe in den letzten Jahren durchgängig angestiegen.

Neue Technologien enthalten regelmäßig auch neue Risiken. Je häufiger diese eingesetzt werden, desto mehr steigt auch hier die Gefahr von Cyberangriffen. Die Gewährleistung von Cybersicherheit muss somit ein ebenso dynamischer Prozess sein, wie die Fortentwicklung der Informationstechnik selbst.

Stetige Aufmerksamkeit und situationsgerechte Anpassung der Cybersicherheitsmaßnahmen sowie die Entwicklung und der Einsatz von Technologien, deren Sicherheit bereits mit dem Design verknüpft ist, sind ein wichtiger Teil zur Lösung des Problems. Diese Strategie ist hierfür ein Baustein. Die fortwährende Sensibilisierung der Nutzenden und der Austausch von Wissen zu Cybergefahren zwischen allen Akteuren sind eine weitere Säule, um Cybersicherheit zu gewährleisten. Verbunden mit der bewährten Arbeit der Sicherheitsbehörden auch im Cyberraum hat Deutschland gute Voraussetzungen, um sich auch den verändernden Cyberbedrohungen anzunehmen.

6 Die Cybersicherheitslandschaft in Deutschland

Cybersicherheit in Deutschland zu gewährleisten ist eine gesamtgesellschaftliche Aufgabe. Eine Vielzahl von Akteuren aus Staat, Wirtschaft, Wissenschaft und Gesellschaft leistet hierfür einen unverzichtbaren Beitrag. Auch jedem einzelnen Mitglied unserer Gesellschaft kommt Verantwortung für die Cybersicherheit zu. Eine umfassende und regelmäßig aktualisierte Liste der Akteure findet sich im „Online-Kompendium Cybersicherheit in Deutschland“[8].

Die Akteure und Initiativen zur Gewährleistung von Cybersicherheit in Deutschland lassen sich grundsätzlich folgenden Bereichen zuordnen, wirken zugleich aber häufig auch bereichsübergreifend zusammen:

1. Zivilgesellschaftliche Initiativen und Akteure
2. Wissenschaftliche Initiativen und Akteure
3. Wirtschaftliche Initiativen und Akteure
4. Staatliche Initiativen und Akteure

6.1 Zivilgesellschaftliche Initiativen und Akteure

Der Großteil der zivilgesellschaftlichen Akteure, die sich in Deutschland im Bereich Cybersicherheit engagieren, sind Vereine und Stiftungen. Hinzu kommt eine große Anzahl unabhängiger ehrenamtlicher Expertinnen und Experten. Diese Akteure erstellen unter anderem politische Analysen und Handlungsempfehlungen, sensibilisieren die Bevölkerung für Belange der Cybersicherheit, vermitteln Medienkompetenz und Technikverständnis und vernetzen verschiedene Gesellschaftsgruppen. Durch die Vielzahl zivilgesellschaftlicher Initiativen und Akteure gelingt es, einer großen Zahl von Adressaten ein ausdifferenziertes Angebot bereitzustellen.

6.2 Wissenschaftliche Initiativen und Akteure

Die Wissenschaft leistet insbesondere durch ihre Forschungstätigkeit in Form von Grundlagenforschung und angewandter Forschung theoretischer, experimenteller und industrieller Natur einen zentralen Beitrag zur Erhöhung der Cybersicherheit in Deutschland. Daraus resultierende Erkenntnisse und Innovationen in Form von Analysen, Handlungsempfehlungen, Lehrinhalten und Technologien bilden eine unverzichtbare Grundlage für konkrete Anwendungsfälle in Staat, Wirtschaft und Gesellschaft.

6.3 Wirtschaftliche Akteure und Initiativen

Wirtschaftliche Akteure und Initiativen engagieren sich in einem breiten Themenspektrum der Cybersicherheit. Sie entwickeln unter anderem innovative technische Lösungen, bringen sich bei der Weiterentwicklung sicherheitsrelevanter Standards und Normen ein und treiben in themenspezifischen Arbeitsgruppen die Vernetzung und Kompetenzentwicklung voran. Cybersicherheit

[8] Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf?__blob=publicationFile&v=4

ist für wirtschaftliche Akteure auch ein zentraler Standort- und Wettbewerbsfaktor. Netzwerke, wie beispielsweise die Allianz für Cybersicherheit, der UP KRITIS oder die Initiative Wirtschaftsschutz, leisten daher einen Beitrag zur Stärkung des Wirtschaftsstandortes Deutschland.

6.4 Staatliche Initiativen und Akteure

Dem Staat kommen bei der Gewährleistung eines hohen Cybersicherheitsniveaus eine herausgehobene Rolle und eine hohe Verantwortung zu. Das staatliche Aufgabenfeld reicht von der Prävention, der Bedrohungslagebilderstellung, der Detektion, der Gefahrenabwehr, der Vorfallsbewältigung und der Strafverfolgung über die Spionageabwehr und die nachrichtendienstliche Vorfeldaufklärung bis hin zur Cyberaußenpolitik und zur Cyberverteidigung. Entsprechend sind auf Bundes- und Landesebene zahlreiche Akteure aktiv, die sich im Rahmen ihrer jeweiligen Zuständigkeiten intensiv mit den Bedrohungen aus dem Cyberraum befassen. Die Aktivitäten des Bundes gliedern sich dabei in eine strategische und eine operative Ebene.

6.4.1 Strategische Ebene

Die strategische Ausrichtung der Cybersicherheitsvorhaben und die Aufsicht über deren Umsetzung sind Aufgabe der Ministerien. Nach dem Ressortprinzip steuern die Ressorts die Aktivitäten in ihrem Bereich eigenständig und eigenverantwortlich. Auf Bundesebene kommt dem Bundesministerium des Innern, für Bau und Heimat (BMI) im Bereich der Cybersicherheitsinnenpolitik und dem Auswärtigen Amt im Bereich der Cyberaußenpolitik zusätzlich eine koordinierende Funktion zu. Die Cyberverteidigung fällt in die Zuständigkeit des Bundesministeriums der Verteidigung (BMVg).

Der NCSR ist strategischer Ratgeber der Bundesregierung. Er wurde mit der „Cybersicherheitsstrategie für Deutschland 2011“ eingeführt und mit der „Cybersicherheitsstrategie für Deutschland 2016“ weiterentwickelt. Durch seine Zusammensetzung aus Vertretern aus Bund, Ländern und Kommunen sowie der Wirtschaft kommt ihm eine Scharnierfunktion zwischen den relevanten Akteuren in der deutschen Cybersicherheitslandschaft zu. Seit Oktober 2018 berät zudem eine ständige wissenschaftliche Arbeitsgruppe den NCSR aus Perspektive der Forschung zu Entwicklungen und Herausforderungen einer sicheren und vertrauenswürdigen Digitalisierung.

Die zuständigen Gremien für die strategische Ausrichtung des Informationssicherheitsmanagements des Bundes und die Umsetzung des Kabinettsbeschlusses der „Leitlinie für Informationssicherheit in der Bundesverwaltung (Umsetzungsplan - UP Bund)“ sind der IT-Rat sowie die AG Informationssicherheitsmanagement des IT-Rates. Beim BMI ist die Rolle der oder des Beauftragten der Bundesregierung für Informationstechnik verankert, der oder dem unter anderem die Aufgabe der Steuerung des Informationssicherheitsmanagements auf Grundlage des UP Bund zufällt.

6.4.2 Operative Ebene

Die operative Umsetzung der strategischen Vorgaben und Zielsetzungen erfolgt insbesondere durch die Geschäftsbereichsbehörden des Bundeskanzleramtes und der Ministerien. Den nachfolgend dargestellten Aufgabenbereichen und Akteuren kommt dabei eine besondere Bedeutung zu.

Das BSI ist die zentrale Stelle für Informationssicherheit des Bundes. Im BSI sind das Bundes Security Operations Center (BSOC), das Computer Emergency Response Team des Bundes (CERT-Bund) und das Nationale IT-Lagezentrum verortet. Letzteres wächst in besonderen Lagen zum Nationalen IT-Krisenreaktionszentrum auf. Darüber hinaus ist das BSI für die Sicherheit und den Schutz der Informationstechnik und der Netze des Bundes sowie der nationalen Kritischen Infrastrukturen zuständig und gestaltet die Informationssicherheit in der Digitalisierung durch Prüfungs-, Standardisierungs-, Zertifizierungs-, Zulassungs- und Beratungsleistungen für Staat, Wirtschaft und Gesellschaft und arbeitet hierzu eng mit Akteuren aus allen Bereichen zusammen.

Das Bundesamt für Verfassungsschutz (BfV) dient dem Schutz der Inneren Sicherheit und informiert die Bundesregierung und die Öffentlichkeit über die Sicherheitslage. Es ist zuständig für die Sammlung und Auswertung von Informationen über nachrichtendienstlich gesteuerte sowie extremistisch oder terroristisch motivierte Cyberangriffe. Der Militärische Abschirmdienst (MAD) schirmt die Bundeswehr bereits außerhalb des Verteidigungs- oder Spannungsfalles sowie bei Einsätzen gegen Spionage und Sabotage sowie Extremismus und Terrorismus im Cyberraum ab. Dem Bundesnachrichtendienst (BND) obliegt die Aufgabe, die erforderlichen Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für Deutschland sind, auch im Cyberraum zu sammeln und auszuwerten. Das Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR) koordiniert die Cyberverteidigung in der Bundeswehr.

Für die Gefahrenabwehr sind in Deutschland grundsätzlich die Länder zuständig. Dem Bund stehen in bestimmten Bereichen gefahrenabwehrrechtliche Sonderzuständigkeiten zu (zum Beispiel in den Bereichen internationaler Terrorismus, Sicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, Grenzschutz oder Eigensicherung), die sich auch auf den Cyberraum erstrecken. Diese Zuständigkeiten werden vom Bundeskriminalamt (BKA), der Bundespolizei (BPOL) und dem BSI wahrgenommen. Die Strafverfolgung im Cyberraum ist Aufgabe der Justiz mit Unterstützung durch die Landeskriminalämter und Polizeibehörden der Länder, beziehungsweise durch das BKA und die BPOL im Rahmen ihrer jeweiligen Zuständigkeiten.

Die Abstimmung zwischen den benannten sowie weiteren relevanten Behörden auf der operativen Ebene erfolgt unter anderem im Cyber-AZ, das bereits 2011 als zentrale Informations- und Koordinationsplattform eingerichtet und über die Jahre weiterentwickelt wurde.

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) wirkt im Schwerpunkt als Dienstleister für die Sicherheitsbehörden im Geschäftsbereich des BMI mit dem Ziel, deren Cyberfähigkeiten und Digitale Souveränität zu stärken.

Zudem kommt den Behörden und Gesellschaften im Besitz des Bundes eine besondere Bedeutung zu, die mit dem sicheren Betrieb der IT-Infrastruktur des Bundes betraut sind. Hierzu zählen die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) als Bundesnetzbetreiberin, das Informationstechnikzentrum Bund sowie das Auswärtige Amt als Betreiber seiner Auslands-IT.

6.4.3 Die Zusammenarbeit zwischen Bund und Ländern

Die vielfältigen staatlichen Aufgaben im Cyberraum können nur durch eine gemeinsame Anstrengung von Bund und Ländern erfüllt werden. Eine intensive Verzahnung der Aktivitäten der Bundes- und Landesebene auf dem Wege einer kooperativen und komplementären Zusammenarbeit ist hierbei unumgänglich.

Zentrale Gremien zur Abstimmung der Bund-Länder-Zusammenarbeit auf strategischer Ebene sind die Innenministerkonferenz und deren Länderarbeitsgruppe Cybersicherheit sowie der IT-Planungsrat und dessen AG Informationssicherheit. Letztere sind auch für das Informationssicherheitsmanagement zwischen Bund und Ländern zuständig.

Auch auf operativer Ebene bestehen zahlreiche Formate der Zusammenarbeit zwischen Bund und Ländern. Nur beispielhaft sind hier die vertrauensvolle Zusammenarbeit der Verfassungsschutzbehörden aus Bund und Ländern im Verfassungsschutzverbund zu nennen, der intensive Austausch im Verwaltungs-CERT-Verbund (VCV) oder die enge Abstimmung der Landeskriminalämter mit dem BKA als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei. Die immer häufiger seitens der Länder eingerichteten zentralen Koordinierungsstellen für Cybersicherheit sind in diese operative Zusammenarbeit ebenfalls eng eingebunden. Das Nationale Verbindungswesen des BSI gestaltet die Beziehungen des BSI zu nationalen Partnern und steht den Ländern als Ansprechpartner auf regionaler Ebene zur Verfügung.

7 Leitlinien der Cybersicherheitsstrategie

Die in der „Cybersicherheitsstrategie für Deutschland 2021“ erstmals aufgeführten strategischen Ziele und operativen Maßnahmen werden im Licht von Leitlinien betrachtet, geprüft und umgesetzt. Die Leitlinien leiten sich aus den die Handlungsfelder übergreifenden Interessen und Belangen ab und dienen zur Bündelung und Fokussierung, um so ein kohärentes Ineinandergreifen der einzelnen strategischen Ziele und Maßnahmen zu gewährleisten.

7.1 Leitlinie: „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“

Cyberbedrohungen und Cyberkriminalität betreffen nicht nur den Staat, sondern auch Unternehmen, wissenschaftliche Einrichtungen, Vereine sowie die Bürgerinnen und Bürger. Um in diesem Umfeld ein hohes Sicherheitsniveau gewährleisten zu können, müssen alle Akteure ihren Beitrag zur Bewältigung von Cyberbedrohungen leisten. Die Bundesregierung versteht Cybersicherheit daher als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Dies setzt ein kooperatives Vorgehen sowie eine vertrauensvolle Zusammenarbeit voraus, um gemeinsame Antworten auf Cyberbedrohungen finden zu können.

Bedrohungen im Cyberraum machen nicht an Ländergrenzen halt. Deutschland ist, wie in vielen anderen Bereichen auch, im Bereich Cybersicherheit in ein Netz europäischer und internationaler Zusammenarbeit eingebunden, weshalb Cybersicherheit auch nur in Kooperation mit unseren europäischen und internationalen Partnern gewährleistet werden kann.

7.2 Leitlinie: „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken“

Das Thema Digitale Souveränität hat seit 2016 deutlich an Relevanz und Aufmerksamkeit gewonnen. Digitale Souveränität wird hier (aus Sicht der Bundesregierung) verstanden als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“[9]. Digitale Souveränität hat somit auch für die Cyber- und Informationssicherheit eine wesentliche Bedeutung; sichere Technologien und Lösungen sowie entsprechende Fähigkeiten, die Chancen und potenziellen Risiken digitaler Technologien erkennen und bewerten zu können, sind eine wesentliche Voraussetzung für die Digitale Souveränität. Ein hohes Cybersicherheitsniveau trägt so zur Stärkung der Digitalen Souveränität von Bürgerinnen und Bürgern, Wirtschaft, Wissenschaft und Staat bei. Auf europäischer Ebene bedeutet Digitale Souveränität eine stärkere wirtschaftliche und sicherheitspolitische Vernetzung mit strategisch wichtigen Partnern, um Abhängigkeiten zu mindern und die politische Handlungs- beziehungsweise Gestaltungsfähigkeit zu bewahren.

[9]Vergleiche Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, abrufbar unter: https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet

Digitale Souveränität ist daher eine zentrale Leitlinie der Cybersicherheitsstrategie 2021 und ein Handlungsmotiv in allen vier Handlungsfeldern. Schwerpunktbereiche sind unter anderem

- die anwendungsorientierte Forschung und Entwicklung sowie der Forschungstransfer (Handlungsfeld 1),
- die Cybersicherheit als Qualitätsmerkmal „Made in Germany“ (Handlungsfeld 2),
- die staatlichen Fähigkeiten zur Beurteilung neuer Technologien und Beauftragung europäischer Anbieter und zur Eigensicherung der Verwaltung (Handlungsfeld 3),
- eine gemeinsame Vision und Strategie der EU für Cybersicherheit und europäische Digitale Souveränität (Handlungsfeld 4).

Bei näherer Betrachtung wird deutlich, dass je nach Akteur und Kontext unterschiedliche Aspekte und Dimensionen Digitaler Souveränität im Vordergrund stehen. Das Thema Digitale Souveränität stellt sich somit mit einer hohen Komplexität und Vielfalt dar und wird je nach Handlungsfeld entsprechend differenziert betrachtet.

Initiativen und Anliegen der Bundesregierung

Mit dem am 12. Februar 2020 von der Bundesregierung beschlossenen neuen „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie“[10] sollen die industriellen Kernfähigkeiten und strategisch relevanten Entwicklungskapazitäten in Deutschland und der EU erhalten und gefördert werden. Diese Strategie bildet den Rahmen für die Politik der Bundesregierung hinsichtlich der Sicherheits- und Verteidigungsindustrie und ist damit wesentliche Leitlinie zum Schutz der Digitalen Souveränität. Damit hat die Bundesregierung bereits entsprechende Maßnahmen in fünf Bereichen benannt:

- Forschung, Entwicklung und Innovationen stärken,
- Rahmenbedingungen für eine effiziente Produktion setzen,
- Beschaffungswesen optimieren,
- Exporte politisch flankieren und verantwortungsvoll kontrollieren und
- Schutz von Sicherheitsinteressen.

Insbesondere sollen zum Schutz der Sicherheitsinteressen Digitale Souveränität und Resilienz gegenüber hybriden Bedrohungen erlangt und die Abhängigkeit von ausländischen Informationstechnologien reduziert werden. Neben den Prüfmechanismen nach dem Außenwirtschaftsgesetz und der Außenwirtschaftsverordnung arbeitet die Bundesregierung an flexiblen und strategisch einsetzbaren Instrumenten als Antwort auf drohende Ausverkäufe zukünftiger sicherheits- und verteidigungsindustrieller Schlüsseltechnologien. Dazu soll auch die Einrichtung eines IT-Sicherheitsfonds vorangetrieben werden, um aktiv unerwünschten Übernahmen begegnen zu können.

Im Bereich „Forschung, Entwicklung und Innovationen stärken“ wird die im Sommer 2020 eingerichtete Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) ambitionierte

[10] Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Branchenfokus/Industrie/branchenfokus-sicherheits-und-verteidigungsindustrie.html

Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zur Bedarfsdeckung Deutschlands im Bereich der Inneren und Äußeren Sicherheit beauftragen und finanzieren.

Um Ideen mit Marktpotenzial im Bereich der IT-Sicherheit schneller in die Anwendung zu bringen, hat die Bundesregierung die Initiative „StartUpSecure“ ins Leben gerufen. Darin werden Unternehmensgründungen im Bereich der IT-Sicherheit gefördert. Für die Begleitung der jungen Gründungen wurden an den nationalen Kompetenzzentren für IT-Sicherheitsforschung ATHENE (Darmstadt), CISPA (Saarbrücken) und KASTEL (Karlsruhe) sowie an der Ruhr-Universität Bochum Inkubatoren eingerichtet.

Im Bereich Forschung zum Zukunftsthema 6G hat die Bundesregierung das Ziel ausgerufen, dass Deutschland eine führende Rolle als Anbieter vertrauenswürdiger Kommunikationstechnologie in der Weltwirtschaft einnimmt und frühzeitig den technologischen Wandel mitgestaltet. In einem ersten Schritt ist der Aufbau von vier 6G-Forschungs-Hubs und einer Plattform für zukünftige Kommunikationstechnologien und 6G geplant.

Mit Blick auf die öffentliche Verwaltung hat der IT-Planungsrat im März 2021 die „Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung“ beschlossen. Diese führt neben den strategischen Zielen „Wechselmöglichkeit“, „Gestaltungsfähigkeit“ und „Einfluss auf Anbieter“ verschiedene Lösungsansätze und Maßnahmen zur Stärkung der Digitalen Souveränität der Verwaltung aus. Hierbei ist neben rechtlichen Rahmenbedingungen und dem Aufbau von Kompetenzen beziehungsweise Expertenwissen auch die Diversifizierung mit bedarfsgerechten Open-Source-basierten IT-Lösungen als Maßnahme zu nennen.

Unter dem Dach der von der Bundesregierung geförderten Initiative „QuNET“[11] entwickeln die Fraunhofer-Gesellschaft, die Max-Planck-Gesellschaft und das Deutsche Zentrum für Luft- und Raumfahrt seit Ende 2019 Technologien für ein Pilotnetz zur Quantenkommunikation in Deutschland. Dieses soll zukünftig der abhör- und manipulationssicheren Datenübertragung dienen.

7.3 Leitlinie: „Digitalisierung sicher gestalten“

Im Vergleich zu 2016 hat die digitale Transformation von Staat (zum Beispiel E-Government-Gesetz, Onlinezugangsgesetz [OZG], IT-Konsolidierung, mobiles Arbeiten), Wirtschaft (zum Beispiel Sicherheitsanforderungen an 5G-Netze) und Gesellschaft (zum Beispiel der elektronische Identitätsnachweis [eID]) wesentlich an Dynamik gewonnen. Im Jahr 2020 stiegen die Anforderungen und Erwartungshaltungen an die Digitalisierung zudem sprunghaft durch die COVID-19-Pandemie.

Cyber- und Informationssicherheit ist eine Grundvoraussetzung für das Gelingen der Digitalisierung in Deutschland. Ohne deren sichere Ausgestaltung können die Menschen sich nicht frei und selbstbestimmt in einer digitalisierten Umgebung bewegen. Ein hohes Niveau an Cybersicherheit

[11] Abrufbar unter: https://www.qunet-initiative.de/

ermöglicht es hingegen, Potenziale der Digitalisierung voll zu nutzen und Gefahren selbstbewusst und selbstbestimmt zu begegnen. Daher wird das Thema „Digitalisierung sicher gestalten“ als Leitlinie der Cybersicherheitsstrategie 2021 in allen Handlungsfeldern durch entsprechende strategische Ziele adressiert.

Initiativen und Anliegen der Bundesregierung

Die Bundesregierung hat verschiedene Initiativen und Maßnahmen vorangebracht, um den digitalen Wandel in Deutschland zu gestalten. Die aktuelle Umsetzungsstrategie „Digitalisierung gestalten“[12] adressiert verschiedene Schwerpunktvorhaben zur Umsetzung digitalpolitischer Maßnahmen, unter anderem in den Bereichen digitale Kompetenzen, Infrastruktur, digitale Transformation von Staat und Gesellschaft sowie zur Ethik für eine digitale Gesellschaft.

Beispiele:

- Im Cybercluster der Universität der Bundeswehr München wird neben der Forschung und Entwicklung am Forschungsinstitut CODE die wissenschaftliche Aus-, Fort- und Weiterbildung insbesondere von Offizieren und Beschäftigten des Bundes mit dem Schwerpunkt Cybersicherheit durchgeführt.
- Unter dem Namen „Digital. Sicher. Souverän.“ hat die Bundesregierung ein neues Forschungsrahmenprogramm zur IT-Sicherheit aufgesetzt.
- Mit der Gründung der Cyberagentur werden ressortübergreifend Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zur Bedarfsdeckung im Bereich der Inneren und Äußeren Sicherheit Deutschlands möglich.

Mit der „Netzstrategie 2030 für die öffentliche Verwaltung“ [13] wurde die Netzstrategie der Bundesregierung aus dem Jahr 2013 überarbeitet und fortgeschrieben. Damit wurde den gestiegenen Anforderungen im Bereich der Kommunikationsfähigkeit der gesamten öffentlichen Verwaltung Deutschlands, neuen technischen Entwicklungen und den erhöhten Sicherheitsanforderungen Rechnung getragen. Ziel ist es, einen Informationsverbund der öffentlichen Verwaltung Deutschlands („IVÖV“) in Betriebsverantwortung der Bundesnetzbetreiberin (BDBOS) zu etablieren. Hierzu wurden folgende strategische Ziele definiert:

- Nationale Digitale Souveränität,
- Leistungsfähigkeit der Netzinfrastruktur,
- Informationssicherheit & Datenschutz & Geheimschutz,
- Zukunftsfähigkeit und Flexibilität und
- Digitale und ebenenübergreifende Zusammenarbeit.

[12] Abrufbar unter: https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002

[13] Abrufbar unter: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/netzstrategie_2030_fuer_die_oeffentliche_verwaltung.html?nn=4624892

Zur Umsetzung dieser strategischen Ziele wurden folgende strategische Handlungsfelder definiert und ein dazugehöriger Umsetzungskatalog erstellt:

- Strategische Ausgestaltung der Fertigungstiefe,
- Weiterentwicklung der aktiven Dienstleistersteuerung,
- Konsolidierung von Weitverkehrsnetzen,
- Internetressourcen und Standardisierung,
- Gewährleistung von Informationssicherheit, Datenschutz und Geheimschutz in Netzinfrastrukturen der öffentlichen Verwaltung,
- Weiterentwicklung des Anforderungs- und Nutzermanagement sowie der Dienstentwicklung und
- Förderung von Innovationen und Schlüsseltechnologien für eine bürgernahe und moderne Verwaltung.

Somit ist die „Netzstrategie 2030 für die öffentliche Verwaltung“ ein wichtiger Baustein, um Cybersicherheit in Deutschland zu gewährleisten.

7.4 Leitlinie: „Ziele messbar und transparent ausgestalten“

Die Transparenz staatlichen Handels ist wichtig für das Vertrauen von Bürgerinnen und Bürgern in den Staat. Der Nutzen und die Wirkung staatlicher Initiativen müssen entsprechend nachvollziehbar sein. Im Rahmen der Cybersicherheitsstrategie 2021 werden daher erstmals die Themen Messbarkeit und Transparenz adressiert. Umsetzung und zukünftige Fortschreibungen können so systematisch vorbereitet werden.

Um den Erfolg der Cybersicherheitsstrategie 2021 bewerten zu können, wird die Zielerreichung sowohl zum Ende der Laufzeit abschließend evaluiert als auch während der Laufzeit regelmäßig überprüft. Hierfür werden in allen Handlungsfeldern die angestrebten Ziele messbar formuliert. Für jedes strategische Ziel werden Indikatoren entwickelt, um die Zielerreichung überprüfen zu können.

Die Cybersicherheitsstrategie 2021 unterscheidet zwischen strategischen Zielen und operativen Maßnahmen:

Strategische Ziele

Strategische Ziele definieren SMARTe (spezifische, messbare, aktiv beeinflussbare, realistische und terminierte) Ziele innerhalb eines Handlungsfeldes, die im Rahmen der Umsetzung der Cybersicherheitsstrategie erreicht werden sollen. Strategische Ziele adressieren die Herausforderungen des Handlungsfeldes und beschreiben einen Zustand, der durch die Strategie angestrebt wird. Strategische Ziele werden spezifisch und konkret formuliert, um überprüfbar zu sein. Für jedes strategische Ziel werden zudem Indikatoren definiert, um die Zielerreichung messen zu können. Die strategischen Ziele sollen grundsätzlich innerhalb eines Zeitraums von fünf Jahren erreichbar sein.

Maßnahmen

Maßnahmen beschreiben Aktivitäten, mit denen die strategischen Ziele erreicht werden sollen. Sie müssen in ihrer Gesamtheit geeignet sein, das jeweilige strategische Ziel in der Laufzeit der Cybersicherheitsstrategie 2021 vollständig zu erreichen. Maßnahmen können beispielsweise einzelne Projekte oder fortlaufende Maßnahmen sein. Die Maßnahmen sind nicht Gegenstand der Strategie, sie werden als fortlaufende Aktivitäten nachgelagert geplant und umgesetzt (vergleiche Kapitel 9 „Umsetzung, Berichtswesen, Controlling und Evaluierung der Cybersicherheitsstrategie“).

8 Handlungsfelder der Cybersicherheitsstrategie

Im folgenden Kapitel werden die Handlungsfelder der Strategie beschrieben und mit den strategischen Zielen verknüpft. Getragen durch das Verständnis, dass Cybersicherheit nur gemeinsam gewährleistet werden kann (siehe Kapitel 7.1 Leitlinie: „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren“), werden die bewährten Handlungsfelder

1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung,
2. Gemeinsamer Auftrag von Staat und Wirtschaft,
3. Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur und
4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

beschrieben. Die strategischen Ziele wurden nach ihrer primären Schwerpunktsetzung den Handlungsfeldern zugeordnet. Einige Ziele sind hinsichtlich der benötigten Akteure, der Schwerpunkte in der Umsetzung oder hinsichtlich der zu erzielenden Wirkung nicht eindeutig nur einem Ziel zuzuordnen. In der Umsetzung ist darauf zu achten, dass alle erforderlichen Akteure eingebunden werden und übergreifend agiert wird.

8.1 Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Damit Bürgerinnen und Bürger die Chancen digitaler Technologien nutzen können, müssen sie sich sicher und selbstbestimmt in einer digitalisierten Umgebung bewegen. Sie müssen neben den Chancen auch die Risiken digitaler Technologien erkennen, bewerten und die Herausforderungen durch eigenes Handeln wirksam bewältigen können.

Einen wichtigen Beitrag, um die Beurteilungskompetenz der Bürgerinnen und Bürger zu steigern, leisten etwa Kennzeichnungen von Produkten und Dienstleistungen, die deren Konformität zu IT-Sicherheitsstandards belegen.

Insgesamt hat die Bundesregierung mehrere Möglichkeiten, um die „Cybersicherheitskompetenz“ der Gesellschaft zu steigern: Sie kann Maßnahmen ergreifen und Produkte anbieten, die die Bürgerinnen und Bürger sensibilisieren, sie kann Maßnahmen des klassischen Verbraucherschutzes ergreifen und sie kann anhand von Regulierungsmaßnahmen einen Rahmen schaffen, der sicheres und selbstbestimmtes Handeln fördert. Hieran orientieren sich die folgenden Ziele.

8.1.1 Digitale Kompetenzen bei allen Anwenderinnen und Anwendern fördern

Warum ist das Ziel relevant?

Das Bewusstsein für sicheres Verhalten im Cyberraum ist bei allen Nutzenden, von Bürgerinnen und Bürgern über kleine wie große Unternehmen bis hin zu allen staatlichen Stellen zentrale Voraussetzung für den Schutz vor Cyberrisiken und digitaler Sorglosigkeit.

Wo stehen wir?

Digitale Kompetenzen zu schaffen, ist ein fortlaufender Prozess, der sich parallel zu neuen Technologien und Trends mitentwickeln muss. In den letzten Jahren ist es gelungen, das Bewusstsein für die Relevanz von IT-Sicherheit bei allen Akteuren deutlich zu steigern. Zahlreiche staatliche und nichtstaatliche Projekte leisten gute Aufklärungsarbeit, die fortgeführt und intensiviert werden muss. Insbesondere im Bereich der schulischen und betrieblichen Bildung sollte das Wissen rund um IT-Sicherheit jedoch noch zielgerichteter gestärkt werden.

Das Bundesministerium für Bildung und Forschung (BMBF) begegnet diesen Herausforderungen mit gezielter Forschungsförderung, beispielsweise im Förderschwerpunkt „Unterstützung von Bürgerinnen und Bürgern bei der privaten IT-Sicherheit“[14] oder mit Förderrichtlinien wie „Sichere Industrie 4.0 in der Praxis“[15] sowie durch die Förderung des „Forum Privatheit“[16], das sich interdisziplinär mit gesellschaftlich relevanten Fragen zum Schutz der Privatheit auseinandersetzt und kontinuierlich zu Cyberrisiken und Datenschutzfragen sensibilisiert.

Auch die seit März 2021 laufende bundesweite Informations- und Sensibilisierungskampagne zur IT-Sicherheit „#einfachaBSIchern“ des BMI und des BSI sowie die Verbraucherschutzseiten des BSI[17] zielen auf die digitale Kompetenz, in dem sie die Anwenderinnen und Anwender für Risiken im Cyberraum sensibilisieren und informieren.

Seit 2006 bietet der durch das BMI geförderte Verein Deutschland sicher im Netz (DsiN) vielfältige Hilfestellungen für Bürgerinnen und Bürger sowie kleinere Unternehmen. Dazu gehören die Angebote der „Digitalen Nachbarschaft“ für Vereine und ehrenamtliche Engagierte für Sicherheit im Netz[18], „PolisiN - Politiker:innen sicher im Netz“[19] für ehren- und hauptamtliche Mandatsträger

[14] Abrufbar unter: https://www.bmbf.de/foerderungen/bekanntmachung-3160.html

[15] Abrufbar unter: https://www.bmbf.de/foerderungen/bekanntmachung-2019.html

[16] Abrufbar unter: https://www.bmbf.de/foerderungen/bekanntmachung-2547.html

[17] Abruf unter: https://www.bsi.bund.de/VerbraucherInnen

[18] Abrufbar unter: https://www.digitale-nachbarschaft.de/

[19] Abrufbar unter: https://polisin.de/

sowie „BottomUp - Berufsschulen für IT-Sicherheit“[20] für Schutzkompetenzen in der Dualen Ausbildung. Mit der durch das Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Transferstelle „IT-Sicherheit im Mittelstand“ (TISiM) betreibt DsiN im Verbund mit weiteren Partnern aus Wirtschaft und Wissenschaft bundesweit 80 Anlaufstellen, um insbesondere kleine Unternehmen, Selbstständige und Freiberufler bei der Umsetzung von IT-Sicherheitsmaßnahmen zu begleiten.

Was wollen wir erreichen?

Das erforderliche Bewusstsein und Verständnis von KMU, Bildungs- und Sozialeinrichtungen, Verbänden, Vereinen, Verbraucherinnen und Verbrauchern im Umgang mit immer komplexer werdenden Technologien, Dienstleistungen und Geschäftsmodellen wird gefördert.

Die Vermittlung digitaler Kompetenzen ist Bestandteil einer breiten Ausbildung an Schulen, Hochschulen, Universitäten und im betrieblichen Umfeld. Zudem können Anwenderinnen und Anwender auf zielgruppenspezifische Informations- und Unterstützungsangebote zu allen Fragen der Informations- und Cybersicherheit zurückgreifen sowie unter anderem ihr Kompetenzniveau über den vom BMI geförderten DsiN-Digitalführerschein[21] zertifizieren lassen. Diese werden weiter ausgestaltet und ausgebaut.

Dadurch verfügen Anwenderinnen und Anwender über digitale Kompetenzen und können die Vorteile der Digitalisierung nutzen. Sie verfügen über ein Problembewusstsein im Hinblick auf Cyberrisiken und sind in der Lage, die Sicherheit von Anwendungen und Diensten zu bewerten und entsprechend risikobewusst zu agieren.

Welche Wirkung erwarten wir?

Wirtschaft (insbesondere KMU), Wissenschaft und Gesellschaft sind resilienter gegenüber den Gefahren im Cyberraum. Sie nutzen die Vorteile der Digitalisierung und wissen mit ihren Herausforderungen umzugehen und sich zu schützen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Der durch das BMI geförderte Digitalführerschein wird in der Bevölkerung gut nachgefragt und trägt zur Steigerung der Digitalkompetenzen bei den Bürgerinnen und Bürgern – sowohl im privaten als auch im beruflichen Kontext – bei.
- Informationsangebote des BSI werden durch Verbraucherinnen und Verbraucher vermehrt angenommen.
- Verbraucherinnen und Verbraucher sind sensibilisiert und informiert, sie beschäftigen sich verstärkt mit Cybersicherheitsthemen und können Cyberrisiken besser einschätzen und ihnen entgegentreten.

---

[20] Abrufbar unter: https://www.dsin-berufsschulen.de/

[21] Abrufbar unter: https://www.sicher-im-netz.de/dsin-digitalfuehrerschein

- Die Zahl der von Cyberangriffen betroffenen Privatpersonen ist rückläufig.

8.1.2 Anwenderfreundlichkeit sicherheitstechnischer Lösungen steigern

Warum ist das Ziel relevant?

Gerade bei IT-Sicherheitslösungen, die zum Teil sehr spezielle Anforderungen erfüllen müssen, spielt Anwenderfreundlichkeit bei der Entwicklung oftmals eine untergeordnete Rolle. Sie ist aber wesentlich für die Akzeptanz und damit die aktive Nutzung entsprechender Produkte. Hinzu kommt, dass auch die (Ausfall-) Sicherheit beziehungsweise „Festigkeit" eines Produktes, also der Schutz vor Fehlfunktionen oder vor Cyberangriffen, wesentlicher Bestandteil der Nutzererfahrung ist, der mit zunehmender Abhängigkeit von IT mehr und mehr an Bedeutung gewinnt.

Wo stehen wir?

Dass sich Informationssicherheit und Anwenderfreundlichkeit nicht ausschließen, zeigen mittlerweile vielfach standardmäßig eingesetzte IT-Sicherheitsmaßnahmen. Beispielhaft zu nennen sind hier die Ende-zu-Ende-Verschlüsselung sowie die sogenannte Zwei-Faktor-Authentifizierung. Deren Anwenderfreundlichkeit ist Hauptgrund für ihre breite Verwendung.

Da jedoch Ausschreibungen von Sicherheitslösungen im Regelfall besonders preissensitiv sind, den Anwenderinnen und Anwendern in der Regel keine Nutzungsalternative zur Verfügung steht und die Nutzererfahrung bei der Realisierung in der Regel eine untergeordnete Rolle spielt, sind Sicherheitslösungen heute oftmals anwenderunfreundlich und werden in der Folge nicht genutzt.

Die bestehende Diskrepanz der Nutzerzahlen zwischen Messenger-Diensten und anderweitigen Sicherheitslösungen (zum Beispiel VPN-Lösungen) verdeutlicht, dass die fachliche Eignung eines Sicherheitsproduktes allein nicht ausreicht, um Anwenderinnen und Anwendern die sinnvolle Nutzung oder IT-Dienstleistern eine skalierbare Lösungsbereitstellung zu ermöglichen. Nur wenn bei der Entwicklung die drei Dimensionen „Sicherheit", „Anwenderfreundlichkeit" und „Betriebsführung" berücksichtigt werden, kann der erwünschte Sicherheitsgewinn auch entfaltet werden.

Was wollen wir erreichen?

Wir haben geprüft, inwiefern in der Bundesverwaltung eingesetzte Sicherheitslösungen entweder anwenderfreundlicher ausgeschrieben oder anwenderfreundliche Lösungen sicherer ausgestaltet werden können.

Wir fördern die Integration prüfbarer Sicherheitseigenschaften in anwenderfreundlichen, marktgängigen IT-Produkten. Best Practices hierfür sind unter anderem die am Markt gängigen Messenger-Apps, die mittlerweile zu einem Großteil Ende-zu-Ende-Verschlüsselung anbieten, ohne dass spürbare Einschränkungen in der Bedienbarkeit wahrnehmbar sind.

Welche Wirkung erwarten wir?

Anwenderfreundlichkeit, Ergonomie, aber auch Leistungsfähigkeit von Sicherheitslösungen entsprechen den erforderlichen, erwünschten sowie gleichermaßen erwarteten Eigenschaften marktgängiger Geräte und Lösungen. Marktgängige Lösungen werden mittels der Integration von IT-

Sicherheitseigenschaften sicherer. Nachdem Entwicklung und Sicherheitsbetrachtung neu ausgerichtet wurden, wird die (Investitions-) Bereitschaft für Einsatz und Nutzung sicherheitstechnischer Lösungen steigen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Bundesregierung hat Anforderungen an die Anwenderfreundlichkeit sicherheitstechnischer Lösungen in ihre Ausschreibungen aufgenommen.
- Die Forschung und Entwicklung im Bereich anwenderfreundlicher Sicherheitslösungen wurde intensiviert. Die Themen Usable Security und Security-by-Design haben verstärkt Einzug in Programme und Richtlinien der Forschungsförderung erhalten.
- Die Anzahl marktgängiger, anwenderfreundlicher Produkte, die IT-Sicherheitseigenschaften integriert haben, wie zum Beispiel Ende-zu-Ende-Verschlüsselung, ist gestiegen.
- Die Nutzung von Produkten mit IT-Sicherheitseigenschaften ist gestiegen.

8.1.3 Staatliche Angebote des digitalen Verbraucherschutzes ausbauen

Warum ist das Ziel relevant?

Durch die zunehmende Vernetzung von Informations- und Unterhaltungselektronik, Haushaltsgeräten oder anderen Gegenständen des täglichen Gebrauchs sowie die Nutzung digitaler Dienste entstehen neue Risiken und potenzielle Angriffsflächen. Sicherheit wird daher im Sinne eines "digitalen Verbraucherschutzes" immer wichtiger – für einzelne Anwenderinnen und Anwender ebenso wie für die Gesellschaft.

Wo stehen wir?

Die Bundesregierung widmet sich mit ihren Angeboten bereits der Information und Sensibilisierung der Verbraucherinnen und Verbraucher. So unterhält zum Beispiel das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) auf seiner Homepage ein Verbraucherportal und fördert die DsiN-Projekte „Digital-Kompass plus“[22] und den durch das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) geförderten „Digitalen Engel“[23] zur Befähigung von älteren Menschen in ländlichen Regionen. Ebenso stellt das BSI Broschüren und Wegweiser[24] für den digitalen Alltag zur Verfügung und stellt über die „Cyberfibel“[25] zusammen mit DsiN umfassende Hilfestellungen für Wissensvermittler im digitalen Verbraucherschutz bereit. Der digitale Verbraucherschutz wurde im Rahmen des IT-Sicherheitsgesetzes im Mai 2021 als Aufgabe des BSI etabliert und der gesamtgesellschaftliche Dialog zur Cybersicherheit verstetigt.

Verbandsklagerecht und Nutzung von Synergien mit Verbraucherzen-tralen

Verbraucherverbände können mittels des Verbandsklagerechts (zum Beispiel Unterlassungsklagegesetz oder Gesetz gegen unlauteren Wettbewerb) gerichtlich durchsetzen, dass Unternehmen bestimmte verbraucherschutzrechtswidrige Geschäftspraktiken unterlassen müssen, ohne dass die Verbände in eigenen Rechten betroffen sind. Das BSI kann mit seiner fachlichen Expertise im Bereich der IT-Sicherheit und im Rahmen seines gesetzlichen Auftrags dieses Vorgehen der Verbraucherzentralen mittelbar unterstützen, indem es informationstechnische Produkte zur Erfüllung seiner gesetzlichen Aufgaben untersucht und die hieraus gewonnenen Erkenntnisse unter Einhaltung der gesetzlichen Vorgaben Dritten zur Verfügung stellt. Ebenso darf das BSI die Verbraucherzentralen allgemein in Fragen der Sicherheit der Informationstechnik beraten. Im Ergebnis kann das BSI daher dazu beitragen, dass Synergieeffekte auch durch die Verbraucherzentralen zur Stärkung des Verbraucherschutzes im Bereich der IT-Sicherheit genutzt werden können.

[22] Abrufbar unter: https://www.digital-kompass.de/

[23] Abrufbar unter: https://www.digitaler-engel.org/

[24] Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Broschueren/broschueren_node.html

[25] Abrufbar unter: https://www.cyberfibel.de/

Was wollen wir erreichen?

Die staatlichen Angebote des digitalen Verbraucherschutzes sind ausgebaut und das Vertrauen der Bürgerinnen und Bürger in die staatliche Unterstützung bei der Nutzung neuer Technologien ist gestärkt. Das BSI steht als Ansprechpartner zur Verfügung und hat dazu sein Service- und Informationsangebot ausgebaut. Auf Basis einer erweiterten Marktbeobachtung für Verbraucherprodukte und -dienste sowie im Austausch mit den entsprechenden Anbietern stellt das BSI sicherheitsrelevante Informationen bereit.

Die Kooperation des BSI mit den Verbraucherzentralen führt zu Synergieeffekten im Bereich technischer Expertise und dem Verbandsklagerecht.

Über einen Beirat Digitaler Verbraucherschutz beim BSI sollen Vertreterinnen und Vertreter aus den etablierten Disziplinen des Digitalen Verbraucherschutzes das BSI in Fragen des Digitalen Verbraucherschutzes unabhängig beraten.

Welche Wirkung erwarten wir?

Mit einer zielgruppengerechten Ansprache durch Informationsübermittlung und Hilfestellung wird das Cybersicherheitsniveau und damit auch die gesellschaftliche Widerstandsfähigkeit gegen Cybergefahren jeglicher Art deutlich erhöht. Die Sicherheitseigenschaften von Verbraucherprodukten wurden als ein Kriterium zur Kaufentscheidung etabliert. Infolgedessen berücksichtigen mehr Hersteller die IT-Sicherheitsaspekte ihrer Produkte.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSI führt eine Marktbeobachtung von IT-Produkten und Dienstleistungen für den Verbrauchermarkt sowie eigene Testungen dieser durch.
- Das BSI hat für die grundsätzliche Beratung, Erfassung, Koordinierung, Beantwortung und Dokumentation von Anfragen der Zielgruppen Staat, Wirtschaft und Gesellschaft ein zentrales Service-Center eingerichtet (Multichannel First-Level-Support).
- Zielgruppenspezifische Bedarfe der Bürgerinnen und Bürger werden ermittelt, um diese Erkenntnisse in adressatengerechte Sensibilisierungsmaßnahmen einfließen zu lassen.
- Beim BSI ist ein Beirat Digitaler Verbraucherschutz dauerhaft etabliert.

8.1.4 Europäisch einheitliche Sicherheitsanforderungen

Warum ist das Ziel relevant?

Die Cybersicherheit von im Markt befindlichen Produkten, aber auch Diensten ist bisweilen unzureichend und auch nicht transparent nachvollziehbar. Diesem Umstand sollte mit einer Erhöhung des Cybersicherheitsniveaus auf europäischer Ebene begegnet werden. Insbesondere sollten EU-weit einheitlich verbindliche IT-Sicherheitsanforderungen eingeführt werden.

Wo stehen wir?

Unter der deutschen EU-Ratspräsidentschaft 2020 wurden Ratsschlussfolgerungen zur Cybersicherheit vernetzter Geräte erarbeitet, die einen wichtigen Anstoß für EU-weit einheitliche, anerkannte und rechtlich verbindliche IT-Sicherheitsanforderungen gegeben haben. Um Verbraucherinnen und Verbrauchern ein klareres Verständnis von in Produkten vorhandenen Cybersicherheitseigenschaften zu ermöglichen, wird mit dem IT-Sicherheitsgesetz 2.0 ein nationales freiwilliges IT-Sicherheitskennzeichen eingeführt.

Was wollen wir erreichen?

Verbraucherinnen und Verbraucher können darauf vertrauen, dass Produkte und Dienste einem angemessenen Cybersicherheitsniveau entsprechen und die Einhaltung der erforderlichen Cybersicherheitseigenschaften europaweit einheitlich geregelt ist.

Die Konformität zu EU-weit gültigen, verbindlichen IT-Sicherheitsanforderungen wird in geeigneter Weise auf den Produkten transparent gemacht. Die Bundesregierung hat das nationale, freiwillige IT-Sicherheitskennzeichen als möglichen Ansatz in die Diskussion eingebracht.

Welche Wirkung erwarten wir?

Verbraucherinnen und Verbraucher werden durch die Nutzung gekennzeichneter Produkte geschützt und ihr Vertrauen in diese wird erhöht. Durch verbindliche IT-Sicherheitsanforderungen werden das Cybersicherheitsniveau im europäischen Binnenmarkt insgesamt erhöht sowie das Sicherheitsbewusstsein in Unternehmen und Wissenschaft gestärkt. Infrastruktur, Mitarbeitende, Produkte und Dienstleistungen werden resilienter gegen Cyberangriffe. Gleichzeitig wird durch verbindliche IT-Sicherheitsanforderungen die Wettbewerbsfähigkeit europäischer Unternehmen gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Infrastrukturen und Kompetenzen zur Marktüberwachung wurden beim BSI aufgebaut und genutzt und kommen insbesondere beim IT-Sicherheitskennzeichen zum Einsatz.
- Das IT-Sicherheitskennzeichen wird in der Fläche von Verbraucherinnen und Verbrauchern sowie Herstellern oder Dienstleistern angenommen und akzeptiert, die Anzahl erteilter nationaler IT-Sicherheitskennzeichen steigt kontinuierlich.
- Es werden verbindliche IT-Sicherheitseigenschaften auf EU-Ebene eingeführt und durch ein geeignetes europäisches Kennzeichen (zum Beispiel die CE-Kennzeichnung oder als

explizites IT-Sicherheitskennzeichen) für Verbraucherinnen und Verbraucher transparent gemacht.

- Verbindliche IT-Sicherheitsanforderungen für IT-Verbraucher-Produkte werden in Folge der Ratsschlussfolgerungen zur Cybersicherheit vernetzter Produkte auf europäischer Ebene vorbereitet und umgesetzt.

8.1.5 Sichere elektronische Identitäten gewährleisten

Warum ist das Ziel relevant?

Im digitalen Zeitalter sind sichere elektronische Identitäten (eIDs) wesentlich für viele alltägliche Tätigkeiten. Sie sind relevant für Wirtschaft, Wissenschaft und private Nutzende. Für staatliches Handeln sind sie sogar ein unverzichtbarer Grundbaustein. Die Festlegung von Anforderungen an eID-Verfahren sowie deren Absicherung sollten daher durch den Staat erfolgen, damit eine einheitliche übergreifende Lösung für alle Anwendungsbereiche geschaffen wird.

Vertrauenswürdige eIDs stärken die Digitale Souveränität und den Binnenmarkt Europas, indem sie einen digitalen Identitätsnachweis gegenüber Diensteanbietern im Internet ermöglichen. Eine Digitalisierung der Verwaltung (zum Beispiel Umsetzung des OZG) setzt sichere und nutzerfreundliche Identitäten voraus. Für deren Umsetzung und als Basis für ein Identitätsökosystem mit der Wirtschaft werden geeignete, in der Bevölkerung breit akzeptierte elektronische Identifizierungsmittel mit der dazugehörigen eID-Infrastruktur benötigt.

Elektronische Identitäten haben das Potenzial, die wirtschaftliche Entwicklung von Volkswirtschaften zu fördern - durch Optimierung von Prozessen und Lieferketten, den nahtlosen und sicheren Austausch vertrauenswürdiger Informationen, Zeitersparnis für Bürgerinnen, Bürger und Unternehmen sowie die Reduktion von Betrugsmöglichkeiten. Dieses Potenzial gilt es auch für Deutschland flächendeckend zu erschließen. Ein zentraler Baustein dafür ist die staatliche deutsche Online-Ausweisfunktion: Dieses international als hochsicher anerkannte Identifizierungsmittel (gemäß eIDAS-Verordnung für das höchstmögliche Vertrauensniveau notifiziert) ist die Grundlage für die hoheitliche Identifizierung. Identität hat jedoch viele Facetten und ist je nach Anwendungsfall deutlich weiter zu verstehen als nur die Angaben auf dem Personalausweis, dem elektronischen Aufenthaltstitel oder der eID-Karte für Bürgerinnen und Bürger der EU, die bei der Online-Ausweisfunktion verwendet werden. Neben der Möglichkeit, mit Hilfe der Online-Ausweisfunktion nachzuweisen, dass Ausweisinhaberinnen und -inhaber sind, wer sie behaupten zu sein, können daher weitere Attribute für weitere digitale Identitäten bedeutend sein, zum Beispiel ein bestimmter Schul- oder Studienabschluss.

Wo stehen wir?

Bürgerinnen und Bürger erledigen Behördliches und Geschäftliches zunehmend mit ihren Smartphones. Sie sollen daher künftig ihre Online-Ausweisfunktion direkt in ihren Smartphones speichern können und sich künftig auch ohne Ausweiskarte nur mit dem Smartphone innerhalb weniger Sekunden sicher digital ausweisen können.

Um das Potenzial von eIDs zu identifizieren, wurde eine interministerielle Projektgruppe gegründet mit dem Ziel, die digitale Identität im Alltag einfacher und komfortabler nutzbar zu machen.

Das BSI gestaltet dafür sichere eIDs durch die Entwicklung von Spezifikationen und die Mitarbeit bei der Pilotierung und Umsetzung neuer Technologien, insbesondere für das smartphonebasierte Online-Ausweisen. Zugleich soll das kartenbasierte Online-Ausweisen für die Bürgerinnen und Bürger durch neue Zusatzdienste und Verbesserungen nutzerfreundlicher werden. Auch privatwirtschaftliche Unternehmen unterhalten auf Basis ihrer Geschäftsmodelle ein umfassendes

Identitätsmanagement. Der sichere staatliche Online-Ausweis kommt hierbei teilweise zum Einsatz, ist aber ein Identifizierungsangebot neben anderen Angeboten. Die verschiedenen Identifizierungsangebote sind in der Regel nicht interoperabel und hinsichtlich der Datenverwendung unterschiedlich ausgestaltet. Zudem ist der Markt stark fragmentiert. Mit der zunehmenden Durchdringung immer weiterer Lebensbereiche mit Technologie sowie den Geschäftsinteressen der privatwirtschaftlichen Anbieter von Identifizierungslösungen bedarf es zur Stärkung der Digitalen Souveränität eines verstärkten staatlichen Angebotes, das Sicherheit, Datenschutzkonformität, Selbstsouveränität, Nutzerfreundlichkeit sowie flexible und weitverbreitete Einsatzmöglichkeiten bietet.

Was wollen wir erreichen?

Der Online-Ausweis auf dem Smartphone ist aus dem Personalausweis abgeleitet und kann im Sicherheitselement des Smartphones gespeichert werden. Diese Smart-eID kann neben der Ausweiskarte für den Identitätsnachweis im Internet gegenüber Unternehmen und Behörden verwendet werden. Die Wirtschaft bietet mehr Anwendungen für den Online-Ausweis und die Smart-eID an. Die Smart-eID ist seitens der Europäischen Kommission notifiziert und somit ein EU-weit anerkanntes Identifizierungsmittel.

Welche Wirkung erwarten wir?

Mit dem Online-Ausweis auf dem Smartphone werden die breite Akzeptanz und Verbreitung der eID-Sicherheitsinfrastruktur in Deutschland geschaffen beziehungsweise ausgebaut und ein Beispiel für sichere Smartphone-Anwendung in der EU gegeben.

Sichere, staatlich geprüfte eIDs schaffen Vertrauen in Technologie, sie schaffen neue Möglichkeiten der Wertschöpfung und schützen unter anderem vor Straftaten auf Basis digitalen Identitätsdiebstahls.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl der Downloads und Installationen der Ausweis-App2 (inklusive Ausweis-Applet) auf dem Smartphone ist gestiegen.
- Die Anzahl aktiver Nutzerinnen und Nutzer des Online-Ausweises ist gestiegen.
- Die Anzahl der Internetangebote für den Online-Ausweis ist gestiegen.
- Die Smart-eID ist seitens der Europäischen Kommission notifiziert und somit ein EU-weit anzuerkennendes Identifizierungsmittel.
- Ein Identitätsökosystem mit der Wirtschaft wurde pilotiert.
- Die Smart-eID ist für das Smartphone bereitgestellt. Es wird eine sichere eID-Infrastruktur für Smartphones angeboten.
- Das kartenbasierte Online-Ausweisen mit dem Personalausweis, dem elektronischen Aufenthaltstitel und der eID-Karte für Unionsbürgerinnen und -bürger ist anwendungsfreundlich ausgestaltet.

8.1.6 Elektronische Identitäten (von Personen und Dingen) im weiteren Sinne und Authentizität und Integrität von Algorithmen, Daten und Dokumenten absichern

Warum ist das Ziel relevant?

Die fortschreitende Digitalisierung ist bereits heute das Ergebnis einer enormen Vernetzung von physischen Objekten, Algorithmen, Daten, Dokumenten und Personen. Die Anzahl und auch die Vernetzung der Teilnehmenden unterschiedlicher digitaler Netzwerke wird in Zukunft stetig zunehmen. Beispiele hierfür sind unter anderem IoT, vernetzte Fahrzeuge, verteilte KI-Systeme, Energienetzwerke und digitale Lernplattformen. Eine Absicherung der Identitäten (Personen und Objekte) beziehungsweise der Authentizität und Integrität (Daten, Algorithmen und Dokumente) der Teilnehmenden dieser Netzwerke ist Grundvoraussetzung für das Vertrauen in diese Netzwerke und damit für die Digitalisierung.

Wo stehen wir?

Identitäten spielen aktuell eine zentrale Rolle in der Digitalisierung. Neben der Identität einer Person aus dem Online-Ausweis[26] gibt es zahlreiche weitere Identitäten, die stetig an Bedeutung zunehmen. Hierzu zählen neben den nicht hoheitlichen Identitäten von Personen, wie zum Beispiel der Schülerausweis und Identitäten von Personen in elektronischen Medien (mediale Identitäten), auch die Identitäten physischer Objekte, wie zum Beispiel von Fahrzeugen oder Sensoren. Zudem spielen die Authentizität und die Integrität von Algorithmen (etwa neuronalen Netzen), von Dokumenten (zum Beispiel Zeugnissen) und von Daten (zum Beispiel Flugrouten und Start- und Landeanweisungen im Luftverkehr) eine bedeutende Rolle.

Diese Identitäten beziehungsweise ihre Authentizität und Integrität können mit hinreichendem Aufwand gefälscht werden. Dies kann Schäden hinsichtlich Finanzen, Gesundheit und persönlicher Reputation nach sich ziehen. Vulnerabilitäten und angemessene Verteidigungsstrategien sind in vielen Fällen Gegenstand aktueller Forschung. So wird die Fälschung medialer Identitäten mittels Methoden der KI (Deep Fakes) auch für Laien immer einfacher und kann für Betrugsversuche oder zur gezielten Beeinflussung von Meinungen eingesetzt werden.

Was wollen wir erreichen?

Die Sicherheit der Identifikation von Teilnehmenden digitaler Netzwerke in unterschiedlichen Anwendungsgebieten ist erhöht. Hierzu werden Grundlagentechnologien wie biometrische Verfahren und hardwarebasierte Identifikationsmerkmale (Physical Unclonable Functions) zusammen mit deren Widerstandsfähigkeit gegenüber Angriffen untersucht und dokumentiert, sowie robuste Absicherungsmethoden entwickelt. Automatisierte Medienfälschungen, insbesondere mittels Methoden der KI, und Angriffe auf biometrische Systeme, zum Beispiel durch die Fusion der biometrischen Merkmale mehrerer Personen (Morphing), wurden einerseits nachvollzogen, andererseits wurden Detektions- und Verteidigungsmaßnahmen grundlegend verbessert. Bewer-

[26] Vergleiche strategisches Ziel 8.1.5 „
Sichere elektronische Identitäten gewährleisten“.

tungsverfahren für Authentisierungs- und Identifizierungsverfahren, die das erforderliche Vertrauensniveau berücksichtigen, werden entwickelt und mittelfristig in Form von Technischen Richtlinien veröffentlicht. Auf dieser Grundlage werden anschließend die Erkenntnisse in nationale und internationale Standardisierungsgremien eingebracht. Public Key Infrastrukturen (technische und organisatorische Infrastrukturen, kurz PKI), die es ermöglichen, kryptografische Schlüsselpaare auszurollen und zu verwalten, werden sicherer gemacht und eID-Interoperabilitätsinfrastrukturen umgesetzt und gepflegt.

Die Integritätssicherung, der Echtheitsnachweis und, bei Bedarf, die Langzeitsicherung von Dokumenten und Daten aus verschiedenen Anwendungsbereichen, wie intelligente Transportsysteme, Smart Metering, Industrie 4.0, elektronische Aufzeichnungssysteme, digitale Bildung, sind mittels verschiedener Technologien weiterentwickelt. Wo möglich und sinnvoll sollten bestehende Standards berücksichtigt werden.

Welche Wirkung erwarten wir?

Mit der Erhöhung der Sicherheit digitaler Netzwerke wird deren Betrieb robuster und das Vertrauen in sie gestärkt. Hierdurch erfolgen eine verstärkte Nutzung und damit insgesamt eine beschleunigte Digitalisierung.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Bewertungsverfahren für Authentisierungs- und Identifizierungsverfahren, die das erforderliche Vertrauensniveau berücksichtigen, wurden entwickelt und einheitlich etabliert. Beispielsweise sind die Sicherheitsanforderungen an Identifizierung- und Authentisierungsmethoden für den Zugang zu digitalen Bildungsangeboten standardisiert.
- In der Biometrie wurden die Aspekte unterschiedlicher Angriffsmethoden detailliert untersucht und dokumentiert und deren Prävention und Detektion systematisch verbessert und praxistauglich umgesetzt. Entsprechende technische Richtlinien wurden veröffentlicht beziehungsweise fortentwickelt.
- Methoden zur zuverlässigen Identifikation drahtloser Geräte mithilfe von Physical Fingerprinting (individuelle Merkmale ihrer elektronischen Bauteile) wurden entwickelt und demonstriert.
- Die Sicherheit von PKI, die dem Ausrollen und Verwalten von kryptografischen Schlüsselpaaren dienen, wurde fortentwickelt, eID-Technologien und PKI wurden fortentwickelt und sichere eID-Interoperabilitätsinfrastrukturen wurden etabliert. Sie werden regelmäßig gepflegt. Ein PKI-Baukasten für Digitalisierungsprojekte wurde etabliert durch die Modularisierung von PKI-Vorgaben und einheitliche Vorgaben für Sicherheitselemente.
- Die Sicherheit von Integritätssicherungsverfahren und Langzeitsicherungstechnologien, basierend auf Technischen Richtlinien des BSI, ist wesentlich erhöht. Entsprechende Technische Richtlinien wurden dementsprechend weiterentwickelt.

- Ein sicherer Siegelserver, der die Überprüfbarkeit von Herkunft und Integrität elektronischer Dokumente sicherstellt, wurde umgesetzt, und digitale Siegel beziehungsweise signierte Barcodes zum Integritätsschutz und zum Echtheitsnachweis von Papierdokumenten und Daten wurden für neue Anwendungsgebiete fortentwickelt.

8.1.7 Voraussetzungen für sichere elektronische Kommunikation und sichere Web-Angebote schaffen

Warum ist das Ziel relevant?

Eine sichere und interoperable Kommunikation und sichere Webangebote sind Grundvoraussetzungen für eine erfolgreiche Digitalisierung in verschiedensten Anwendungsbereichen, wie zum Beispiel der Fahrzeug-zu-Fahrzeug- und der Fahrzeug-zu-Cloud-Kommunikation, der elektronischen Post, dem Gesundheitswesen und der Umsetzung des OZG.

Wo stehen wir?

Im Bereich der Umsetzung des OZG hat das BSI Vorgaben in Form Technischer Richtlinien an den Betrieb interoperabler Nutzerkonten (Bürgerkonten) als Identifizierungskomponenten für Online-Verwaltungsleistungen formuliert, mit Bund und Ländern abgestimmt und veröffentlicht. Eine Umsetzung der Anforderungen durch die Lösungen von Bund und Ländern steht noch aus. Parallel sind im Rahmen einer Pilotierung Vorgaben an Postfächer der interoperablen Nutzerkonten zu formulieren und umzusetzen.

Im Bereich der Telematikinfrastruktur 2.0 stimmt das BSI zurzeit mit der gematik GmbH die Konzeption für die Telematikinfrastruktur 2.0 ab. Geplante Finalisierung der Abstimmung ist Ende 2021.

Was wollen wir erreichen?

Ziel ist die (Fort-)Entwicklung anwendungsspezifischer kryptografischer Vorgaben für die sichere und interoperable Verwendung von Kommunikationsprotokollen und deren Einbringung als Stand der Technik in Gesetzesvorhaben. Anwendungsspezifische kryptografische Vorgaben, Prüfkriterien und Profile werden für weitere Anwendungsfälle erweitert, unter anderem für den Mobilitätsbereich, den Gesundheitsbereich, die Verwaltung und den Bereich Industrie 4.0.

Welche Wirkung erwarten wir?

Durch eine geeignete Umsetzung der Maßnahmen ist ein gesteigertes Vertrauen in die Digitalisierung in wichtigen Anwendungsgebieten und damit eine verstärkte Nutzung entsprechender Produkte zu erwarten.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Im Mobilitätsbereich ist die IT-Sicherheit der Kommunikation zwischen Fahrzeugen und der Cloud-Anbindung von Fahrzeugen erhöht.
- In der kontinuierlichen Fortentwicklung der Telematikinfrastruktur sind sowohl die Nutzung stationärer Anwendungen als auch neu eingeführte mobile Nutzungsmöglichkeiten von TI-Anwendungen für Versicherte und Leistungserbringer zu jedem Zeitpunkt sicher.
- Neben De-Mail steht der Verwaltung mit den Postfächern der Interoperablen Nutzerkonten ein weiterer sicherer Kommunikationsweg zur Verfügung. Dies wird durch eine mit

Bund und Ländern abgestimmte Technische Richtlinie des BSI sichergestellt. Zur sicheren Umsetzung des OZG wurde eine Technische Richtlinie erstellt.

8.1.8 Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure fördern

Warum ist das Ziel relevant?

Das zügige Schließen erkannter Sicherheitslücken in Systemen, Produkten und Dienstleistungen ist ein Eckpfeiler der Cybersicherheit. Wer eine Sicherheitslücke entdeckt, sollte sich unmittelbar und vertrauensvoll an den Hersteller des betroffenen Produktes beziehungsweise an den Anbieter der betroffenen Dienstleistung wenden, damit erkannte Sicherheitslücken in einem angemessenen Zeitraum mittels eines Patches oder Updates geschlossen werden. Dabei muss sorgsam abgewogen werden, ob eine öffentliche Kommunikation der Sicherheitslücken erfolgen sollte, bevor entsprechende Updates oder Patches verfügbar sind. Die Umsetzung dieser Anforderungen in einem abgestimmten Prozess nennt sich Coordinated Vulnerability Disclosure (CVD).

Wo stehen wir?

In der Praxis besteht bis heute kein allgemein gültiger Rahmen, der beschreibt, welche Akteure in welchem Umfang und mit welchen Methoden und Instrumenten Sicherheitslücken finden und den Herstellern melden dürfen. Die Frage des Umgangs wird deshalb von den Unternehmen selbst beantwortet. Dies führt dazu, dass einige Unternehmen unter anderem Bug-Bounty-Programme (Initiativen zur Identifizierung, Behebung und Bekanntmachung von Fehlern) unterhalten, um einen monetären Anreiz für ein koordiniertes Vorgehen (im Sinne des CVD) zu bieten, und andere Unternehmen gerichtlich gegen das Aufdecken vorgehen, weil sie ihre Rechte verletzt sehen. In der Folge besteht Unsicherheit, die dazu führt, dass gewisse Softwareprodukte nicht mehr untersucht werden oder aber Erkenntnisse zu kritischen Sicherheitslücken nicht zeitnah den Herstellern gemeldet werden.

Was wollen wir erreichen?

Zur Stärkung einer proaktiven Schwachstellen-Governance genießen innerhalb eines von der Bundesregierung entwickelten Rahmens Handelnde Rechtssicherheit, wenn sie mit ihren Erkenntnissen über Sicherheitslücken an betroffene Unternehmen herantreten. Sie haben zuverlässige Kontaktstellen, denen sie ihre Erkenntnisse melden können. Dies können eine verpflichtend einzurichtende Kontaktstelle im Unternehmen selbst oder das BSI als öffentliche und vermittelnde Stelle sein.

Der Gesetzgeber nimmt die betroffenen Unternehmen in die Pflicht, Kontaktstellen sowie Prozesse vorzuhalten, um gemeldete Schwachstellen in einem angemessen kurzen Zeitraum schließen zu können. Dabei wird geprüft, inwiefern Rechte und Pflichten auf beiden Seiten des CVD geregelt werden, beispielsweise eine Sperrfrist für Veröffentlichungen, eine verbindliche Frist für Patches oder Updates. Es existiert ein zwischen BSI und Herstellern oder Dienstleistern koordiniertes Vorgehen, das über den reinen Informationsaustausch hinausgeht. Dies betrifft auch Schwachstellen in den IT-Lieferketten von Produkten und Dienstleistungen (Supply Chain Security).

IT-Sicherheitslücken werden einerseits schnellstmöglich an betroffene Unternehmen gemeldet. Andererseits bestehen unternehmensinterne Prozesse, die eine zügige Prüfung und Schließung der gemeldeten Sicherheitslücke in Form eines Patches oder Updates ermöglichen.

Das BSI ist auf Basis seines CVD-Prozesses an dem Austausch beteiligt. Hierdurch unterstützt es das Melden von Sicherheitslücken als neutrale und fachlich kompetente Vermittlungsinstanz. Es warnt gegebenenfalls öffentlichkeitswirksam und bringt Erkenntnisse der Schwachstellenlandschaft in das nationale Cyberbedrohungslagebild sowie in die allgemeine und branchenspezifische Gefährdungslage (insbesondere Kritische Infrastrukturen) ein. Anwenderinnen und Anwender werden schnellstmöglich vor Sicherheitslücken gewarnt und über mögliche Schutzmaßnahmen informiert.

Es wird sichergestellt, dass vertrauliche Detailinformationen über Sicherheitslücken nicht an Unbefugte gelangen, bevor entsprechende Patches oder Updates bereitstehen. Die speziellen Interessen der Sicherheitsbehörden werden in dem strategischen Ziel 8.3.10 „Den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits fördern“Den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits fördern adressiert.

Welche Wirkung erwarten wir?

Anwenderinnen und Anwender, Kritische Infrastrukturen und Institutionen von besonderem öffentlichen Interesse sind besser vor Cyberangriffen geschützt, da IT-Sicherheitslücken in Systemen, Produkten und Dienstleistungen zügig kommuniziert und behoben werden, geeignete Schutzmaßnahmen ergriffen werden und vertrauliche Detailinformationen über IT-Sicherheitslücken vor der Behebung des Problems nicht in die Hände maliziöser Cyberakteure gelangen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es besteht Rechtssicherheit für das Suchen und Finden von Sicherheitslücken.
- Die Bundesregierung regelt die Beteiligung des BSI an CVD-Ereignissen und veröffentlicht einen abgestimmten Prozess zur verantwortungsvollen Veröffentlichung von Schwachstellen (CVD-Prozess).
- Entdeckte Sicherheitslücken werden zunehmend gemeldet.
- Anreizstrukturen für Hersteller und Dienstleister, gemeldete Lücken in einem angemessenen Zeitraum zu schließen, wurden gestärkt.

8.1.9 Verschlüsselung als Voraussetzung eines souveränen und selbstbestimmten Handelns flächendeckend einsetzen

Warum ist das Ziel relevant?

Verschlüsselung stellt die Wahrung von Vertraulichkeit, Integrität und Authentizität digitaler Informationen sicher und ist deshalb ein wesentlicher Eckpfeiler der Cyber- und Informationssicherheit. Der Einsatz von Verschlüsselungsverfahren schützt die Nutzenden aus Staat, Wirtschaft und Gesellschaft effektiv vor Diebstahl, Spionage oder Sabotage persönlicher, geschäftlicher oder hoheitlicher digitaler Information und Kommunikation. Sie schaffen Vertrauen und erhöhen dadurch die Akzeptanz für die Nutzung neuer Technologien. Allerdings sind Verschlüsselungsverfahren einem sich ständig verändernden Bedrohungspotential ausgesetzt, was deren kontinuierliche Bewertung und Fortentwicklung zwingend erforderlich macht.

Mit zunehmenden Entwicklungen im Bereich Quantentechnologie verschärft sich diese Notwendigkeit, da viele heute eingesetzte Verschlüsselungsverfahren zukünftig nicht mehr sicher sein werden. Dieses Ziel fokussiert auf die Interessen der Gesellschaft und Wirtschaft. Die speziellen Interessen der Sicherheitsbehörden werden in dem strategischen Ziel 8.3.9 „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten“ adressiert.

Wo stehen wir?

Seit Veröffentlichung der letzten Cybersicherheitsstrategie im Jahr 2016 hat sich der Einsatz von Verschlüsselungsverfahren vor allem im Bereich der Unternehmen und Organisationen aus Sicht der Cyber- und Informationssicherheit positiv entwickelt. Unternehmen schützen ihre Organisationsnetzwerke mit VPN-Lösungen oder nehmen entsprechende verschlüsselte IT-Dienstleistungen in Anspruch.

Private Nutzende wiederum profitieren von den sicheren Angeboten der Ende-zu-Ende-verschlüsselten Messenger-Dienste, den mittlerweile weitgehend standardisiert eingesetzten TLS-Protokollen im World Wide Web oder dem zunehmenden Einsatz von Verschlüsselung bei Cloud-Dienstleistungen.

Dabei bleibt festzuhalten, dass ein Großteil der Nutzenden in Deutschland (außer in Messenger-Diensten) kaum Verschlüsselungslösungen (zum Beispiel VPN-Apps) nutzt und die Absicherung ihrer Informationen den kommerziellen Anbietern überlässt. Doch gerade im rasant wachsenden Markt des IoT sind verschlüsselte Produkte bislang in der Minderzahl. Diese Entwicklung ist bedenklich, da IoT-Produkte künftig in besonderem Maße in das tägliche Leben integriert werden, ohne die entstehenden Daten eigenständig abzusichern. Dieses Verhalten vergrößert die Angriffsfläche erheblich. Mittels Verschlüsselung könnte die Nutzung von IoT erheblich sicherer werden.

Was wollen wir erreichen?

Die Bundesregierung schafft Vertrauen und Verlässlichkeit in die Digitalisierung, indem sie auch weiterhin den flächendeckenden Einsatz sicherer Verschlüsselungstechnologien fördert und sich für den Abbau rechtlicher, wirtschaftlicher und technischer Hemmnisse beim Einsatz von Verschlüsselungslösungen einsetzt.

Dabei setzt sich die Bunderegierung international gegen die Einführung von Verboten des Einsatzes von Verschlüsselungstechnologien ein und sieht auch von eigenen Verboten ab.

Weiterhin fördert die Bundesregierung die Entwicklung neuer Verschlüsselungslösungen, insbesondere im Bereich der Post-Quanten-Kryptografie, indem sie die Kryptologie als wissenschaftliche Disziplin fördert, Marktanreize zur Produktentwicklung setzt, verstärkt Eigenentwicklungen und Entwicklungsbeteiligungen anstößt und am Markt verfügbare Produkte mittels Zulassung und Zertifizierung auf ihre Verlässlichkeit hin prüft.

Welche Wirkung erwarten wir?

Die konsequente Verschlüsselung digitaler Kommunikation und Speicherung erschwert den unerlaubten Zugriff und die Ausnutzung erheblich. Staat, Wirtschaft und Gesellschaft werden besser vor Cyberrisiken geschützt. Des Weiteren schaffen sichere Kommunikationsmöglichkeiten Vertrauen und Verlässlichkeit in einer digitalisierten Umgebung. Dies eröffnet Chancen für die Digitalisierung weiterer Lebensbereiche, für neue Geschäftsmodelle und weitere technische Innovationen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es wurden Initiativen zur Förderung von Verschlüsselung in Wissenschaft, Wirtschaft, Gesellschaft sowie in internationale Gremien, die diesen Zweck verfolgen, eingebracht.
- Es wurden weitere Initiativen nach dem Vorbild der Implementierung von Post-Quanten-Kryptografie in Open Source Produkten etabliert.
- Die Höhe der Fördermittel für Grundlagen- und Anwendungsforschung in der Kryptografie ist gestiegen.
- Die Anzahl geprüfter und zugelassener beziehungsweise zertifizierter Verschlüsselungslösungen ist gestiegen.
- Bürgerinnen und Bürger sowie Unternehmen verwenden mehr sicher verschlüsselte Kommunikationsmittel.

8.1.10 IT-Sicherheit durch KI und IT-Sicherheit für KI gewährleisten

Warum ist das Ziel relevant?

KI ist eine der zentralen Schlüsseltechnologien des 21. Jahrhunderts und Treiber für die fortschreitende Digitalisierung von Produkten, Dienstleistungen und Prozessen. Bereits heute beeinflusst KI sicherheitskritische Prozesse und Entscheidungen, zum Beispiel im Kontext von Biometrie, Gesundheitswesen oder Mobilität.

Für Cybersicherheit ergeben sich durch den zunehmenden Einsatz von KI neue Chancen, aber auch Risiken: Mithilfe von KI-Systemen können Sicherheitslücken identifiziert oder Angriffe zeitnah erkannt und abgewehrt werden. Bestehende Instrumente zur Verteidigung gegenüber Cyberangriffen können effizienter gestaltet und neue Instrumente entwickelt werden.

Gleichzeitig führt der verstärkte Einsatz KI-basierter Systeme für die Automatisierung von Prozessen und Entscheidungen zu neuen Sicherheitsbedrohungen, die von etablierten IT-Sicherheitsstandards bisher nicht abgedeckt werden.

KI-Strategie für Deutschland

KI birgt als Schlüsseltechnologie großes Potenzial für Wirtschaftswachstum und Produktivitätszuwächse. Um dieses Potenzial zum Wohle der Menschen und der Umwelt verantwortungsvoll, sicher und gemeinwohlorientiert zu fördern und zu nutzen, hat die Bundesregierung mit der „Strategie Künstliche Intelligenz“ (KI-Strategie) einen Handlungsrahmen entwickelt und weitreichende Maßnahmen beschlossen.

Mit der 2018 verabschiedeten und 2020 fortgeschriebenen Strategie hat die Bundesregierung ihr Engagement für die Zukunftstechnologie KI weiter gestärkt: Bis 2025 werden die Investitionen des Bundes für KI aus Mitteln des Konjunktur- beziehungsweise Zukunftspaketes von drei auf fünf Milliarden Euro erhöht.

Die Strategie ist abrufbar unter https://www.ki-strategie-deutschland.de/home.html.

Wo stehen wir?

KI-basierte Systeme werden zunehmend genutzt und kommen in verschiedensten Szenarien zum Einsatz. Bislang fehlen einheitliche Kriterien, Methoden und Werkzeuge zur Bewertung von KI-Systemen. Mit dem derzeit auf europäischer Ebene verhandelten Verordnungsentwurf AI Act[27] der Kommission werden jedoch Regulierungsanforderungen mit entsprechenden Prüfkriterien entwickelt, die dann auch in Deutschland umgesetzt werden müssen. Die Bundesregierung fördert verschiedene Maßnahmen in Forschung und Wirtschaft im Bereich KI. Sie bringt ihre Expertise in nationale und internationale Standardisierungsprozesse ein und gestaltet damit aktiv Normen und Standards.

Was wollen wir erreichen?

KI-Systeme erreichen ein von ihrem jeweiligen Einsatzzweck abhängiges, möglichst hohes IT-Sicherheitsniveau und werden gleichzeitig zur Gewährleistung eines hohen IT-Sicherheitsniveaus

[27] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206

eingesetzt (IT-Sicherheit für KI und IT-Sicherheit durch KI). Die Einsatzmöglichkeiten von KI-Systemen zum Schutz von (staatlichen) IT-Systemen werden hierfür fortlaufend geprüft.

Der Regulierungsrahmen von IT-Sicherheitsanforderungen schließt die Sicherheit von KI-Systemen mit ein. Für KI-Systeme gibt es klar definierte IT-Sicherheitsanforderungen, welche die Besonderheiten der Systeme berücksichtigen. Die Sicherheitseigenschaften von KI-basierten Systemen können durch effektive und effiziente Prüfkriterien und -methoden evaluiert werden. Diese berücksichtigen insbesondere auch neuartige Angriffstechniken, die die spezifischen Eigenschaften von KI-Systemen ausnutzen. Dies gilt es insbesondere auch im europäischen AI Act zu berücksichtigen, damit dort hohe IT-Sicherheitsstandards gesetzt werden für KI-Anwendungen, deren Risiko als hoch bewertet wird.

IT-Sicherheit ist ein Grundbaustein, der bei der Entwicklung von KI-Systemen berücksichtigt wird (Security-by-Design). Diese erfüllen ein von ihrem jeweiligen Einsatzzweck abhängiges IT-Sicherheits-Niveau.

Neben dem Schutz KI-basierter Systeme (IT-Sicherheit für KI) werden KI-basierte Systeme auch für bessere Analyse- und Darstellungsformate sowie bessere Schutzmaßnahmen genutzt (IT-Sicherheit durch KI). Insbesondere werden diese bei der Erkennung von Angriffen auf Netzwerke oder durch die Sicherheitsbehörden im Rahmen der Strafverfolgung eingesetzt. Dabei ist zu beachten, dass es insbesondere in Bezug auf Hasskriminalität immer einer Beurteilung des Kontextes bedarf, die KI nicht leisten kann.

In einem gemeinsamen Prozess mit Partnern aus Forschung, Wirtschaft und Verwaltung entwickelt die Bundesregierung die technologischen Grundlagen zur Bewertung solcher Systeme und überführt sie in die Praxis. Dabei setzt sich die Bundesregierung für die Durchsetzung europäischer Werte in KI-Produkten und KI-Dienstleistungen weltweit ein.

Welche Wirkung erwarten wir?

Durch die Gewährleistung einer nachweisbaren Sicherheit von KI wird ein wichtiger Grundstein für die Akzeptanz und den Erfolg dieser für die Digitalisierung essenziellen Schlüsseltechnologie gelegt. Nur so können die Chancen der Technologie für Staat, Wirtschaft und Gesellschaft ausgeschöpft werden. Zudem wird so das Vertrauen der Benutzerinnen und Benutzer in KI-basierte Systeme aufgebaut und aufrechterhalten.

Gleichzeitig wird die Sicherheit von Staat, Wirtschaft und Gesellschaft durch den Einsatz von KI für IT-Sicherheitsanwendungen sowie durch die bessere Absicherung von KI-Systemen erhöht. Im Ergebnis werden auch die nationale und die europäische Wirtschaft gefördert und damit die Digitale Souveränität in einem globalen KI-Markt gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl und Qualität wissenschaftlicher Publikationen, die sich mit KI-spezifischen Angriffsvektoren und entsprechenden Gegenmaßnahmen und deren Einsatz in relevanten Anwendungsbereichen auseinandersetzen, ist signifikant gestiegen.

- Die Bundesregierung hat erfolgreich darauf hingewirkt, dass IT-Sicherheitsaspekte in der kommenden KI-Regulierung auf EU-Ebene sowie in der Umsetzung auf nationaler Ebene angemessen berücksichtigt werden.
- Es wurden Prüfkriterien, -werkzeuge und -methoden entwickelt, um Cybersicherheitsaspekte KI-basierter Systeme zu evaluieren. In relevanten, besonders kritischen Anwendungsbereichen wurden hierzu entsprechende Technische Richtlinien veröffentlicht, die als Grundlage für Standardisierungsvorhaben genutzt werden.
- KI-Systeme werden verstärkt und erfolgreich zur Angriffserkennung und -abwehr eingesetzt.

8.2 Handlungsfeld 2: Gemeinsamer Auftrag von Staat und Wirtschaft

Unternehmen in Deutschland sind regelmäßig Ziel von Cyberangriffen. Allein die von Ransomware-Angriffen verursachten Schäden, bei denen den Betroffenen der Zugang auf ihre Daten oder Systeme blockiert wird, sind erheblich. Zudem nimmt die Anzahl neuer Schadprogramm-Varianten zu und es werden immer wieder kritische Schwachstellen in weitverbreiteten Software-Produkten lokalisiert.

Insbesondere Kritische Infrastrukturen sind von zentraler Bedeutung für die Funktionsfähigkeit des Gemeinwesens. Durch ihren Ausfall oder ihre Beeinträchtigung entstehen Versorgungsengpässe, die eine Gefahr für die öffentliche Sicherheit darstellen. Mit dem BSI-Gesetz[28] ist ihr Schutz deshalb gesetzlich verankert.

In Deutschland ansässige Unternehmen müssen in der Lage sein, sich selbst und ihre Kundinnen und Kunden angemessen vor Cyberangriffen zu schützen. Hierzu gehören in der Regel das zeitnahe Einspielen von Updates sowie eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter. Je nach Anforderung an die Sicherheitsbelange des jeweiligen Unternehmens sollten auch regelmäßige Schulungen des Personals selbstverständlich sein sowie die Einführung und der Unterhalt eines Informationssicherheitsmanagementsystems (ISMS) nach nationalen oder internationalen Normen wie zum Beispiel der ISO 27001 oder dem BSI IT-Grundschutz. Ebenso stehen die Hersteller in der Pflicht, eigene Qualitätssicherungsmaßnahmen mit Blick auf die Gewährleistung hochqualitativer Produkte auszubauen, in ihren Produkten gefundene Sicherheitslücken zeitnah zu schließen und damit zum Schutz der Nutzenden zu einem hohen Cybersicherheitsniveau in Deutschland beizutragen.

Zukunfts- und Schlüsseltechnologien wie IoT, KI, Blockchain, Big Data oder Quantentechnologie sorgen für Innovationssprünge und verändern die Rahmenbedingung für die Cybersicherheit in Deutschland. Sie eröffnen neue Potenziale, um bestehende Instrumente der Cybersicherheit zu verbessern. Gleichzeitig können hierdurch neue Cyberrisiken entstehen. Um Anwenderinnen und Anwender zu schützen, muss die Sicherheit der Schlüsseltechnologien deshalb bereits als zentraler Baustein im Entwicklungsprozess verankert und im Sinne eines Security-by-Design-Ansatzes gelebt werden.

Eine exzellente IT-Sicherheitsforschung sowie gut ausgebildete IT-Sicherheitsfachkräfte sind dabei wichtige, nachhaltige Grundpfeiler für die Wahrung der Cybersicherheit.

Die Bundesregierung wird Maßnahmen erarbeiten, um die bereits bestehende, vertrauensvolle und enge Zusammenarbeit von Staat und Wirtschaft fortzuführen. Das Fundament ist eine starke deutsche IT-Wirtschaft, die durch eine moderne Wirtschaftspolitik zu fördern ist.

[28] Abrufbar unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

Um die Cybersicherheit der Wirtschaft zu stärken, bedarf es folglich einerseits einer Kooperation von Staat und Wirtschaft; die Bundesregierung ist aber auch gehalten, die erforderlichen Rahmenbedingungen zu schaffen. An diesen beiden Ansätzen orientieren sich die folgenden Ziele.

8.2.1 Den NCSR in seiner Koordinierungsfunktion für die Cybersicherheitslandschaft stärken

Warum ist das Ziel relevant?

Die Digitalisierung hat alle Lebens- und Wirtschaftsbereiche erfasst. Die Gewährleistung eines hohen Maßes an Cybersicherheit nimmt daher eine gesamtgesellschaftliche Bedeutung ein. Um dieser Entwicklung Rechnung zu tragen, muss der NCSR in seiner strategischen Beratung der Bundesregierung die verschiedenen Perspektiven aus Wirtschaft und Gesellschaft bündeln und diese stärker formalisieren.

Wo stehen wir?

Der 2011 als Impulsgeber und strategischer Ratgeber etablierte NCSR ist das in der deutschen Cybersicherheitslandschaft höchstrangig besetzte Gremium. Er erhielt durch die Cybersicherheitsstrategie 2016 einen erweiterten Auftrag zur Identifizierung langfristiger Handlungsnotwendigkeiten und Trends sowie zur Erarbeitung von Handlungsempfehlungen. Zu diesem Zweck wurde 2017 ein Fachbeirat eingerichtet, dessen Empfehlungen in einem Abschlussbericht zusammengefasst wurden. Der Fachbeirat hat unter anderem die dauerhafte Begleitung der Arbeit des NCSR durch eine wissenschaftliche Arbeitsgruppe empfohlen, die in regelmäßigen Abständen Impulspapiere erarbeitet und diese auch der Öffentlichkeit zur Verfügung stellt.

Was wollen wir erreichen?

Der NCSR soll künftig seine Rolle als Impulsgeber für Fragen der Cybersicherheit noch stärker als bisher wahrnehmen. Hierfür ist seine Rolle als strategischer Berater der Bundesregierung ausgebaut und bedarfsorientiert formalisiert worden. Ebenso entwickelt er eine größere Strahlkraft in Wirtschaft, Wissenschaft und Gesellschaft hinein und begleitet dauerhaft die Umsetzung und Fortentwicklung der Cybersicherheitsstrategie.

Zu diesem Zweck ermitteln wir, wie die Zusammenarbeit und das bereits in der Cybersicherheitsstrategie 2016 eingeführte Berichtswesen an das Bundeskabinett verbindlicher gestaltet werden können. Darüber hinaus werden wir Möglichkeiten für eine stärkere Wirkung in die Öffentlichkeit hinein sowie eine vertiefte Einbindung von Wirtschaft, Wissenschaft und Zivilgesellschaft in die Arbeit des NCSR prüfen.

Welche Wirkung erwarten wir?

Wir erwarten vom NCSR eine umfassendere Perspektive auf Themen der Cybersicherheit. Der erweiterte Austausch soll ein tiefergehendes Verständnis für die Positionen der beteiligten Akteure untereinander ermöglichen. Die erweiterten Möglichkeiten des NCSR, mit wahrnehmbaren Impulsen in die Wirtschaft und Gesellschaft hineinzuwirken, sollen nicht zuletzt die Kohärenz der Aktivitäten in der Cybersicherheitslandschaft stärken.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand des folgenden Kriteriums überprüfen:

- Es wurde ein in der Bundesregierung und mit dem NCSR abgestimmtes Konzeptpapier erarbeitet. Dieses zeigt Maßnahmen auf, mit denen zum einen ein zielorientierterer Beratungsprozess der Bundesregierung durch den NCSR ermöglicht wird und zum anderen den Entscheidungsträgerinnen und Entscheidungsträgern in den jeweiligen zuständigen Gremien eine umfassendere Perspektive auf die Cybersicherheitslandschaft eröffnet wird.

8.2.2 Die Zusammenarbeit von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft im Bereich der Cybersicherheit verbessern

Warum ist das Ziel relevant?

Eine nachhaltige Stärkung der Cybersicherheit in Deutschland kann nur in einem gemeinschaftlichen Schulterschluss von Staat, Wirtschaft sowie Zivilgesellschaft und Wissenschaft erreicht werden.

Die gesamtgesellschaftliche Zusammenarbeit muss weiter verbessert und durch neue Kooperationsmodelle gestärkt werden. So werden die Verbraucherinnen und Verbraucher, Wissenschaftlerinnen und Wissenschaftler sowie Entscheidungsträgerinnen und -träger der Wirtschaft und des Staates über Cybersicherheitsrisiken und -gefahren aufgeklärt und bei der Prävention unterstützt. Außerdem können staatliche Angebote und realisierbare Vorgaben zielgenau und praxistauglich entwickelt werden.

Wo stehen wir?

Wirtschaftsvertreterinnen und -vertreter werden bereits in vielen Bereichen und Prozessen integriert. Enge Kooperationen zwischen Staat und Wirtschaft existieren insbesondere im Bereich der Kritischen Infrastrukturen und für den Wirtschaftsschutz. Etablierte Foren sind unter anderem der UP KRITIS, die Allianz für Cybersicherheit, der „Dialog für Cybersicherheit“ des BSI oder die Initiative Wirtschaftsschutz[29].

Das BMWi unterstützt KMU bei der Digitalisierung und der IT-Sicherheit. Hier werden Anwenderinnen und Anwender durch gut verständliche, neutrale, praxisorientierte Informationen sowie durch konkrete Hilfe bei der Konzeption und Umsetzung unterstützt.

Im Nationalen Pakt Cybersicherheit wurde im April 2021 eine gesamtgesellschaftliche Erklärung zur Cybersicherheit zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft abgestimmt und veröffentlicht. In der finalisierten Erklärung wurden 13 Handlungsfelder benannt, an deren Umsetzung alle Gesellschaftsgruppen gemeinschaftlich arbeiten sollten[30].

Dieser Dialog lebt von einer lebendigen Zusammensetzung der Teilnehmenden, steht aber noch am Anfang und soll aufbauend auf den Erkenntnissen aus dem Nationalen Pakt Cybersicherheit gestärkt werden.

---

[29]Die Initiative Wirtschaftsschutz (www.wirtschaftsschutz.info) als durch das BMI koordinierte Initiative zur Umsetzung der Nationalen Strategie für Wirtschaftsschutz analysiert gemeinsam mit Experten von Sicherheitsbehörden (BfV, BKA, BND und BSI) sowie Spitzenwirtschafts- und Sicherheitsverbänden (BDI, DIHK, ASW Bundesverband und BDSW) die Risikolage und entwickelt Handlungskonzepte für einen ganzheitlichen Wirtschaftsschutz.

[30] Abrufbar unter: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationaler-pakt-cybersicherheit/gesamtgesellschaftliche-erklaerung/gesamtgesellschaftliche-erklaerung-artikel.html

Was wollen wir erreichen?

Im Rahmen von Angeboten der zuständigen staatlichen Stellen werden Wirtschaft, Wissenschaft und Gesellschaft bei der Gestaltung von Cybersicherheit aktiv beteiligt. Der Austausch bietet Raum, um gemeinsam nachhaltige Handlungsoptionen und Lösungen im Bereich der Cybersicherheit zu entwickeln. Themen und Bedarfe der verschiedenen Gruppen werden frühzeitig erkannt und fließen in die Arbeit der staatlichen Akteure ein.

Provider und IT-Sicherheitsdienstleister setzen Anforderungen an IT-Sicherheitsprodukte und -systeme um und können durch ihren direkten Kontakt mit Anwenderinnen und Anwendern Herausforderungen und Trends frühzeitig erkennen. Staatliche Stellen beziehen sie deshalb frühzeitig in die Festlegung gesetzlicher Anforderungen für IT-Sicherheitsprodukte ein und suchen gemeinsam mit ihnen nach einer realisierbaren Umsetzungsmöglichkeit.

Welche Wirkung erwarten wir?

Die Fortentwicklung eines gesamtgesellschaftlichen Dialogs im Bereich der IT-Sicherheit führt zu einer gesteigerten Akzeptanz staatlicher Institutionen. Dies erleichtert die Zusammenarbeit und hilft, die Präsenz von Cybersicherheitsthemen auf allen Ebenen der Anwendung von IT zu erhöhen.

Eine gestärkte Zusammenarbeit durch Kooperationsmodelle ermöglicht Multiplikatoreffekte bei der Wissensvermittlung. Auf Basis bestehender Kooperationsbeziehungen kann ein Austausch bereits zu Beginn von Entwicklungsvorhaben und im Rahmen der Definition von Prozessen erfolgen. Ergebnisse können hierdurch anwenderfreundlicher gestaltet sowie Zeitersparnisse und Synergien realisiert werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl der Mitgliedschaften in der Allianz für Cybersicherheit ist gestiegen.
- Der gesamtgesellschaftliche Dialog im Bereich der IT-Sicherheit beim BSI ist fortentwickelt, in dem gemeinschaftlich an den akuten Themen der IT-Sicherheit gearbeitet wird.
- Die Bundesregierung wird aktiv auf die Umsetzung der 13 Handlungsfelder aus der gesamtgesellschaftlichen Erklärung des Nationalen Pakts Cybersicherheit hinwirken, dazu Stakeholder gewinnen und die Umsetzung nachvollziehbar dokumentieren.
- Staatliche Unterstützungsangebote, unter anderem in Form verschiedener Kooperationsmodelle sowie über Social Media und Newsletter, sind erweitert und die Anzahl der Nutzerinnen und Nutzer der Angebote ist gestiegen.
- Der Anteil großer Schadprogrammwellen, die mittels technischer Sensoren entdeckt werden, ist gestiegen.
- Die Anzahl der Angebote der Initiative Wirtschaftsschutz für Unternehmen, Forschungseinrichtungen und Kommunen ist gestiegen.
- Das Mittelstand-Digital-Netzwerk des BMWi ist bekannt und seine Angebote zur IT-Sicherheit werden von der Wirtschaft und insbesondere von KMU genutzt.

8.2.3 Eine kooperative Kommunikationsplattform zu Cyberangriffen zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft aufbauen

Warum ist das Ziel relevant?

Die von Cyberangriffen betroffenen Organisationen in Staat, Wirtschaft, Wissenschaft und Gesellschaft benötigen für die Detektion dieser Angriffe nutzbare technische Informationen. Diese Informationen basieren auf Analysen der Cyberangriffe, die beispielsweise Bundesbehörden und IT-Sicherheitsdienstleister durchführen. Wenn die betroffenen Organisationen effektiv und effizient mit den technischen Informationen versorgt werden, kann dies zu einer signifikanten Verringerung oder gar Verhinderung von Schäden durch Cyberangriffe führen.

Wo stehen wir?

Cyberangriffe werden durch eine Vielzahl von Akteuren abgewehrt. In der Folge sind die notwendigen Informationen für eine effektive Abwehr von Cyberangriffen oftmals fragmentiert und stehen den betroffenen Organisationen nicht immer zeitnah und vollumfassend zur Verfügung. Die Zusammenarbeit mit Providern wurde zwar verstärkt (wie in der „Cybersicherheitsstrategie für Deutschland 2016“ genannt). Sie stellt aber nur einen Teil des notwendigen Informationsaustausches dar.

Was wollen wir erreichen?

Für den Erfolg ist es erforderlich, dass alle an der Cyberabwehr beteiligten Organisationen in ihrem jeweiligen Verantwortungsbereich so weit Informationen beitragen, wie Datenschutz und Geheimhaltungspflichten es ermöglichen. Die Detektionsleistung ist insbesondere auch in der Fläche der öffentlichen Kommunikationsnetze durch das Einbeziehen der Provider zu verbessern. Der Staat als neutraler Vermittler zwischen den Teilnehmenden schafft für den Informationsaustausch die notwendige Basis für eine kooperative Kommunikationsplattform (Information Sharing Plattform). Durch den vertrauensvollen Austausch aller beteiligten Organisationen kann die Informationsbasis über Cyberangriffe zur Verbesserung der Cyberabwehr für alle beteiligten Organisationen erweitert werden.

Zu Cyberangriffen werden allgemeine Informationen und insbesondere technische Merkmale für die Detektion zwischen den betroffenen und auswertenden Organisationen (zum Beispiel BSI, Sicherheitsbehörden, IT-Sicherheitsdienstleistern und große Unternehmen) über die Kommunikationsplattform effizient ausgetauscht. Dies ermöglicht eine bessere Bedrohungsanalyse und zielgenaue Cyberabwehr. Die Informationen werden effizient, das heißt insbesondere auch soweit rechtlich und technisch möglich automatisiert, geteilt und erreichen eine hohe Reichweite. Die Informationen sind zudem an die Fähigkeiten der jeweiligen Nutzergruppe (zum Beispiel KMU) angepasst. Sensible Informationen werden im Rahmen des Informationsaustausches wirksam geschützt.

Welche Wirkung erwarten wir?

Durch freiwillige Teilnahme möglichst vieler von Cyberangriffen betroffener Organisationen am Informationsaustausch über die kooperative Kommunikationsplattform (Information Sharing Portal) ist die Detektion von Cyberangriffen erfolgreicher und lässt eine schnellere Abwehr und

Attribuierung zu. Die bessere Vernetzung führt zu einer verstärkten Sensibilisierung insbesondere von Unternehmen und Wissenschaft. Der Schaden durch Cyberangriffe wird reduziert oder verhindert.

Für die Schaffung einer Informationsbasis zu Cyberangriffen erhalten unter Einhaltung von Datenschutz und Geheimhaltungspflichten insbesondere die IT-Sicherheitsdienstleister und für die Cyberabwehr sowie Cyberverteidigung zuständigen staatlichen Behörden die notwendigen Informationen zu Cyberangriffen aus den Detektionsergebnissen der betroffenen Organisationen und tauschen diese auch für bessere Analyseergebnisse aus. Dies ermöglicht fortlaufend die Analyse von Cyberangriffen zu verbessern und die Erstellung neuer, zielgenauerer technischer Merkmale zur Detektion. Dies wird zur Stärkung der Abwehr in Unternehmen und öffentlichen Netzen eingesetzt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die neue kooperative Plattform „Information Sharing Portal“ für den freiwilligen Austausch von Informationen zu Cyberangriffen ist etabliert.
- Sensitive Detailinformationen werden unter Einhaltung unter anderem der geltenden rechtlichen Regelungen und der bestehenden Übermittlungsvorschriften vertrauensvoll behandelt und so wirksam gegen Missbrauch geschützt.
- Anreize für die Teilnahme am Informationsaustausch und für das Teilen von Informationen wurden gestärkt.
- Die Anzahl der zwischen den betroffenen Organisationen ausgetauschten allgemeinen Informationen und technischen Merkmalen zu Cyberangriffen hat zugenommen und den Schutz vor Schäden durch Cyberangriffe verbessert.

8.2.4 Unternehmen in Deutschland schützen

Warum ist das Ziel relevant?

Die Gefahren, denen Unternehmen in Deutschland im Kontext von Cyberangriffen ausgesetzt sind, sind vielgestaltig und dynamisch. Insbesondere KMU sind den Herausforderungen aufgrund von Mängeln an Ressourcen und Wissen nicht ausreichend gewachsen. Sie benötigen daher besondere Förderung für einen ausreichenden Schutz vor Cyberangriffen. Sie stellen zahlenmäßig jedoch den größten Anteil an allen Unternehmen dar.

Wo stehen wir?

Es bestehen vielfältige Initiativen zum Austausch zwischen Staat und Wirtschaft zu Fragen der Cybersicherheit, wie beispielsweise die „Initiative IT-Sicherheit in der Wirtschaft“[31] des BMWi, die Allianz für Cybersicherheit oder das vom BMI und vom Bundesverband der Deutschen Industrie (BDI) ins Leben gerufene „Cyberbündnis mit der Wirtschaft“.

Auch in der seit 2016 etablierten Initiative Wirtschaftsschutz werden die unternehmerischen Gefahren in der Cyberwelt kontinuierlich miteinbezogen. Darüber hinaus stehen auch die Nachrichtendienste, beispielsweise die Fallaufnahme des BfV oder der Cyber-Intelligence-Bereich des BND, und Polizeibehörden den Unternehmen als vertrauensvolle Ansprechpartner zur Verfügung. Dies wird ergänzt durch die zentralen Ansprechstellen Cyber-Crime der Polizeien der Länder und des Bundes, die speziell für Unternehmen sowie öffentliche und nichtöffentliche Institutionen eingerichtet worden sind, um als kompetente Ansprechpartner IT-Sicherheitsvorfälle aus diesen Bereichen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen.

Was wollen wir erreichen?

Die Zusammenarbeit zwischen Staat und Wirtschaft wurde weiter ausgebaut. Die Dialog- und Informationsaustauschplattformen zwischen Staat und Wirtschaft sind gestärkt, darunter fallen der UP KRITIS, die Allianz für Cybersicherheit, der Nationale Pakt Cybersicherheit, das Cyberbündnis mit der Wirtschaft sowie die Initiative Wirtschaftsschutz.

Die Interaktion der Unternehmen mit den zuständigen Stellen in den Teilbereichen Prävention, Detektion und Reaktion der Cybersicherheit ist gestärkt. Unternehmen tragen hierdurch mehr zur Detektion und Aufklärung von Cybersicherheitsbedrohungen bei. Cybersicherheit ist integraler Bestandteil eines ganzheitlichen Wirtschaftsschutzes.

Maßnahmen zum Schutz von Unternehmen (insbesondere KMU), Rüstungsindustrie und Unternehmen mit deutscher Schlüsseltechnologie werden in Abstimmung mit und im Zusammenwirken von Bund und Ländern durchgeführt. Dabei wird das funktionsfähige Netzwerk des Wirtschaftsschutzes im Verfassungsschutzverbund einbezogen. Die Maßnahmen der „Initiative IT-Si-

[31] Abrufbar unter: https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Home/home.html

cherheit in der Wirtschaft“ samt der TISiM werden umgesetzt und Förderprogramme (zum Beispiel „go-digital“[32] und „Digital Jetzt“[33]) bedarfsorientiert fortentwickelt. Das Netzwerk der Mittelstand-Digital-Zentren ist insbesondere im Hinblick auf das Querschnittsthema IT-Sicherheit weiterentwickelt.

Das Informationsangebot zur Unterstützung von Unternehmen ist bedarfsgerecht ausgebaut. Die Unternehmen und insbesondere KMU sind für IT-Sicherheit sensibilisiert, sie besitzen ein erhöhtes Problembewusstsein für Cyberrisiken und verfügen über entsprechende Beurteilungs- sowie Lösungskompetenzen. IT-Sicherheitsmaßnahmen von Unternehmen, insbesondere KMU, werden unterstützt. Dazu sind die Unterstützungsangebote des BSI in Richtung Wirtschaft insbesondere im Rahmen der Allianz für Cybersicherheit ausgebaut.

Welche Wirkung erwarten wir?

Unternehmen (insbesondere KMU und Handwerk) werden bei der Umsetzung von IT-Sicherheitsmaßnahmen gezielter unter Berücksichtigung des jeweiligen Cyberrisikos unterstützt und haben das Wissen, um organisatorische, technische und personelle Maßnahmen effizient zu initiieren. Sie sind hierdurch in der Lage, sich effektiv vor Cyberangriffen zu schützen. Hierdurch wird die Wettbewerbsfähigkeit der deutschen Wirtschaft gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Angebote der Mittelstand-Digital-Zentren werden durch die Wirtschaft angenommen.
- Die TISiM ist insbesondere bei KMU und Handwerk bekannt und ihre Angebote werden nachgefragt.
- Förderprogramme, die auch auf Unterstützung der IT-Sicherheit von KMU, einschließlich Handwerk und freie Berufe, abzielen (insbesondere „go-digital“ und „Digital Jetzt“), sind bekannt und werden nachgefragt.
- Die Anzahl der Mitglieder und Angebote in der Allianz für Cybersicherheit ist gestiegen.
- Die Anzahl der Nutzenden der Unterstützungsangebote des BSI ist nachweislich gestiegen.
- Die Umsetzung empfohlener Cybersicherheitsvorkehrungen ist gestiegen.
- Der prozentuale Anteil betroffener Unternehmen, die nach BSI-Warnungen reagiert und ihre Sicherheitslücken geschlossen haben, ist gestiegen.
- Die „Initiative Wirtschaftsschutz“ hat Projekte zum ganzheitlichen Schutz der Wertschöpfungskette vor Know-how- und Informationsabfluss etabliert.

[32] Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html

[33] Abrufbar unter: https://www.bmwi.de/Redaktion/DE/Dossier/digital-jetzt.html

8.2.5 Die deutsche digitale Wirtschaft stärken

Warum ist das Ziel relevant?

Die Wirtschaft kann einerseits auf einer Vielzahl von Innovationen und Erfolgen aufbauen, befindet sich aber gleichzeitig in einem herausfordernden internationalen Wettbewerb. Neben neuen Anwendungsfeldern, wie SmartHome und SmartCity, ist insbesondere auch die Digitalisierung klassischer Wirtschaftszweige relevant. Um die führende Rolle der deutschen Wirtschaft auch in der digitalisierten Zukunft zu sichern, in weiteren Wirtschaftszweigen zu ermöglichen und die Digitale Souveränität zu stärken, bedarf es gezielter Maßnahmen. Dabei sind auch die zugehörigen Lieferketten zu berücksichtigen.

Wo stehen wir?

Einerseits dominieren ausländische Firmen wichtige Digitalisierungsfelder, insbesondere jene, die datengetrieben sind. Andererseits zählen Deutschland und Europa in vielen Forschungsbereichen der Digitalisierung zur Weltspitze und sind für ihre hohen Standards bekannt. In diesem Spannungsfeld müssen die Firmen in die Lage versetzt werden, ihre Vorteile zu nutzen, um konkurrenzfähig zu bleiben oder konkurrenzfähig zu werden.

Was wollen wir erreichen?

Durch die gezielte Förderung von Schlüsseltechnologien[34], durch Beratung, Zuwendungen, gemeinsame Projekte und die Vernetzung mit relevanten Forscherinnen und Forschern soll die deutsche Digitalwirtschaft gezielt gestärkt werden. Eine weitere Stärkung soll sich aus der Kooperation mit Gremien zur gemeinsamen Entwicklung von Handlungsempfehlungen und Standards für wichtige Anwendungsbereiche (zum Beispiel in der Elektromobilität oder bei den Smart-Home-Produkten) ergeben.

Konkret sollen durch die Erhöhung der IT-Sicherheit ihrer Produkte beziehungsweise durch die Entwicklung von Produkten zur Erhöhung der IT-Sicherheit folgende Wirtschaftszweige und Lieferketten gezielt gestärkt werden: Mobilitäts- und Automobilindustrie, Energiewirtschaft, Smart Home beziehungsweise IoT und Smart Cities, Industrie 4.0, Gesundheitswesen, Finanzwesen und die IT-Sicherheits-Industrie mit den Feldern Biometrie, Langzeitsicherung und Quantentechnologie.

Die Smart-Metering-PKI, eine zentrale Infrastrukturkomponente für die Digitalisierung der Energiewende, wird erfolgreich und mit wachsender Nutzerzahl betrieben. Die BMWi-BSI-Roadmap zur Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid (Intelligentes Stromnetz), Smart Mobility (intelligente Mobilität) und Smart-beziehungsweise Sub Metering (intelligente Energieverbrauchsmessung, auch in Mehrparteienhäusern) wurde im Rahmen mehrerer Standardisierungsprojekte umgesetzt.

---

[34] Vergleiche strategische Ziele 8.1.10 „IT-Sicherheit durch KI und IT-Sicherheit für KI gewährleisten“ und 8.2.9 „IT-Sicherheit durch Quantentechnologie gewährleisten“IT-Sicherheit durch Quantentechnologie gewährleisten.

Welche Wirkung erwarten wir?

Durch eine geeignete Umsetzung sind einerseits Produkte mit erhöhter IT-Sicherheit und andererseits innovative Produkte, die die IT-Sicherheit erhöhen, zu erwarten. Konsequenz sind eine größere Wettbewerbsfähigkeit, eine größere Akzeptanz und eine größere Verbreitung dieser Produkte. Dank Innovationen durch Forschung und Vernetzung kann die deutsche Digitalwirtschaft eine internationale Vorreiterrolle einnehmen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Datenübertragung von und zu Mobilitätsdatenräumen sowie autonome Fahrfunktionen wurden abgesichert, die Resistenz gegen Angriffe auf die Sensorik von Fahrzeugen wurde gesteigert und entsprechende Technische Richtlinien wurden veröffentlicht. Die (Typ-)Genehmigung und Marktbeobachtung von Kraftfahrzeugen und Kraftfahrzeugteilen zur Gewährleistung der Cybersicherheit wurde vom BSI in Zusammenarbeit mit dem Kraftfahrtbundesamt gestaltet.
- Die Smart-Metering-PKI, eine zentrale Infrastrukturkomponente für die Digitalisierung der Energiewende, wird erfolgreich und mit wachsender Nutzerzahl betrieben. Die BMWi-BSI-Roadmap zur Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid (Steuerbare Verbrauchs- und Erzeugungsanlagen), Smart Mobility (Integration der Ladesäuleninfrastruktur von Elektromobilen) und Smart beziehungsweise Sub Metering (Spartenübergreifende Verbrauchsmessung wie Strom, Gas, Wasser, Heizen beziehungsweise Wärme) wurde im Rahmen mehrerer Standardisierungsprojekte umgesetzt. Im Bereich Smart Home beziehungsweise Consumer-IoT wurden Standards, Normen, Technische Richtlinien und Prüfkriterien (zum Beispiel Prüfspezifikation Router-TR) unter anderem für die Anwendung in Verbindung mit nationalen und internationalen Labeling- und Zertifizierungsverfahren (zum Beispiel im Rahmen des Cybersecurity Act) in Zusammenarbeit mit erforderlichen Stakeholdern aus Staat, Wirtschaft und Gesellschaft entwickelt.
- Im Bereich Smart Cities wurden bestehende kommunale IoT-Infrastrukturen analysiert, Handlungsempfehlungen für deren sicheren Aufbau und Betrieb erstellt, Technische Richtlinien und Standards für Schlüsseltechnologien und Plattformen in Kooperation mit erforderlichen Stakeholdern aus Staat, Wirtschaft und Gesellschaft erarbeitet. Zudem wurden rechtliche Rahmenbedingungen für eine verbindliche Umsetzungsverpflichtung der Maßnahmen zur Verbesserung der IT-Sicherheit in kritischen Einsatzbereichen geschaffen.
- Im Bereich Industrie 4.0 wurde im internationalen Rahmen ein Konzept von Vertrauensinfrastrukturen für den Aufbau digitaler Wertschöpfungsnetze abgestimmt, es wurden Handlungsempfehlungen (Best Practices) für KMU zur Umsetzung wichtiger Komponenten von Vertrauensinfrastrukturen erstellt. Zudem wurden Dienstleistungsschnittstellen für eine sichere Digitalisierung und Industrie 4.0 geschaffen.
- Im Gesundheitswesen wurde ein Katalog von Sicherheitsanforderungen für Digitale Gesundheitsanwendungen im Rahmen des Zulassungsverfahrens etabliert, die Aktivitäten zur digitalen Pandemiebekämpfung wurden fortgeführt. Die Initiativen im Gesundheitswesen wurden auf den Bereich des Rettungswesens erweitert.

- Im Finanzwesen wurden die Sicherheitsanalysen von Online-Bezahlvorgängen kommuniziert und fortgeschrieben und die Sicherheitsanforderungen an Biometrie-Anwendungen für die Zwei-Faktor-Authentisierung etabliert.

8.2.6 Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen

Warum ist das Ziel relevant?

Der Regulierungsrahmen für die Cybersicherheit von Produkten und Dienstleistungen ist national und international uneinheitlich. Er verteilt sich auf eine Vielzahl von Standards, Normen und Gesetzen. Teilweise sind verbindliche Vorgaben nicht oder nur unzureichend vorhanden. Die Zuordnung der jeweils relevanten Regulierungen ist zudem fehleranfällig und aufwendig.

Im Bereich der Überwachungstechnik führen die aktuellen EU-Regelungen gerade dazu, dass Hersteller ihren Sitz aus den EU-Mitgliedstaaten in Nicht-EU-Staaten verlegen, da der Import von dort in die EU deutlich einfacher ist als der Export aus der EU in Nicht-EU-Staaten. Dies führt etwa im Bereich der Telekommunikationsüberwachung (TKÜ), der Digitalen Forensik und der Big-Data-Analyse zu einem Technologieverlust und wirkt der angestrebten Digitalen Souveränität entgegen.

Wo stehen wir?

Das Ziel, nur solche Geräte in Verkehr zu bringen, die Schutz vor grundlegenden Cybersicherheitsrisiken versprechen, lässt sich nur auf EU-Ebene erreichen. Die Kommission beabsichtigt daher, an vernetzbare Geräte entsprechende Anforderungen als Voraussetzung für eine Bereitstellung auf dem Markt zu stellen. Dieser Schritt würde die Situation bereits kurz- bis mittelfristig erheblich verbessern, da kein neues Rechtsetzungsvorhaben initiiert werden muss. Die Wirkung setzt dementsprechend schneller ein. Dieses Vorhaben wird daher von Deutschland ausdrücklich unterstützt.

Was wollen wir erreichen?

EU-weit sind einheitliche gesetzliche Anforderungen inklusive Marktzugangsregelungen sowie Normen und Standards für Unternehmen im Bereich der Cybersicherheit definiert. Doppelregulierungen werden vermieden. Die Bundesregierung setzt sich abgestimmt in nationalen, europäischen und internationalen Standardisierungs- und Normungsgremien dafür ein, dass einheitliche Normen und Standards für Unternehmen in der EU entwickelt und eingeführt werden. Die NIS Richtlinie 2.0[35] der EU wird aktiv mitgestaltet und deutsche Belange werden in den Nachfolgelegislativakt eingebracht. Sektorspezifische Legislativvorschläge, wie zum Beispiel der DORA Verordnungsvorschlag für den Finanzsektor[36], werden aktiv begleitet.

Die internationale Zusammenarbeit, ebenso wie die Gremienarbeit im Bereich der Standardisierung ist gestärkt. Die internationale Wettbewerbsfähigkeit der nationalen und europäischen Standardisierungs- und Zertifizierungsstellen ist erhöht, die Verfahren bleiben international führend.

---

[35] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0823

[36] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020PC0595

Auch mit Blick auf Digitale Souveränität engagiert sich Deutschland in den europäischen und internationalen Normungsgremien. Eine strategisch ausgerichtete Standardisierungspolitik ist gerade im Umfeld von Informations- und Kommunikationstechnik (IKT), Software und KI erforderlich. Dazu wird ein interministerieller Ausschuss Informations- und Kommunikationstechnologie-Standardisierung eingerichtet, mit dem Cybersicherheit gefördert und die Mitbestimmung in den europäischen und weltweiten Standardisierungsgremien gesichert wird. Die für die wesentlichen Technologiefelder relevanten Stakeholder (Bundesressorts, Wirtschaft, Forschung und Normierungsorganisationen) werden daran beteiligt.

Für den Einsatz beziehungsweise das Inverkehrbringen vernetzter Geräte innerhalb der EU werden die Verhandlungen auf EU-Ebene für einen horizontal wirkenden, einheitlichen Rechtsrahmen aufgenommen, der, wo es nötig ist, durch spezialgesetzliche, sektorale Regelungen ergänzt wird. Die Bundesregierung hat dies maßgeblich stimuliert und unterstützt den Prozess aktiv. So wird sichergestellt, dass ausreichend sichere Produkte innerhalb der EU in Umlauf gebracht und vernetzt werden.

Welche Wirkung erwarten wir?

Die Schaffung eines einheitlichen europäischen Regulierungsrahmens für Unternehmen führt unter anderem zu besserem Marktzugang, da Produkte und Dienstleistungen besser vergleichbar gemacht werden. Die Unternehmen profitieren von einheitlichen europaweiten Standards, die die Bürokratieaufwände reduzieren und ihre Wettbewerbsfähigkeit stärken.

Durch standardisierte Produktqualität und -sicherheit wird das Vertrauen der Verbraucherinnen und Verbraucher erhöht. Die Interoperabilität zwischen Produkten und Dienstleistungen kann durch Normungen verbessert werden. Auch dienen die Normungen als Türöffner und können den Export zum EU-Binnenmarkt oder weltweit fördern.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Doppelregulierungen für Unternehmen sind minimiert.
- Deutschland bringt sich aktiv bei der Erstellung eines EU-weit einheitlichen, horizontalen Rechtsrahmens für die Cybersicherheit und sektorale Cyberregulierungen ein.
- Ein interministerieller Ausschuss IKT-Standardisierung für die Cybersicherheit ist gegründet.
- Die Anzahl der beteiligten Stakeholder und Technologiefelder im interministeriellen Ausschuss IKT-Standardisierung für die Cybersicherheit ist gestiegen.

8.2.7 Forschung und Entwicklung resilienter, sicherer IT-Produkte, Dienstleistungen und Systeme für den EU-Binnenmarkt fördern

Warum ist das Ziel relevant?

Die IT-Sicherheitsforschung von heute führt zu den Innovationen von morgen. Sie ist notwendig, um die Resilienz von IT-Systemen und die Digitale Souveränität zu stärken. Während das Ziel 8.2.6 „Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen“ auf die gezielte Zusammenarbeit von Staat und Experten der Wirtschaft abzielt, richtet sich dieses Ziel in der Wirkung an die breite Allgemeinheit.

Wo stehen wir?

Deutschland und Europa verfügen über eine solide wissenschaftliche Basis in der IT-Sicherheitsforschung. Mit dem Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ wurden frühzeitig die Weichen gestellt. Mit dem Nachfolgeprogramm „Digital. Sicher. Souverän“ wird die IT-Sicherheitsforschung in Deutschland seit 2021 weiter konsequent und zielgerichtet vorangetrieben.

Mit dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE, dem CISPA Helmholtz-Zentrum für Informationssicherheit und dem Institut für Informationssicherheit und Verlässlichkeit KASTEL fördert das BMBF Forschungseinrichtungen an der Weltspitze der IT-Sicherheitsforschung. Exzellente IT-Sicherheitsforschung betreiben darüber hinaus das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), das Fraunhofer-Institut für Sichere Informationstechnologie (SIT), das Max-Planck-Institut für Sicherheit und Privatsphäre, das Forschungsinstitut CODE an der Universität der Bundeswehr München sowie eine Vielzahl weiterer international sichtbarer Forschungsgruppen an Universitäten und anderen Einrichtungen.

Mit der Cyberagentur werden ressortübergreifend ambitionierte Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zur Bedarfsdeckung im Bereich der Inneren und Äußeren Sicherheit Deutschlands beauftragt und finanziert.

Neben der Wissenschaft und Großunternehmen sind KMU sowie Start-ups als Rückgrat des deutschen Mittelstands Treiber von Innovationen. Mit den sehr erfolgreichen Maßnahmen „StartUp-Secure“[37] und „KMU-innovativ“[38] unterstützt das BMBF Forschung und Transfer in diesem wichtigen Wirtschaftszweig.

---

[37] Abrufbar unter: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/startup-secure

[38] Abrufbar unter: https://www.bmbf.de/bmbf/de/forschung/innovativer-mittelstand/kmu-innovativ/kmu-innovativ_node.html

Aufgrund eines nur sehr kleinen Business Eco Systems, das heißt eines Verbundes von Unternehmen, die auf eine gemeinsame Wertschöpfung ausgerichtet sind, insbesondere für Hochsicherheitsprodukte, sind Investitionen von Sicherheitsunternehmen in Fort- und Neuentwicklungen oftmals gering. Die Bereitschaft nimmt mit höher abzudeckenden Verschlusssachen-Graden ab.

Was wollen wir erreichen?

Die IT-Sicherheitsforschung zu Zukunftstechnologien sowie zu Cyberbedrohungen liefert wichtige und relevante Erkenntnisse. Hierfür werden Universitäten, Hochschulen und Forschungseinrichtungen genauso wie Unternehmen und forschende öffentliche Einrichtungen gezielt gefördert, wird Nachwuchs für IT-Sicherheit begeistert und ausgebildet sowie die Bund-Länder übergreifende Zusammenarbeit in der Forschung gestärkt.

Grundlegende IT-Sicherheitstechnologien werden als offene Technologien zugänglich und dadurch transparent, nachvollziehbar und leichter einsetzbar gemacht.

Im Sinne eines „Netzwerke-schützen-Netzwerke"-Ansatzes wird die Vernetzung von wirtschaftlichen, wissenschaftlichen und zivilgesellschaftlichen Akteuren untereinander gefördert. Der Wissenstransfer in die Wirtschaft ist gesichert. Um Erkenntnisse aus der Forschung in marktfähige Produkte oder in die fachliche Anwendung zu überführen, werden Kooperationen zwischen Forschung, Wirtschaft und staatlichen Einrichtungen gefördert und Anreize für Ausgründungen geschaffen. Dadurch können Synergien genutzt und zusätzliche Forschungserkenntnisse generiert werden.

Die Entwicklung und Einführung zukunftsweisender Technologien (zum Beispiel der Mobilfunknetze der 5. und 6. Generation) ist von hoher strategischer Bedeutung für die Wahrung der Digitalen Souveränität in Deutschland und der EU. Um das zu ermöglichen, werden entsprechende offene Basistechnologien, insbesondere offene und sichere Standards und Normen für Hard- und Software, und interoperable Schnittstellen aktiv von staatlicher Seite gefördert und mit geeigneten Regulierungsansätzen begleitet. Dadurch wird langfristig eine stärkere Technologiebasis für die Wertschöpfung etabliert.

Mit dem Forschungsprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän" wird die IT-Sicherheitsforschung in Deutschland weiter konsequent vorangetrieben.

Welche Wirkung erwarten wir?

Die Risiken für Wirtschaft, Staat und Gesellschaft durch neue Bedrohungslagen und Technologien werden verringert und die Widerstandskraft gegenüber einer sich ständig wandelnden Bedrohungslage wird unterstützt.

Durch den Transfer von Forschungsergebnissen, zum Beispiel in Form von Handlungsempfehlungen und Technologien, und die Kommerzialisierung von IT-Sicherheitslösungen wird die IT-Sicherheit von Wirtschaft, Bürgerinnen und Bürgern sowie des Staates gestärkt. Die Realisierung von Cybersicherheit wird für alle Akteure einfacher und günstiger.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl an Projekten und Unternehmen in der Forschung sowie der Umfang der Förderung des Forschungsrahmenprogramms der Bundesregierung ist gestiegen.
- Standards und Normen für offene Basistechnologien wurden mit Förderung entwickelt und erfolgreich erprobt sowie gegebenenfalls von Standardisierungs-, Normungs- oder Zertifizierungsgremien anerkannt (zum Beispiel Open RAN).
- IT-Sicherheitsforschung in Deutschland ist international anerkannt.
- Innovationen aus der IT-Sicherheitsforschung werden vermehrt durch Unternehmen und Startups umgesetzt beziehungsweise kommerzialisiert.
- Handlungsempfehlungen aufgrund der Forschungsergebnisse liegen vor.

8.2.8 Sicherheit von Zukunfts- und Schlüsseltechnologien im Sinne eines Security-by-Design-Ansatzes stärken

Warum ist das Ziel relevant?

Zukunfts- und Schlüsseltechnologien wie KI, IoT oder Robotik sind Treiber für die fortschreitende Digitalisierung von Produkten, Dienstleistungen und Prozessen. Um sicherzustellen, dass die hieraus entstehenden Innovationsimpulse nicht durch IT-sicherheitstechnische Risiken abgebremst werden, müssen Sicherheitsanforderungen von vornherein im Entwicklungsprozess berücksichtigt werden. Durch Security-by-Design werden sie bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt, um spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren.

Wo stehen wir?

Die Bundesregierung fordert Security-by-Design-Ansätze schon seit mehreren Jahren in der Forschungsförderung, zuletzt verstärkt durch die Förderung vertrauenswürdiger Mikroelektronik und IT-Systeme. Gerade für sicherheitskritische Anwendungen wie das autonome Fahren oder Industrie 4.0 treiben Wissenschaft und Wirtschaft entsprechende Lösungen voran. Dennoch findet der Ansatz heute insbesondere im Anwenderbereich noch keine ausreichende Berücksichtigung bei der Entwicklung digitaler Hard- und Software-Produkte und -Dienste. Security ist vielfach noch eine nach- oder nebenrangige Eigenschaft von Produkten und Diensten und steht als Verkaufsargument meist nicht im Fokus. Produkte und Dienstleistungen werden durch die höheren Qualitätsanforderungen in Produktion und Betrieb für die Sicherheitsanforderungen teurer und dadurch in ihrer Wettbewerbsfähigkeit gegenüber unsicheren Produkten und Diensten benachteiligt. In der Folge ist die IT-Sicherheit vieler Produkte und Dienste durchschnittlich oder gar schlecht.

Was wollen wir erreichen?

Bei der Entwicklung von Produkten und Lösungen auf Basis von Schlüssel- und Zukunftstechnologien wird der Security-by-Design-Ansatz von vornherein berücksichtigt.

Security-by-Design ist als Ansatz bei Entwicklerinnen und Entwicklern von Hard- und Software bekannt. Bei Projekten mit staatlicher Förderung oder Beauftragung wird der Security-by-Design-Ansatz weiter verstärkt angewendet. Die Planung und Ausgestaltung einer ganzheitlichen Sicherheitsarchitektur werden konsequent umgesetzt.

Bei der Einführung neuer Technologien im Rahmen von Projekten mit staatlicher Förderung oder Beauftragung für den produktiven Einsatz wird durch die im jeweiligen Fall zuständige Stelle im geeigneten Umfang eine Risikoreduzierung durch Security-by-Design und eine Folgenabschätzung für die Cybersicherheit gefördert. Dadurch können mögliche Risiken in einem frühen Stadium der Entwicklung reduziert und erkannt werden. Die Bundesregierung fördert damit die Entwicklung und Produktion vertrauenswürdiger IT-Systeme.

Entlang der gesamten Wertschöpfungskette stehen wettbewerbsfähig die Informationen zur Herstellung und Nutzung vertrauenswürdiger IT zur Verfügung. Zudem ist der Austausch mit wirtschaftlichen Akteuren zu Forschung, Entwicklung, Produktion und Betrieb zu vertrauenswürdiger

IT etabliert. Die sich beteiligenden wirtschaftlichen Akteure bilden ein Netzwerk und tauschen sich zu den Technologien, Entwicklungswerkzeugen und Geschäftsmodellen aus.

Eine Infrastruktur für das Qualitätsmanagement vertrauenswürdiger IT auf Basis sicherer Hard- und Software als Open Source komplettiert die wettbewerbsfähige Bereitstellung der notwendigen Informationen. Hierdurch wird die Wettbewerbsfähigkeit vertrauenswürdiger IT-Systeme gefördert.

Welche Wirkung erwarten wir?

Indem Sicherheitseigenschaften bereits als Designkriterium bei der Entwicklung von Hard- und Software Lösungen auf Basis von Zukunfts- und Schlüsseltechnologien verankert werden, werden Systemfehler von vornherein vermieden und mögliche Angriffsflächen klein gehalten. Hierdurch wird die Sicherheit in der Anwendung von Schlüsseltechnologien sichergestellt.

Durch die Steigerung der Wettbewerbsfähigkeit vertrauenswürdiger IT-Lösungen steigt auch ihr Marktanteil und damit das allgemeine Cybersicherheitsniveau.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Einhaltung von Security-by-Design wird zunehmend Bestandteil in Vergabeverfahren in staatlich geförderten oder beauftragten Projekten für den produktiven Einsatz.
- Es sind Anforderungen, Kriterien und Standards festgelegt, die IT-Systeme erfüllen müssen, um als vertrauenswürdig zu gelten (einschließlich vertrauenswürdiger Elektronik).
- Entlang der Wertschöpfungskette vertrauenswürdiger IT-Systeme ist eine Organisations-, Qualitätssicherungs- und Kommunikationsinfrastruktur gegründet. Im Rahmen des Netzwerkes zu vertrauenswürdiger IT, das die wirtschaftlichen Akteure gebildet haben, werden Projekte zu verschiedenen Technologiefeldern bearbeitet.
- Die Anzahl der Stakeholder, die sich an dem Netzwerk zu vertrauenswürdiger IT beteiligen, ist gestiegen.
- Vertrauenswürdige IT-Produkte werden im Markt erfolgreich angeboten.

8.2.9 IT-Sicherheit durch Quantentechnologie gewährleisten

Warum ist das Ziel relevant?

Die Entwicklung im Bereich der Quantentechnologie schreitet rapide voran, mit enormem Potenzial und auch neuen Herausforderungen für die Cybersicherheit.

Quantencomputer eröffnen die Chance, verschiedene Optimierungsprobleme effizienter zu lösen als herkömmliche Computer. Sie haben aber auch das Potenzial, grundlegende mathematische Annahmen zu brechen, auf denen kryptografische Algorithmen beruhen, die derzeit weit verbreitet im Einsatz sind und die die Grundlage unserer IT-Sicherheit bilden. Hier gilt es, kryptografische Verfahren zu entwickeln, die auch mit Quantencomputern nicht gebrochen werden können (sogenannte Post-Quantum-Verfahren), und Kryptoagilität zu fördern, das heißt die Fähigkeit, modular kryptografische Verfahren im Betrieb durch andere zu ersetzen.

Quantentechnologien nutzen die besonderen physikalischen Effekte auf der Ebene einzelner oder weniger Teilchen aus. Quantencomputer nutzen das für eine neuartige Rechenarchitektur aus, die für manche komplexen Probleme eine sehr viel effizientere Lösung ermöglicht. Dies ist eine Hilfe bei Optimierungsproblemen, gefährdet aber auch einige aktuelle kryptografische Verfahren und damit die Cybersicherheit. Quantenschlüsselaustausch ermöglicht mit Quanteneffekten kryptografische Schlüssel theoretisch abhörsicher auszutauschen und trägt so zu sichererer Kommunikation bei.

Daneben verspricht etwa der Quantenschlüsselaustausch die Möglichkeit, kryptografische Schlüssel sicher zu verteilen und damit sichere Datenübertragung zu ermöglichen. Dazu braucht es neben der physikalischen Technologie auch die Einbindung in Standardisierung in praktisch nutzbare, sichere Systemarchitekturen. Ebenfalls von hoher Relevanz ist Digitale Souveränität im Bereich Quantentechnologien. Es sollte der Anspruch der Bundesregierung sein, Expertise im Bereich Quantentechnologien für die Kernaspekte Quantencomputing, Quantenkommunikation und Post-Quanten-Kryptografie zu haben. Entscheidend ist zudem, dass auch Produkte aus Deutschland oder der EU zur Verfügung stehen.

Wo stehen wir?

Im Jahr 2020 hat die Bundesregierung deshalb beschlossen, zusätzlich zwei Milliarden Euro in die Förderung der Quantentechnologie zu investieren und es wurde eine „Roadmap Quantencomputing“[39] erarbeitet.

Das BMBF fördert sowohl die Erforschung und Entwicklung grundlegender Technologien als auch deren Transfer in Anwendungen sowie mehrere Projekte zur Entwicklung neuer Quantenprozessoren; ein Wettbewerb zum Aufbau von Hubs, d. h. Verbünden von unterschiedlichen Akteuren, und zum Bau kompletter Quantencomputer-Systeme wird neue Forschungs- und Entwicklungs-Strukturen etablieren. Ebenso fördert das BMBF Projekte zur Erforschung der Post-Quanten-

[39] Abrufbar unter: https://www.bundesregierung.de/breg-de/aktuelles/quantencomputing-1836542

Kryptografie. Durch das BSI wurden erste Empfehlungen zu Algorithmen für die Post-Quanten-Kryptografie sowie für die Migration zu quantensicherer Kryptografie veröffentlicht.

Was wollen wir erreichen?

Quantentechnologische Systeme werden zur Gewährleistung eines hohen IT-Sicherheitsniveaus eingesetzt und ihr Einsatz wird gefördert.

Die Auswirkungen von Quantencomputing auf die Cybersicherheit werden erforscht und technologische Innovationen für mehr Cybersicherheit genutzt. Dazu gehört beispielsweise die Erforschung des Einsatzes von Quantentechnologie (Quantencomputer und Sensoren) in der Seitenkanalanalyse.

Wichtige Voraussetzung für den Einsatz von Quantum Key Distribution (QKD) in hochsicheren Netzen ist die zertifizierbare Sicherheit von Produkten. Hierzu entwickelt die Bundesregierung ein Protection Profile gemäß Common Criteria, begleitet die Erstellung zusätzlich benötigter technischer Angaben durch Studien und erforscht quantitative und qualitative Aspekte der vorliegenden Sicherheitsbeweise.

Der mögliche Sicherheitsgewinn durch QKD wird nicht nur in Forschungsprototypen, sondern auch im realen Einsatz demonstriert, um die Praxistauglichkeit zu demonstrieren.

Der Austausch von durch Quantencomputer gefährdeten Algorithmen durch neue, standardisierte Algorithmen wurde vorbereitet.

Welche Wirkung erwarten wir?

Durch die Nutzung der Potenziale und die Minimierung der Risiken, die durch quantentechnologische Systeme entstehen, wird ein nachhaltig hohes IT-Sicherheitsniveau zum Schutz von Staat, Wirtschaft und Gesellschaft gewährleistet. Zudem wird die technologische Souveränität Deutschlands in der Quantenkommunikation gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Im Bereich des Quantencomputing stehen bis 2025 Rechner mit mindestens 100 Qubits auf der Basis souveräner Technologie aus Deutschland und Europa bereit und stehen für Anwendungsuntersuchungen aus dem Sicherheitsbereich zur Verfügung.
- Im Hochsicherheitsbereich hat der Wechsel zu quantensicherer Kryptografie begonnen.
- In Staat, Wirtschaft und Gesellschaft ist die Dringlichkeit des Wechsels zu quantensicherer Kryptografie akzeptiert und in kritischen Bereichen eingeleitet. Pilot-Infrastrukturen binden Partner aus den verschiedenen Bereichen ein.
- Technologien und Lösungen der Quantenkommunikation von Anbietern aus Deutschland und Europa stehen für Staat, Wirtschaft und Gesellschaft zur Verfügung.
- Die Studie zur Realisierbarkeit von Quantencomputern wird fortgeführt und aktualisiert.

8.2.10 Prüf- und Abnahmeverfahren mit Innovationszyklen harmonisieren (Time-to-Market)

Warum ist das Ziel relevant?

Neue IT-Produkte und Dienstleistungen werden, unter anderem in den Bereichen Smart Home, Automotive, Medizintechnik und Energie in kurzen Innovationszyklen zur Markteinführung gebracht und ermöglichen insbesondere im Bereich von IoT-Anwendungen die zunehmende Vernetzung aller Lebensbereiche. Vor allem bei neu angebotenen Soft- und Hardwareprodukten ist es nicht ausgeschlossen, dass noch nicht alle sicherheitsrelevanten Aspekte betrachtet werden oder erkennbar sind. Kriminelle versuchen, potenzielle Schwachstellen auszunutzen, um in Systeme einzudringen oder sie für strafrechtlich relevante Zwecke zu missbrauchen. Abgesehen von einer konsequenten Strafverfolgung sollte der Staat den Unternehmen Unterstützung bieten, die Produkte von Anfang an sicherer und weniger anfällig zu gestalten.

Wo stehen wir?

Staatliche Stellen müssen in der Lage sein, Aufbau und Funktionen neuer IT-Produkte und Dienstleistungen zu verstehen und mit entsprechenden Anforderungen an diese Technologien ein Mindestmaß an Sicherheit bei deren Nutzung zu gewährleisten. Hierbei gilt es, maßvoll zu agieren, damit Innovationspotenziale genutzt werden und neue Prüfverfahren eine hohe Akzeptanz bei den Herstellern erzielen können.

Was wollen wir erreichen?

Staatliche Stellen müssen in der Lage sein, als kompetente und vertrauenswürdige Dienstleister verlässliche Sicherheitsaussagen zu neuen Technologien zu treffen und darauf aufbauend regulatorische Vorgaben zu machen, Informationen bereitzustellen und Empfehlungen zu geben.

Neue Prüf- und Abnahmeverfahren, die den beschleunigten Innovationszyklen der IT-Wirtschaft Rechnung tragen (Time-to-Market), sind implementiert. Die Qualität der Verfahren hat hierdurch keine Einbußen erfahren. Die Akzeptanz für die Berücksichtigung von Sicherheitseigenschaften steigt.

Um neben der sachgerechten Produkt- und Dienstleistungszertifizierung auch die Akzeptanz für Informationssicherheit in der Digitalisierung zu stärken, wird die Entwicklung neuer Zertifizierungsverfahren vorangetrieben. Produkte und Dienstleistungen werden sachgerecht zertifiziert. Dabei wird ein zwischen Mindeststandards und Ressourceneinsatz ausgewogener Ansatz verfolgt. IT-Sicherheit besitzt hierdurch eine hohe Akzeptanz als Bestandteil digitaler Produkte und Dienstleistungen.

Damit dies neben dem staatlich-behördlichen Angebot gelingt, liegen geeignete Akkreditierungen für Prüf- und Konformitätsbewertungsstellen vor. Diese ergeben sich gegebenenfalls aus bestehenden Cybersecurity Act-Schemata, aber auch aus Akkreditierungsregeln der Deutschen Akkreditierungsstelle GmbH (DAkkS).

Welche Wirkung erwarten wir?

Mit der Implementierung neuer Prüf- und Abnahmeverfahren wird die Akzeptanz für die Berücksichtigung von Sicherheitseigenschaften erhöht.

Anwenderinnen und Anwender werden durch die sachgerechte Zertifizierung von Produkten und Dienstleistungen besser vor Cyberangriffen geschützt. Gleichzeitig wird die Innovationskraft der deutschen und europäischen Wirtschaft sichergestellt und nachhaltig gestärkt. IT-Sicherheit wird dabei als Qualitätsmerkmal der Produkte deutscher und europäischer Anbieter verankert. Die Angebotsbreite an qualitativen Prüf- und Abnahmeverfahren nimmt zu.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Für neuartige Anwendungsfelder stehen Technische Richtlinien zur Verfügung, deren Inhalte zeitnah in Standardisierungsgremien eingebracht werden.
- Neue Prüf-, Abnahme- und Zertifizierungsverfahren (beschleunigte Sicherheitszertifizierung, IT-Sicherheitskennzeichen, 5G, Medizinprodukte, (teil-) autonome Fahrzeuge, Energie, Marktaufsicht) sind etabliert.
- Neue Märkte sind zertifizierungstechnisch erschlossen.
- Die Anzahl erteilter Zertifikate ist gestiegen.
- Standards, Technische Richtlinien und Prüfspezifikationen im Bereich Smart Home beziehungsweise Consumer-IoT wurden geschaffen.

8.2.11 Schutz Kritischer Infrastrukturen weiter verbessern

Warum ist das Ziel relevant?

Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Sie zu sichern und so ihren Ausfall oder ihre Beeinträchtigung zu verhindern, ist damit bereits der Begriffsbestimmung nach ein relevantes Ziel und für das Funktionieren des Gemeinwesens und für den Schutz der Grundrechte Einzelner von hoher Bedeutung.

Wo stehen wir?

Mit dem BSI-Gesetz und der Verordnung zur Bestimmung Kritischer Infrastrukturen[40] liegt bereits seit mehreren Jahren ein Rechtsrahmen für die Cybersicherheit in Kritischen Infrastrukturen vor, der kontinuierlich weiterentwickelt wird. Gemäß den gesetzlichen Vorgaben haben die Betreiber Kritischer Infrastrukturen dem BSI regelmäßig Nachweise über technische und organisatorische Maßnahmen zur IT-Sicherheit vorzulegen. Im Gegenzug werden die Unternehmen in einen vertrauensvollen Informationsaustausch mit dem Bundesamt einbezogen. Auf Ebene von Bund und Ländern bestehen mit den Koordinierungsstellen (KOST) KRITIS der Länder und der AG KOST KRITIS zwischen Bund und Ländern wichtige Strukturen für eine koordinierende und vernetzende Behandlung von KRITIS-Belangen einschließlich der Cybersicherheit im Sinne eines All-Gefahren-Ansatzes.

Die Nationale Strategie zum Schutz Kritischer Infrastrukturen

Der Schutz Kritischer Infrastrukturen richtet sein Augenmerk auf jene Systeme, Einrichtungen und Anlagen, von deren Funktionieren die Bereitstellung gesellschaftswichtiger Dienstleistungen in besonderem Maße abhängt. Im Juni 2009 verabschiedete das Bundeskabinett die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“ - kurz: KRITIS-Strategie - um den bereits laufenden Aktivitäten einen gemeinsamen Rahmen zu geben und die strategischen Weichen für eine ressortübergreifend abgestimmte Aufgabenwahrnehmung zu stellen. Zu den Kernelementen der Strategie gehört auch der All-Gefahren-Ansatz, der sowohl die Cybersicherheit als auch den sogenannten „physischen Schutz" als Teilaspekte eines ganzheitlichen Schutzes Kritischer Infrastrukturen ausweist.

Die Strategie ist abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html.

Was wollen wir erreichen?

Staat und Wirtschaft arbeiten eng zusammen, um Kritische Infrastrukturen zu schützen und schnell auf Cybersicherheitsvorfälle reagieren zu können. Bedrohungen durch Cybersabotage werden frühzeitig erkannt. Relevante Informationen über Cybersicherheitsvorfälle sind für die zu schützenden Unternehmen und die zuständigen Behörden unverzüglich verfügbar.

Durch Prüfung der eingereichten Nachweise sowie der gegebenenfalls notwendigen Nachbesserungen ist ein Rückschluss auf die Verbesserung des Cybersicherheitsniveaus in den betroffenen Unternehmen möglich. Es ist wesentlich, dass reaktive Maßnahmen durch proaktive Maßnahmen

[40] Abrufbar unter: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

ergänzt werden, beispielsweise durch das Vorhalten eines umfassenden Cyberbedrohungslagebildes mitsamt der Möglichkeit, etwaige Cyberangriffe (oder Vorbereitungen dazu) auf KRITIS frühzeitig im Vorfeld zu erkennen und abzuwehren.

Zum Schutz Kritischer Infrastrukturen vor IT-Störungen oder Cyberangriffen sind bestehende Anforderungen weiter ausgestaltet und die Umsetzung bei den KRITIS-Betreibern wird verstärkt unterstützt. Die Unterstützung von Betreibern Kritischer Infrastrukturen durch Behörden bei Cyber- und IT-Vorfällen wird priorisiert. Bestehende Mindestanforderungen an KRITIS-Betreiber im Hinblick auf die Absicherung von IT-Systemen orientieren sich dabei am Stand der Technik. Sie werden aufgrund der sich verändernden Bedrohungslage stetig überprüft und bei Bedarf angepasst. Dies kann auf Basis vorliegender Nachweise beurteilt und durch Vor-Ort-Prüfungen zusätzlich abgesichert werden.

KRITIS-Betreiber sind auf freiwilliger Basis an einen nationalen Informationsaustausch angeschlossen. Hierdurch ist die nationale Früherkennungsfähigkeit für maliziöse Aktivitäten von Cyberakteuren verbessert. KRITIS-Betreiber können aufgrund früher Hinweise schneller auf etwaige gegen sie gerichtete Cyberbedrohungen reagieren. Die bestehenden Warnangebote des BSI für Betreiber Kritischer Infrastrukturen sind auch für weitere Unternehmen und Einrichtungen in KRITIS-Sektoren mit Versorgungsauftrag geöffnet.

Welche Wirkung erwarten wir?

Die sichere Bereitstellung der Dienstleistungen Kritischer Infrastrukturen, zu denen unter anderem die Versorgung mit Strom, Wasser, Lebensmitteln und Kommunikation oder das Gesundheitswesen sowie viele weitere zählen, ist Grundvoraussetzung für die Versorgung der Bevölkerung sowie das Funktionieren von Staat, Wirtschaft und Gesellschaft. Eine erfolgreiche Absicherung der IT-Komponenten in Kritischen Infrastrukturen beugt Risiken vor und stabilisiert so die gesellschaftliche und wirtschaftliche Entwicklung.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Der Rahmen zur Durchführung von Vor-Ort-Prüfungen ist erweitert. Entsprechende Änderungen sind bis 2026 durchgeführt oder in Arbeit.
- Die Bundesregierung hat den Stand der Technik für weitere KRITIS-Branchen konkretisiert, soweit dieser nicht bereits auf der Grundlage bestehender EU-weiter oder internationaler Normungssysteme definiert ist.
- Die KRITIS-Betreiber können über einen nationalen Informationsaustausch zu Cyberangriffen ihre jeweilige Abwehr stärken.

8.2.12 Cybersicherheitszertifizierung

Warum ist das Ziel relevant?

Zertifizierung und Konformitätsbewertung der Sicherheitsaspekte von Produkten, Dienstleistungen und Prozessen schaffen Vertrauen und Vergleichbarkeit und fördern die Bestrebungen zu einem höheren Cybersicherheitsniveau.

Wo stehen wir?

Deutsche Zertifizierungen im Kontext der IT-Sicherheit sind weltweit anerkannt.

Durch den Cybersecurity Act[41] werden neue Zertifizierungsschemata entwickelt und eingeführt. Das BSI hat sich als zuverlässiger und vertrauenswürdiger Partner für den Nachweis hoher Anforderungen an die Cyber- und Informationssicherheit etabliert, befindet sich aber im internationalen Umfeld in zunehmendem Wettbewerb mit anderen nationalen Stellen.

Was wollen wir erreichen?

Die Umsetzung des im Cybersecurity Act verankerten Cybersicherheitszertifizierungsrahmens wird aktiv begleitet und die Erarbeitung von Zertifizierungsschemata vorangetrieben. Die internationale Wettbewerbsfähigkeit der nationalen Standardisierungs- und Zertifizierungsstellen ist erhöht, um auch weiterhin international führend zu bleiben. Das BSI wird sich für die Erfordernisse, die sich aus dem Cybersecurity Act und aus nationalen Zertifizierungsvorhaben ergeben, entsprechend aufstellen, so dass adäquate Zertifizierungsangebote bereitstehen. Wir wollen die Zertifizierungslandschaft modernisieren und mit Blick auf Time-to-Market-Aspekte interessante Zertifizierungsmöglichkeiten bieten. In der Funktion als Nationale Behörde für die Cybersicherheitszertifizierung wird das BSI aktiv an der Entwicklung und

Cybersecurity Act

Unter der Verordnung (EU) 2019/881 trat der Cybersecurity Act im Juni 2019 in Kraft. Dieser beinhaltet neben der Stärkung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und deren Aufgabenweiterentwicklung auch die Einführung eines EU-weiten Zertifizierungsrahmens für die Cybersicherheit. Dies dient dem Ziel, den Bereich der Cybersicherheit und die damit verbundene Zertifizierung europäisch harmonisiert zu regeln und eine Fragmentierung des Binnenmarktes zu vermeiden. Unter Berücksichtigung der verschiedenen Vertrauenswürdigkeitsstufen niedrig (basic), mittel (substantial) und hoch (high) werden sukzessive spezielle Zertifizierungsschemata erarbeitet und implementiert. Diese gelten EU-weit, werden gleichermaßen von allen Mitgliedstaaten anerkannt und ersetzen existierende nationale beziehungsweise multilaterale Schemata mit gleichem Zertifizierungsinhalt. Beispielhaft ist hierbei die Überführung des SOGIS-MRA zu nennen, welches die sogenannten Common Criteria in ein europäisch harmonisiertes Schema überführt. Die Anwendung der Schemata des CSA ist grundsätzlich freiwillig angelegt. Jedoch besteht die Möglichkeit, entsprechende Zertifizierungserfordernisse oder EU-Konformitätserklärungen spezialgesetzlich vorzugeben.

[41] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R0881

Gestaltung von Zertifizierungsschemata gemäß dem Cybersecurity Act mitwirken.

Welche Wirkung erwarten wir?

Das BSI baut seinen hervorragenden Ruf als Zertifizierungsstelle weiter aus und ist als Nationale Behörde für Cybersicherheitszertifizierung etabliert. Die verfügbaren Zertifizierungsangebote des BSI, aber auch von privaten Anbietern werden aktiv genutzt, um im Sinne der Vertrauensbildung für ein hohes Cybersicherheitsniveau in Europa beizutragen. Unternehmen und andere potenzielle Antragsteller von Zertifizierungen machen verstärkt Gebrauch von Zertifizierungsmöglichkeiten, auch ohne gesetzlich vorgeschriebenes Erfordernis.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSI bleibt die nationale Zertifizierungsbehörde mit den meisten behördlich erteilten IT-Sicherheitszertifikaten weltweit.
- Die angekündigten Zertifizierungsschemata im Rahmen des CSA sind erlassen und besitzen Gültigkeit: Common Criteria (EUCC), Cloud Services (EUCS), IoT und 5G.
- Die beschleunigte Sicherheitszertifizierung wurde international harmonisiert und im Rahmen des CSA als Zertifizierungsschema eingeführt.
- Die Anzahl zertifizierter Produkte unter der Aufsicht der Nationalen Behörde für die Cybersicherheitszertifizierung ist gestiegen. Die Anzahl von Unternehmen und Organisationen, die IT-Grundschutz anwenden, ist gestiegen.

8.2.13 Telekommunikationsinfrastrukturen der Zukunft sichern

Warum ist das Ziel relevant?

Die Mobilfunknetze der aktuellen, fünften Generation (5G) und der kommenden, sechsten Generation (6G) zeichnen sich durch virtualisierte Netzkomponenten aus. Zentrale Funktionen des Netzes werden allein durch Software realisiert. Teilweise kann diese auf allgemein verfügbarer Hardware betrieben werden. Mit der Virtualisierung geschaffene Angriffsflächen gilt es so klein wie möglich zu halten und verbleibende Risiken zu beherrschen.

Die europäischen Hersteller von Netztechnik befinden sich in einem intensiven Wettbewerb. Viele Anbieter von Mobilfunktechnologie sind heute verstärkt in Asien und den USA beheimatet, mit einer starken Tendenz zu oligopolistischen Marktstrukturen. Damit Deutschland und Europa nicht durch weiteren Verlust von Know-how und Abwanderung von Produktionskapazitäten in einseitige Abhängigkeiten geraten, ist es erforderlich, etablierte Anbieter in Deutschland und Europa zu stärken oder aufzubauen. Durch den Einsatz offener Basistechnologien wie Open RAN, eine herstellerunabhängige Mobilfunkarchitektur, können Abhängigkeiten von wenigen dominanten Netzausrüstern reduziert, der Markteintritt neuer, auch kleinerer europäischer Anbieter erleichtert, mehr Innovationen und aufgrund höherer Transparenz und Kontrolle mehr Sicherheit im Netz ermöglicht werden. Open RAN dient daher auch direkt der Stärkung der Digitalen Souveränität und der Cybersicherheit in Telekommunikationsnetzen[42].

Wo stehen wir?

Mobilfunknetze sind bereits heute Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung. Zudem existiert ein Katalog mit Sicherheitsanforderungen für Telekommunikationsnetze. Im Rahmen eines technologie- und herstellerneutralen Ansatzes will die Bundesregierung die Anforderungen an die Sicherheit der Kommunikationsnetze deutlich erhöhen, ohne vorab konkrete Hersteller von Netzwerkkomponenten vom 5G-Netzausbau auszuschließen. Eine diesbezügliche Regelung wurde im Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) hinsichtlich sogenannter kritischer Komponenten (Produkte, die in bestimmten Kritischen Infrastrukturen eingesetzt werden) vorgenommen.

Forschung und Entwicklung im Telekommunikationsbereich haben in Deutschland gute Voraussetzungen und einen guten Ruf. Verbesserungsfähig ist die Überführung der wissenschaftlichen Leistungen in marktfähige Produkte deutscher Unternehmen.

Was wollen wir erreichen?

Die Sicherheit und Beherrschbarkeit der Telekommunikationsnetze – insbesondere der 5G-, zukünftigen 6G- und weltraumbasierten Infrastruktur als Rückgrat der Digitalisierung der Gesellschaft – werden über einen ganzheitlichen Ansatz fortlaufend evaluiert und an die neuen Gefähr-

[42] Vergleiche strategisches Ziel 8.2.7 „Forschung und Entwicklung resilienter, sicherer IT-Produkte, Dienstleistungen und Systeme für den EU-Binnenmarkt fördern“.

dungen angepasst. Im Bereich 6G wird früh und intensiv auf ein hohes Sicherheitsniveau hingearbeitet. Die Bundesregierung fördert die Forschung und Entwicklung eines ganzheitlichen 6G-Systems. Dies soll eine Grundlage für Akteure aus Deutschland schaffen, um die 6G-Standardisierung maßgeblich mitzuprägen und entsprechende Technologien in den Markt zu bringen. Entsprechende offene Basistechnologien, insbesondere offene und sichere Standards für Hard- und Software, und interoperable Schnittstellen werden aktiv von staatlicher Seite gefördert und mit geeigneten Regulierungsansätzen begleitet[43].

Deutsche und europäische Netzinfrastruktur- und Cloudanbieter sowie die Analyse und Erforschung neuer Cybersicherheitsrisiken in diesen Netzen werden gefördert.

Es sind Mechanismen entwickelt und in Kraft gesetzt, mittels derer aus Forschungsergebnissen marktfähige Produkte deutscher Firmen entstehen, die dauerhaft in Deutschland hergestellt werden. Sicherheitsstandards „Made in Germany" nehmen hierdurch einen Platz auf dem Weltmarkt ein.

Welche Wirkung erwarten wir?

Durch die Förderung deutscher und europäischer Anbieter sowie die Weiterentwicklung eigener Kompetenzen in der Erforschung neuer Cybersicherheitsrisiken wird das souveräne Handeln Deutschlands im Cyberraum sichergestellt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Verfügbarkeit der Telekommunikationsnetze und deren Widerstandsfähigkeit gegenüber Störungen und Angriffen wurde erhöht.
- Die Vertraulichkeit der Telekommunikation ist bis auf die gesetzlich vorgesehenen Ausnahmen gewahrt; das Fernmeldegeheimnis wird aktiv geschützt.
- Die Integrität der Telekommunikationsnetze ist gewahrt.
- Software und Hardware der kritischen Komponenten wird vor ihrem Einsatz einer Überprüfung unterzogen, mit der Schwachstellen erkannt und beseitigt werden.
- Deutsche und europäische Unternehmen sind in den betreffenden Standardisierungsgremien präsent und prägen maßgeblich die Standardisierung zukünftiger Telekommunikationssysteme mit einer gesteigerten Anzahl von Standardisierungsbeiträgen.
- Die Anzahl der (Erst-) Anmeldungen standardessenzieller Patente in Europa ist gestiegen.
- Der Anteil standardessenzieller Patente aus Deutschland in den internationalen Standards ist gestiegen.
- Der Anteil deutscher und europäischer Netzkomponenten in Telekommunikationsnetzen ist gestiegen.

[43] Vergleiche strategisches Ziel 8.2.6 „Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen".

- Technologie-Roadmaps für den zukünftigen 6G-Standard wurden berücksichtigt, um frühzeitig wirksame und nachvollziehbare Kriterien und Maßstäbe in einem Sicherheitskatalog für 6G-Netzkomponenten zu definieren.

8.3 Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur

Deutschland verfügt über eine leistungsfähige Cybersicherheitsarchitektur. Die Institutionen des Bundes arbeiten zur Gewährleistung der Sicherheit im Cyberraum eng zusammen. Der bereits langjährig etablierte intensive Austausch zwischen Bundes- und Landesbehörden wurde in den letzten Jahren in zentralen Bereichen weiter ausgebaut. Diese Kooperationen dienen einem Ziel: allen Menschen in Deutschland die freiheitliche Nutzung des digitalen Raumes zu ermöglichen und dabei auf ein größtmögliches Maß an Sicherheit vertrauen zu können.

Doch rasante Entwicklungen im Cyberraum stellen die staatlichen Akteure beständig vor neue Herausforderungen:

- Durch die mittlerweile alle Lebensbereiche durchdringende Digitalisierung wächst die Bedeutung, die die Cybersicherheit für die Funktionsfähigkeit von Gesellschaft, Wirtschaft und Staat einnimmt.
- Neue technologische Entwicklungen können neue Angriffsflächen bieten, aber auch neue Abwehrmöglichkeiten, die es zu erschließen gilt.
- Die Bereitschaft anderer Staaten, Cyberangriffe mit dem Ziel der Spionage, Sabotage und politischen Einflussnahme durchzuführen, steigt immer weiter.
- Angreifer professionalisieren sich zunehmend und entwickeln ihre Methoden und Techniken bei Cyberangriffen kontinuierlich weiter.

Diesen Herausforderungen kann nur effektiv begegnet werden, indem die Cybersicherheitsarchitektur in Deutschland einem permanenten Prozess der Überprüfung und Weiterentwicklung unterzogen wird:

- Das Zusammenspiel der staatlichen Institutionen muss fortlaufend strukturell und prozessual bewertet und gegebenenfalls angepasst werden, um Barrieren, die eine effektive Zusammenarbeit verhindern, weiter abzubauen. Dabei gilt es, die Zusammenarbeit zwischen Bund und Ländern stetig weiterzuentwickeln und Schnittstellen zu Akteuren außerhalb der (Bundes-)Verwaltung zu berücksichtigen. Alle Zuständigkeiten und Aufgaben innerhalb der Cybersicherheitsarchitektur müssen klar definiert sein.
- Es ist kontinuierlich zu prüfen, ob die staatlichen Institutionen über ausreichende Kompetenzen und Befugnisse verfügen, um die Sicherheit von Bürgerinnen und Bürgern, Wirtschaft und Staat auch im Cyberraum zu gewährleisten. Sollten Regelungs- oder Fähigkeitslücken identifiziert werden, sind diese zu schließen. Sollten sich Befugnisse als nicht mehr erforderlich erweisen, sind diese abzuschaffen.
- Zudem müssen für neue Herausforderungen im Cyberraum auch neue Mittel und Wege gefunden werden, diese schnell zu erkennen und ihnen wirksam begegnen zu können.

Mit den folgenden strategischen Zielen wollen wir, die Bundesregierung, diese Aufgaben angehen.

8.3.1 Die Möglichkeiten des Bundes zur Gefahrenabwehr bei Cyberangriffen verbessern

Warum ist das Ziel relevant?

In Deutschland sind für die Gefahrenabwehr grundsätzlich die Länder zuständig. Cyberangriffe stellen jedoch vielfach eine länderübergreifende Gefahr dar und haben häufig eine internationale Dimension. Zur Abwehr von Cyberangriffen ist zudem äußerst hohe technische Expertise erforderlich, die effektiv nur an wenigen Stellen in Deutschland aufgebaut werden kann. Soweit Cyberangriffe einen im Ausland liegenden Ausgangspunkt haben, kann die Abwehr dieser Angriffe zudem außen- und sicherheitspolitische Bezüge mit sich bringen, also kompetenziell an die Bundesebene adressiert sein.

Wo stehen wir?

Dem Bund stehen nach geltendem Verfassungsrecht lediglich in bestimmten Bereichen gefahrenabwehrrechtliche Sonderzuständigkeiten zu (zum Beispiel in den Bereichen Eigensicherung, internationaler Terrorismus, Grenzschutz oder Sicherheit auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes). In allen anderen Fällen kann der Bund wegen der grundsätzlichen Landeszuständigkeit für die Gefahrenabwehr selbst bei bedeutenden, komplexen und/oder länderübergreifenden Cybergefahrenlagen, die einer bundeseinheitlichen Lösung und vielfach auch internationaler Abstimmung bedürften, nicht selbst gefahrenabwehrend tätig werden. Diese Zuständigkeitsaufteilung wird der aktuellen und sich absehbar weiter verschärfenden Bedrohungslage im Cyberbereich nicht gerecht. Cybergefahren in Deutschland kann so dauerhaft nicht wirksam begegnet werden.

Was wollen wir erreichen?

Wir streben an, im Grundgesetz eine erweiterte Gesetzgebungs- und Verwaltungskompetenz des Bundes zur Abwehr von Gefahren zu verankern, die von besonders schweren und bedeutenden Cyberangriffen auf informationstechnische Systeme und Netze ausgehen. Darauf aufbauend ist zu klären, ob es entsprechend neuer oder ergänzter Aufgaben und Befugnisse der (Sicherheits-)Behörden des Bundes bedarf.

Welche Wirkung erwarten wir?

Durch die Schaffung einer erweiterten Gesetzgebungs- und Verwaltungskompetenz des Bundes für die Gefahrenabwehr besonders schwerer und bedeutender Cyberangriffe werden die Möglichkeiten für eine effektive Cyberabwehr erweitert. Gegen die Ursachen schwerer Cyberangriffe kann aktiv vorgegangen werden, um deren schädliche Wirkung im besten Fall komplett zu unterbinden. Damit steigt das gesamtstaatliche Cybersicherheitsniveau.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Durch eine Änderung des Grundgesetzes wurden die Möglichkeiten des Bundes zur Abwehr von Gefahren erweitert, die von besonders schweren und bedeutenden Cyberangriffen ausgehen.

- Für die (Sicherheits-)Behörden des Bundes wurden Aufgaben und Befugnisse zur Gefahrenabwehr im Cyberraum ausgebaut.

8.3.2 Die technisch-operativen Einheiten des BSI zukunftsfähig ausgestalten und vernetzen

Warum ist das Ziel relevant?

Das BSI muss seine Fähigkeiten zur technisch-operativen Detektion von und Reaktion auf Cybersicherheitsvorfälle permanent an die sich dynamisch entwickelnde Bedrohungslage anpassen. Dabei braucht es technisch, personell und finanziell gut ausgestatte operative Einheiten, die mit den entsprechenden Einheiten anderer nationaler Stellen, Stellen der EU, der Länder, der Wirtschaft und der Wissenschaft bestens vernetzt agieren.

Wo stehen wir?

Die technisch-operativen Einheiten des BSI bestehen aus dem Nationalen IT-Lagezentrum, dem CERT-Bund, den Mobile Incident Response Teams (MIRTs) sowie dem BSOC.

Das nationale IT-Lagezentrum bündelt und bewertet aktuelle Beobachtungen und Aktivitäten im Cyberraum, um frühzeitig bedrohliche Lagen feststellen und zeitnah reagieren zu können. Dabei arbeitet das Nationale IT-Lagezentrum eng mit dem CERT-Bund als der zentralen Stelle im BSI für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen zusammen. Das CERT-Bund ist sowohl im Verwaltungs-CERT-Verbund (VCV) mit den Länder-CERTs als auch im deutschen CERT-Verbund mit den Teams großer Organisationen und Unternehmen organisiert.

Die MIRTs unterstützen vor Ort bei der Bewältigung gravierender Cybersicherheitsvorfälle und stehen einem steigenden Bedarf gegenüber. Aufgabe des BSOC ist es insbesondere, sicherheitsrelevante Ereignisse für die Regierungsnetze und IT-Systeme des Bundes zu detektieren und auszuwerten.

Was wollen wir erreichen?

Um ein möglichst umfassendes Bild der aktuellen Lage zu gewinnen, bauen das Nationale IT-Lagezentrum und die Beobachtungsstellen von Ländern, Wirtschaft und Wissenschaft ihre Informationskanäle aus und synchronisieren verstärkt ihre gewonnenen Lageinformationen.[44] Dies ermöglicht es CERTs von Bund, Ländern, Wirtschaft und Wissenschaft, Vorfälle noch effektiver zu bewerten, daraus gewonnene Erkenntnisse zu teilen und Reaktionsmaßnahmen einzuleiten. Hierzu wird das BSI seine Analysekapazitäten erhöhen, mehr Informationen und Erkenntnisse mit seinen Partnern teilen sowie die Informationen standardisiert und zielgruppengerecht aufbereiten. Die Vernetzungsstrukturen werden regelmäßig evaluiert und verbessert.

Die MIRTs sind technisch, personell und finanziell so ausgebaut, dass sie die steigenden Bedarfe Kritischer Infrastrukturen sowie von Institutionen im besonderen öffentlichen Interesse an professioneller Unterstützung vor Ort nachhaltig erfüllen können.

---

[44] Zur Stärkung des Informationsaustausches im Cyber-AZ siehe strategisches Ziel 8.3.4 „Das Cyber-AZ weiterentwickeln“.

Das BSOC arbeitet mit den für Detektion zuständigen Stellen der Länder eng zusammen. Die Gründung eines SOC-Verbundes als Ergänzung des VCV mit hiervon abgegrenzten Aufgaben wird dabei in Betracht gezogen. Gleichzeitig ist das BSOC als nationale Koordinationsstelle für das von der EU-Kommission geplante Cyber Shield etabliert.

Welche Wirkung erwarten wir?

Die technisch, personell und finanziell weiterentwickelten und besser vernetzten technisch-operativen Stellen des BSI sind in der Lage, schnell und effektiv zu handeln. Cybersicherheitsvorfälle in den Regierungsnetzen und in der Bundesverwaltung werden zeitnah und zuverlässig erkannt. Die Schadenswirkung von Cyberangriffen wird minimiert. Betroffene innerhalb und außerhalb der Bundesverwaltung werden bestmöglich bei der Bewältigung von Cybersicherheitsvorfällen unterstützt. Neue Angriffsmethoden und eine höhere Anzahl von Cyberangriffen können erkannt und bewältigt werden. Der Informationsaustausch zwischen Bund und Ländern und mittels des EU Cyber Shields erhöht die Erkennungsrate sicherheitsrelevanter Ereignisse und reduziert die Erfolgswahrscheinlichkeit von Angriffen spürbar.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSOC ist als nationale Verbindungsstelle der EU Cyber Shield-Initiative etabliert.
- Das BSOC kooperiert mit den zuständigen Länder-Stellen im Bereich der Detektion.
- Die MIRTs können den von Kritischen Infrastrukturen sowie von Institutionen im besonderen öffentlichen Interesse gemeldeten Unterstützungsbedarf zeitnah und effektiv erfüllen.

8.3.3 Die institutionalisierte Zusammenarbeit zwischen dem BSI und den Ländern stärken

Warum ist das Ziel relevant?

Der Cyberraum ist länderübergreifend hoch vernetzt. Um in diesem Umfeld ein möglichst einheitliches Sicherheitsniveau zu gewährleisten und effektiv auf Cyberbedrohungen zu reagieren, ist eine enge Zusammenarbeit zwischen Bund und Ländern unter Einbindung der Kommunen unabdingbar. Für die erforderliche intensive und dauerhafte gegenseitige Information, Abstimmung und Unterstützung bedarf es institutionalisierter Kooperationsformen.

Wo stehen wir?

Für die Bereiche Cyberkriminalität und Cyberspionage bestehen im Bund-Länder-Verhältnis bewährte Gremienstrukturen. Darüber hinaus sind das BKA und das BfV mit ihrer jeweiligen Zentralstellenfunktion bereits als tragende Säulen einer föderal integrierten Cybersicherheitsarchitektur ausgestaltet.

Auch im Aufgabenbereich des BSI gibt es im Bund-Länder-Verhältnis funktionierende Kooperationsplattformen – insbesondere im Bereich der präventiven Eigensicherung der Verwaltungen. Ebenso hat sich die Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz als Austauschplattform zwischen Bund und Ländern bewährt. Darüber hinaus wurde dem BSI die Unterstützung der Länder als gesetzliche Aufgabe übertragen. Aufgrund der grundgesetzlichen Zuständigkeitsverteilung zwischen Bund und Ländern ist diese jedoch auf eine ergänzende Hilfeleistung im Einzelfall im Rahmen der Amtshilfe beschränkt.

Was wollen wir erreichen?

Um die effektive Zusammenarbeit zwischen dem BSI und den Ländern zeitnah zu stärken, wird der Abschluss verbindlicher bilateraler Kooperationsvereinbarungen angestrebt, in denen die Schwerpunkte des gemeinsamen Engagements festgeschrieben werden. Die jeweilige Kooperationsvereinbarung führt die Felder, in denen eine Zusammenarbeit zwischen dem BSI und dem jeweiligen Land bereits stattfindet oder künftig stattfinden soll, in einer Vereinbarung zusammen und gibt dieser Kooperation einen planbaren und strukturierten Rahmen.

Um die institutionalisierte Zusammenarbeit zwischen Bund und Ländern zu vertiefen, wird darüber hinaus angestrebt, das BSI in seinem Aufgabenbereich zu einer Zentralstelle im Bund-Länder-Verhältnis auszubauen und somit – neben dem BKA im Polizeiwesen und dem BfV im Verfassungsschutzverbund – zur dritten Säule einer föderal integrierten Cybersicherheitsarchitektur weiterzuentwickeln. Als Zentralstellen ausgestaltete Bundesbehörden erlauben organisatorische Verbindungen verschiedener Bundes- und Landesbehörden zur dauerhaften gegenseitigen Information, Abstimmung und Unterstützung.

Welche Wirkung erwarten wir?

Durch die intensivere Zusammenarbeit zwischen Bund und Ländern auf Grundlage bilateraler Kooperationsvereinbarungen werden Ressourcen des Staates durch abgestimmtes Handeln und die Bündelung von Kompetenzen effektiver eingesetzt. Zielgruppen in Staat, Wirtschaft und Gesellschaft können breiter und zielgenauer adressiert werden. Der Wissens- und Kompetenztransfer zwischen Bund und Ländern nimmt zu.

Durch den Ausbau des BSI zur Zentralstelle wird ein weiterer Schritt zu einer effektiven Cybersicherheitsarchitektur gegangen. Auf die Zentralstellenfunktion des BSI kann eine kooperative und komplementäre Aufgabenverteilung zwischen Bund und Ländern gestützt werden, in deren Umsetzung ein umfassender Informationsaustausch gewährleistet ist und eine dauerhafte und regelmäßige gegenseitige Unterstützung stattfinden kann. Auf dieser Basis werden die Fähigkeit zur Prävention, Erkennung von und Reaktion auf Cyberbedrohungen und damit das gesamtstaatliche Cybersicherheitsniveau verbessert.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das BSI hat bilaterale Kooperationsvereinbarungen mit den Ländern abgeschlossen und führt auf deren Grundlage gemeinsame Vorhaben durch.
- Das BSI wurde durch Änderung des Grundgesetzes und nachfolgende einfachrechtliche Anpassungen zur Zentralstelle in seinem Aufgabenbereich im Bund-Länder-Verhältnis ausgebaut.

8.3.4 Das Cyber-AZ weiterentwickeln

Warum ist das Ziel relevant?

Cyberbedrohungen sowie Motivation und Ziel von Cyberangriffen sind oftmals nicht unmittelbar erkennbar. Je nach konkreter Fallgestaltung werden Cyberangriffe, Cyberbedrohungen und Cybergefahren daher regelmäßig nur einem Teil der zuständigen Behörden oder auch nur einzelnen betroffenen Einrichtungen bekannt. Darüber hinaus ist nicht immer gewährleistet, dass gesamtstaatlich relevante Sachverhalte zeitnah als solche erkannt werden. Dadurch wird eine angemessene Reaktion auf die Cybervorfälle erschwert.

Wo stehen wir?

Das Cyber-AZ ist eine 2011 gegründete Kooperations- und Informationsplattform, an der zurzeit das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das BSI, das BfV, das BKA, der BND, das Bundespolizeipräsidium (BPOLP) und das KdoCIR beteiligt sind. Es ist ein wesentlicher Bestandteil der Cybersicherheitsarchitektur Deutschlands, dessen Arbeitsweise sich stetig an aktuelle Entwicklungen anpassen muss. 2019 wurde die Zusammenarbeit im Cyber-AZ neu konzipiert. Damit wurden weitere Maßnahmen ergriffen, um die Fähigkeit zur koordinierten und kooperativen Bewältigung von Sachverhalten mit gesamtstaatlicher Relevanz auszubauen und den Informationsaustausch weiter zu verbessern.

Was wollen wir erreichen?

Das Cyber-AZ als zentrale Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-) Behörden wird in Abhängigkeit von der Entwicklung der Bedrohungslage fortentwickelt. Zur Stärkung des insbesondere ressortübergreifenden Informationsaustausches zu Cyberangriffen, Cyberbedrohungen und Cybergefahren werden die Grundlagen für den behördenübergreifenden Austausch von Informationen angepasst, der Austausch intensiviert und – soweit zur Zielerreichung geeignet – weitere Partner in die Arbeit des Cyber-AZ integriert; hierzu gehören insbesondere auch die Länder.

Durch den intensivierten Austausch, technisch unterstützte Lageinformationsverarbeitungs-, Auswerte- und Darstellungssysteme und dadurch verbesserte bedarfsgerechte Analysen wird die Berichterstattung des Cyber-AZ erweitert und verbessert. Der digitale Austausch auch von höher eingestuften Informationen zwischen allen teilnehmenden Institutionen soll möglich, die Auswertefähigkeit des Cyber-AZ beschleunigt und das Führen eines aktuellen, abgestimmten Gesamtlagebildes zur Cybersicherheitslage ermöglicht werden. Neue Berichtsformate des Cyber-AZ sollen zu Cyberangriffen in und Cybergefahren für Deutschland einen umfassenden und aktuellen Überblick gewährleisten. Dies schließt auch einen leistungsfähigen Informationsaustausch mit der Wirtschaft ein. Zudem ist sichergestellt, dass bei komplexen Cyberlagen der Übergang von der Cyberabwehr zur Cyberverteidigung erkannt wird.

Welche Wirkung erwarten wir?

Informationen zu Cybersicherheitsvorfällen werden schneller unter Berücksichtigung aller betroffenen Behörden kommuniziert und komplexe Cyberlagen so besser behörden- und ressortübergreifend koordiniert.

Die Erweiterung des Cyber-AZ durch Einbindung weiterer ausgewählter Einrichtungen, Stellen oder Organisationen trägt dazu bei, zusätzliche Informationsquellen oder Handlungsoptionen zu erschließen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Grundlagen für den behördenübergreifenden Austausch von Informationen im Cyber-AZ wurden angepasst.
- Cybersicherheitsvorfälle und Cyberlagen werden schnell und effektiv bearbeitet.
- Ein umfassendes und aktuelles Cyberlagebild ist jederzeit verfügbar.

8.3.5 Cyber- und Informationssicherheit der Bundesverwaltung stärken

Warum ist das Ziel relevant?

Die Bundesverwaltung befindet sich inmitten eines Prozesses der digitalen Transformation. Eine digitale Verwaltung ist maßgeblich für ein funktionsfähiges, effizientes und modernes Staatswesen. Gleichzeitig steigt auch der Anteil digitaler Angebote des Bundes für Wirtschaft und Gesellschaft. Auch hier ist Cyber- und Informationssicherheit essenziell für die Funktionsfähigkeit und Vertrauenswürdigkeit der staatlichen digitalen Angebote.

Wo stehen wir?

Das Informationssicherheitsmanagement der Bundesverwaltung beruht auf dem vom Kabinett beschlossenen UP Bund. Der UP Bund ist die Informationssicherheitsrichtlinie des Bundes und formuliert die verbindlichen Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Informationen und der dabei genutzten IT-Systeme, Dienste und Kommunikationsnetzinfrastrukturen des Bundes. Unter anderem regelt er die Einhaltung des IT-Grundschutzes sowie der vom BSI entwickelten Mindeststandards durch die Bundesbehörden. Laut UP Bund ist bei ressortübergreifenden Vorhaben frühzeitig, das heißt bereits in der Initiierungs- und Konzeptionsphase, sicherzustellen, dass die Aspekte der Informationssicherheit in angemessener Weise berücksichtigt werden. Das BSI ist in geeigneter Weise in beratender Rolle einzubinden.

Was wollen wir erreichen?

Die Cybersicherheitsarchitektur des Bundes soll auf strategischer Ebene gestärkt werden. Zudem soll auf operativer Ebene ein Kompetenzzentrum Operative Sicherheitsberatung Bund im BSI eingerichtet werden, um die Ressorts bei der Umsetzung von Sicherheitsvorhaben zu unterstützen. Darüber hinaus stärken wir die Rolle der Informationssicherheitsbeauftragten der Bundesverwaltung, indem wir hierfür eine gesetzliche Grundlage schaffen.

Welche Wirkung erwarten wir?

Wir verbessern und stärken das vorhandene Informationssicherheitsmanagement der Bundesverwaltung und die Unterstützung der Informationssicherheitsbeauftragten der einzelnen Bundesbehörden durch das BSI vor Ort. Außerdem stellen wir sicher, dass das BSI frühzeitig in die Digitalisierungsvorhaben des Bundes eingebunden wird. Informationssicherheit wird so zu einem natürlichen Bestandteil in der Digitalisierung der Bundesverwaltung.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die gesetzliche Grundlage für die Rolle der Informationssicherheitsbeauftragten der Bundesverwaltung wurde geschaffen.
- Die Überprüfung vorhandener Rollen und Schnittstellen im Informationssicherheitsmanagement auf Verbesserungspotential ist erfolgt. Ein Konzept für deren bedarfsweisen Ausbau beziehungsweise die Entwicklung neuer Rollen im Hinblick auf die Erhöhung der Cyber- und Informationssicherheit sowie die Zusammenarbeit der (Ressort-)Informationssicherheitsbeauftragten untereinander auf Ebene des Bundes liegt vor.

- Die Zusammenarbeit zwischen den Ressort-IT-Sicherheitsbeauftragten des Bundes ist deutlich gestärkt, inhaltliche wie ggf. auch institutionelle Maßnahmen dazu sind getroffen.
- Das Kompetenzzentrum Operative Sicherheitsberatung Bund des BSI wurde eingerichtet und hat seine Arbeit aufgenommen.
- Ein gezieltes Verstärkungsprogramm für die Cyber- und Informationssicherheit des Bundes ist ressortübergreifend abgestimmt und verabschiedet.

8.3.6 Cybersicherheit im Umfeld von Wahlen erhöhen

Warum ist das Ziel relevant?

Allgemeine, unmittelbare, freie, gleiche und geheime Wahlen sind das Fundament unserer Demokratie. Auch vor diesem Fundament macht die Digitalisierung nicht halt – das Internet dient als Informationsquelle für die politische Meinungsbildung, soziale Medien werden als Instrument für den Wahlkampf genutzt und nicht zuletzt erfolgt auch die Übermittlung der vorläufigen Wahlergebnisse digital. Die Absicherung des Wahlumfeldes ist daher auch eine Herausforderung für die Cybersicherheit.

Darüber hinaus ist gerade vor Wahlen die Gefahr von Einflussnahmeoperationen durch ausländische Nachrichtendienste erhöht. Ereignisse im Ausland verdeutlichen die Fähigkeiten und die grundsätzliche Bereitschaft zu Einflussnahmeversuchen durch Veröffentlichung ausspionierter kompromittierender oder auch manipulierter Daten.

Wo stehen wir?

Im Umfeld von Wahlen sensibilisieren die Behörden des Bundes relevante Akteure für Cybergefahren und beraten zur Informationssicherheit. Zudem entwickelt das BSI im Auftrag des Bundeswahlleiters Sicherheitsanforderungen zum Schutz der Ergebnisübermittlung von Bundestagswahlen. Die Aufklärung von Cyberangriffen zur Einflussnahme im Vorfeld von Wahlen nehmen die Nachrichtendienste in ihrer Funktion als Frühwarnsystem wahr.

Was wollen wir erreichen?

Um die Verwundbarkeit des zunehmend digitalisierten Wahlumfeldes und der Wahlinfrastruktur zu reduzieren, wird angestrebt, die Cybersicherheit im Umfeld von Wahlen zu erhöhen.

Die Behörden des Bundes unterstützen relevante Akteure im Wahlumfeld im Hinblick auf die Cybersicherheit. Im jeweiligen Zuständigkeitsbereich analysieren sie Risiken, identifizieren Sicherheitsanforderungen und stehen im politischen Raum als Ansprechpartner für Belange der Cybersicherheit im Zusammenhang mit Wahlen zur Verfügung.

Welche Wirkung erwarten wir?

Wahlen werden durch Erreichung eines angemessenen Sicherheitsniveaus des Wahlumfeldes mittels Prävention, Vorfeldaufklärung, Detektion und Reaktion geschützt. Das politische Umfeld ist sich der Bedrohungssituation im Cyberraum im Zusammenhang mit Wahlen bewusst und kann entsprechende Schutzmaßnahmen ergreifen.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es existieren stets der Lageentwicklung angepasste Handlungsempfehlungen und ein Beratungsangebot für Wahlleitungen auf Bundes- und Landesebene.
- Zielgruppen des politischen Raumes werden für Belange der Cybersicherheit im Umfeld von Wahlen sensibilisiert.

- Es existiert ein fundiertes und auf den Aspekt „Wahlen“ spezifiziertes Cyberbedrohungslagebild, welches schädliche Akteure, deren Motive und Vorgehensweisen benennt.

8.3.7 Strafverfolgung im Cyberraum intensivieren

Warum ist das Ziel relevant?

Nicht nur die Zahl der von Cyberkriminalität betroffenen Computersysteme und Endgeräte steigt, sondern auch die Professionalität der Täterinnen und Täter. Einerseits versuchen Täterinnen und Täter weiterhin, mit möglichst geringem Aufwand möglichst viele Computer mit Schadsoftware zu infizieren, um beispielsweise Kontodaten und Passwörter zu stehlen. Andererseits gibt es jedoch auch immer mehr sehr gut vorbereitete und hoch organisierte Cyberangriffe auf ausgewählte Ziele (beispielsweise Wirtschaftsunternehmen oder Kritische Infrastrukturen), bei denen das Schadenspotenzial für die Betroffenen erheblich größer ist. Gleichzeitig bringen aktuelle technische Entwicklungen, wie beispielsweise Automotive IT oder IoT, immer neue Tatmöglichkeiten und Deliktsphänomene hervor.

Angesichts dieser sich entwickelnden Bedrohungslage im Cyberraum müssen die Sicherheitsbehörden des Bundes und der Länder ihre gesetzlichen Aufgaben zur Verfolgung von Straftaten in der digitalen Welt genauso wie in der analogen Welt wahrnehmen können. Hierzu benötigen sie ausreichende Befugnisse[45].

Wo stehen wir?

Die Computerstraftaten sind in den §§ 202a ff., 263a, 269 f. und 303a f. des Strafgesetzbuches geregelt. In den vergangenen Jahren sind eine Reihe von Änderungs- und Überarbeitungsvorschlägen für das Computerstrafrecht vorgelegt und diskutiert worden, unter anderem gab es mehrere Gesetzesinitiativen des Bundesrats.

Was wollen wir erreichen?

Die Sicherheitsbehörden des Bundes und der Länder benötigen ausreichende Befugnisse, um ihre Aufgaben in der digitalen Welt ebenso effektiv wahrnehmen zu können wie in der analogen Welt. Die Befugnisse werden daher fortlaufend überprüft und erforderlichenfalls an neue technische Entwicklungen angepasst. Dabei ist unter anderem zu prüfen, ob Ermittlungsmaßnahmen, wie TKÜ und Online-Durchsuchung, auch für die Ermittlung von Computerdelikten zur Verfügung stehen sollten.

Zudem sollen die geltenden strafrechtlichen Regelungen im Bereich des Computerstrafrechts auf Reformbedarf überprüft werden.

Welche Wirkung erwarten wir?

Die Arbeitsfähigkeit der Sicherheitsbehörden bleibt im digitalen Zeitalter erhalten. Sie können angemessen auf neue Deliktsphänomene und erhöhtes Gefahrenpotential im Cyberraum reagieren.

---

[45] Zur internationalen Strafverfolgung und Bekämpfung von Cyberkriminalität siehe auch das strategische Ziel **Fehler! Verweisquelle konnte nicht gefunden werden.** „Internationale Zusammenarbeit bei der Strafverfolgung stärken und internationale Cyberkriminalität bekämpfen".

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Befugnisse aus der Strafprozessordnung entsprechen den Anforderungen der Praxis.
- Für das Strafgesetzbuch werden, sofern eine Überprüfung entsprechenden Bedarf ergibt, Gesetzgebungsvorschläge vorgelegt.

8.3.8 Zentrale Kompetenz- und Service-Dienstleistungen des BKA zur Bekämpfung von Cyberkriminalität ausbauen

Warum ist das Ziel relevant?

Im Rahmen seiner bestehenden Aufgaben unterstützt das BKA die Polizeien des Bundes und der Länder, indem zum einen operative Daten zur Verfügung gestellt werden und zum anderen modernste Technik für die kriminalpolizeiliche Arbeit gebündelt vorgehalten wird. Cyberkriminalität ist weiter zunehmend durch Angriffe gekennzeichnet, die in ihrem Auftreten in einem bestimmten Zeitraum quantitativ wellenförmig zu- und wieder abnehmen und dabei Geschädigte in mehreren Bundesländern oder aber im gesamten Bundesgebiet betreffen. Um einen Serienzusammenhang zu erkennen, ist eine umfängliche Koordination mit allen betroffenen Ermittlungsbehörden notwendig.

Wo stehen wir?

Das BKA hat mit dem Konzept der CyberToolBox begonnen, Informationen, Daten und Werkzeuge zur Verfügung zu stellen. Die CyberToolBox wurde Ende 2019 ausgerollt und als operatives Informationsportal etabliert. Die darin bereitgestellten Werkzeuge und Datensets wurden seitdem sukzessive ausgebaut. Aktuell nutzen über 5.000 Mitarbeiterinnen und Mitarbeiter von Strafverfolgungsbehörden die dort bereitgestellten Werkzeuge und innerhalb von zwölf Monaten konnten in mehr als 8.000 Fällen in den Ländern isoliert (zu gleichen Tat- beziehungsweise Täterstrukturen) geführte Ermittlungsverfahren zusammengeführt werden.

Das BKA unterstützt die Polizeidienststellen des Bundes und der Länder bei der Koordinierung beziehungsweise Durchführung von zentralen Ermittlungen im Zusammenhang mit Straftatenwellen.

Was wollen wir erreichen?

Der Austausch von Informationen, Kompetenzen und Tools zwischen dem BKA und den Polizeidienststellen des Bundes und der Länder im Rahmen der jeweils bestehenden Rechtsvorschriften ist qualitativ und quantitativ intensiviert. Die weiterentwickelte CyberToolBox befriedigt einen wesentlichen Teil der datenbasierten operativen Informations- und Unterstützungsbedürfnisse der Länder und eröffnet ihnen Zugang zu allen phänomenrelevanten Informationen, Daten und Werkzeugen, die sie benötigen. Eine bundesweite Community von Cyberkriminalitäts-Ermittlungsdienststellen befördert den direkten und effizienten Austausch operativer und ermittlungsrelevanter Erkenntnisse und Methoden.

Sofern durch eine oder mehrere Polizeidienststellen des Bundes oder der Länder oder durch das BKA eine Straftatenwelle festgestellt wird, koordinieren die genannten Behörden die Durchführung von „Zentralen Ermittlungen“, die langfristig verstärkt zu führen sein werden.

Welche Wirkung erwarten wir?

Diese Erweiterungen des Funktions- und Leistungsumfangs der CyberToolBox werden die Nutzerzahlen steigen lassen und eine höhere Anzahl von an das BKA übermittelten Operativdaten bewirken. Auf dieser Basis ist es dem BKA dann wiederum möglich, die notwendigen Zentralstellenaufgaben wahrzunehmen.

Beim Auftreten von Straftatenwellen trägt das Instrument der „Zentralen Ermittlungen“ zu einer bedarfsgerechten Auslastung der Polizeidienststellen und effektiven Ermittlungsführung bei, insbesondere zur Vermeidung von Doppelarbeit.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das Instrument der „Zentralen Ermittlungen“ wird häufiger angewandt.
- Die Nutzerzahl der CyberToolBox ist gestiegen.
- Die Anzahl der übermittelten fachlichen Anfragen an die CyberToolBox ist gestiegen.
- Die Treffer- und Auskunftsquote der CyberToolBox ist gestiegen.
- Die Anzahl der durch die CyberToolBox bereitgestellten Daten ist gestiegen.

8.3.9 Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten

Warum ist das Ziel relevant?

Immer mehr Kommunikationskanäle und Datenspeicherdienste werden durch Ende-zu-Ende-Verschlüsselung gesichert. Die sichere Verschlüsselung ist ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Staat, Wirtschaft und Gesellschaft. Doch auch Kriminelle nutzen Verschlüsselungslösungen für die Vorbereitung und Durchführung von Straftaten. Die Verschlüsselung macht den Zugang zu Kommunikationsinhalten und deren Analyse im Rahmen einer rechtmäßig angeordneten TKÜ, die insbesondere bei schwersten Straftaten und der organisierten Kriminalität eine zentrale Erkenntnisquelle für die Ermittlungsbehörden darstellt, äußerst schwierig oder gar praktisch unmöglich.

Daher gilt es entsprechend dem Grundsatz „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung", die Privatsphäre und die Sicherheit der Kommunikation durch Verschlüsselung zu schützen. Gleichzeitig soll für die zuständigen Behörden die Möglichkeit aufrechterhalten werden, über einen rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke im Rahmen der Bekämpfung schwerer und/oder organisierter Kriminalität, Kinderpornographie und Terrorismus – auch in der digitalen Welt – zu verfügen und die Rechtsstaatlichkeit zu wahren.

Wo stehen wir?

Die bisher etablierten Ausgleichsmaßnahmen der sogenannten Informationstechnischen Überwachung (Quellen-TKÜ) sowie die Onlinedurchsuchung sind wegen der operativen und technischen Herausforderungen in der Praxis auf Einzelfälle beschränkt.

Damit die Sicherheitsbehörden auch künftig in der Lage sind, ihre gesetzlichen Aufgaben vollständig zu erfüllen, sind neue Herangehensweisen in Bezug auf den unverschlüsselten Zugriff auf ursprünglich verschlüsselte Kommunikationsinhalte erforderlich.

Der Rat der Europäischen Union hat im Dezember 2020 eine Entschließung zum Umgang mit Verschlüsselung verabschiedet, in der die Notwendigkeit des Grundsatzes „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" hervorgehoben wird. Es soll ein Dialog mit den Technologieunternehmen geführt werden, um einen technikneutralen Ansatz für Ausgleichsmaßnahmen zur TKÜ zu finden unter Wahrung der grundrechtlichen Schutzvorgaben.

Was wollen wir erreichen?

Es bestehen die notwendigen Voraussetzungen, die den zuständigen Behörden einen rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke im Rahmen der Bekämpfung schwerer und/oder organisierter Kriminalität, Kinderpornographie und Terrorismus einräumen und gleichzeitig die Privatsphäre, die Grundrechte und die Sicherheit der Kommunikation schützen.

Hierzu werden, zunächst in enger Abstimmung mit den Diensteanbietern, anderen betroffenen Interessenträgern und allen zuständigen Behörden, technische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation entwickelt. Um einem Missbrauch dieser Lösungen sowohl im europäischen als auch im internationalen Bereich vorzubeugen, werden technische, organisatorische und rechtliche Maßnahmen mit vorgesehen.

Welche Wirkung erwarten wir?

Die deutschen Sicherheitsbehörden können ihre gesetzlich vorgesehenen technischen Möglichkeiten der TKÜ auch bei verschlüsselten Inhalten effektiv wahrnehmen. Damit bleibt die TKÜ weiterhin ein zentraler Bestandteil der Ermittlungsmöglichkeiten und nachrichtendienstlichen Aufklärung. Die effektive Strafverfolgung und rechtzeitige Gefahrenabwehr bei schweren und schwersten Straftaten sowie die nachrichtendienstliche Aufklärung in hervorgehobenen Fällen ist dadurch weiterhin gewährleistet und unter anderem organisierte Kriminalität und Terrorismus können weiterhin wirksam bekämpft werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das Ziel eines europäischen Ansatzes unter Bezugnahme auf die Entschließung des Rates der EU zum Umgang mit Verschlüsselung mit Fokus auf einem technikneutralen Ansatz und dem dauerhaften Dialog mit den Diensteanbietern ist verankert.
- Technische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation sind in enger Abstimmung mit allen betroffenen Unternehmen, Interessenträgern und zuständigen Behörden auf europäischer Ebene entwickelt.
- Vorschläge für gesetzliche Grundlagen, die den rechtmäßigen und verhältnismäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation ermöglichen, wurden erarbeitet.

8.3.10 Den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits fördern

Warum ist das Ziel relevant?

Die Ziele, einerseits größtmögliche IT-Sicherheit zu gewährleisten, und andererseits die Notwendigkeit, Strafverfolgungs- und Sicherheitsbehörden die Erfüllung ihres gesetzlichen Auftrags zu ermöglichen, stehen in einem Spannungsverhältnis zueinander.

Dieses Spannungsverhältnis ist innerhalb der gesetzlichen Rahmenbedingungen und unter Bewahrung des größtmöglichen Schutzes für alle betroffenen (Grund-)Rechtsgüter aufzulösen. Im Interesse der Sicherheit, Vertraulichkeit und Integrität informationstechnischer Systeme ist es essenziell, dass erkannte Schwachstellen grundsätzlich geschlossen beziehungsweise zu diesem Zweck an die Hersteller gemeldet werden. Die Strafverfolgungs- und Sicherheitsbehörden müssen auch unter Berücksichtigung dieser Maßgaben ihrer Ermittlungs- und Aufklärungsarbeit weiterhin effektiv, gegebenenfalls mit restriktiven Ausnahmen, nachkommen können.

Eine **Schwachstelle** ist definiert als eine Sicherheitslücke in Soft- oder Hardware, die einzeln oder kombiniert genutzt werden kann, um (in der Regel unbemerkt) aktiven Zugriff auf ein Hard- oder Softwaresystem zu erhalten. Man unterscheidet zwischen sogenannten Zero-Day (auch 0-day), dem Hersteller unbekannten, und sogenannten n-Day Sicherheitslücken, die dem Hersteller bereits n Tage bekannt sind.

Ein **Exploit** (englisch to exploit: ausnutzen) ist ein Werkzeug oder eine systematische Möglichkeit (auch Beschreibung), um Schwachstellen und Fehlfunktionen von Hard- oder Software auszunutzen, um sich Zugriff auf die Daten oder Ressourcen zu verschaffen.

Wo stehen wir?

Die Nutzung von Zero-Day-Schwachstellen zu Zwecken der nachrichtendienstlichen Aufklärung, Gefahrenabwehr und Strafverfolgung erfolgt aktuell nach den für die jeweilige Sicherheitsbehörde geltenden internen Behördenvorgaben. Für diese im Einzelfall durchzuführende Nutzung gelten die allgemeinen Vorschriften.

Um diesen Prozess zu verbessern, wird an einer ausgewogenen behördenübergreifenden Strategie für den Umgang mit Schwachstellen für die Strafverfolgungs- und Sicherheitsbehörden gearbeitet (sogenannter Schwachstellenmanagementprozess - Vulnerability Equities Process).

Was wollen wir erreichen?

Eine ausgewogene behördenübergreifende Strategie zum Umgang mit Zero-Day-Schwachstellen nach den jeweils geltenden gesetzlichen Vorgaben bei den Strafverfolgungs- und Sicherheitsbehörden über bereits vorhandene interne Behördenvorgaben hinaus bringt die Interessen der Cyber- und Informationssicherheit sowie der Strafverfolgungs- und Sicherheitsbehörden in einen angemessenen Ausgleich. Grundlage dafür sind standardisierte Prozesse bei den Sicherheitsbehörden für einen sicheren und sachgerechten Umgang mit Schwachstellen und Exploits.

Kernpunkt dieser Prozesse ist die Risikoabwägung zwischen dem Gefährdungspotential von (Zero-Day-)Schwachstellen bei temporärer Ausnutzung durch die Sicherheits- und Strafverfol-

gungsbehörden und dem prognostizierten Nutzen für die nachrichtendienstliche Aufklärung, Gefahrenabwehr und Strafverfolgung (zur Einleitung des Coordinated Vulnerability Disclosure-Prozesses siehe strategisches Ziel 8.1.8 „Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure fördern“).

Durch diesen Rahmen entsteht ein „verantwortungsvolles Schwachstellenmanagement“, welches klare Richtlinien für den Umgang mit Schwachstellen vorgibt. Der geschilderte Konflikt zwischen IT-Sicherheit und nachrichtendienstlicher Aufklärung, Gefahrenabwehr sowie Strafverfolgung wird so aufgelöst. Dabei steht der größtmögliche Schutz der Bevölkerung im Vordergrund. Abgewogen werden daher solche Gefahren, die Schwachstellen in informationstechnischen Systemen mit sich bringen, mit dem Erfolg bei der Erkennung und Abwehr schwerer Gefahren sowie einer effektiven Strafverfolgung, die mit Hilfe der Nutzung von (Zero-Day-)Schwachstellen erzielt werden können.

Welche Wirkung erwarten wir?

Das Sicherheitsniveau im Bereich der öffentlichen Sicherheit ist ebenso erhöht wie das Niveau der allgemeinen IT-Sicherheit. Inkonsistenzen im Umgang mit Zero-Day-Schwachstellen und Exploits sind beseitigt und es gibt einen verlässlichen nationalen Rahmen zum verantwortungsvollen Umgang mit diesen Instrumenten.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand des folgenden Kriteriums überprüfen:

- Es ist ein verbindliches Vorgehen etabliert, das den verantwortungsvollen Umgang mit Zero-Day-Schwachstellen und Exploits regelt.

8.3.11 Die Digitale Souveränität der Sicherheitsbehörden durch den Ausbau der ZITiS stärken

Warum ist das Ziel relevant?

Die Sicherheitsbehörden benötigen gerade in ihren kritischen Arbeitsfeldern der Cybersicherheit Lieferanten, die auch im Krisenfall zuverlässig zur Verfügung stehen. Sie sind auf Werkzeuge angewiesen, deren Funktionsweise auch vor dem Hintergrund ihrer Einsatzfähigkeit zur gesetzlichen Auftragserfüllung, wie zum Beispiel bei einer TKÜ, transparent dargelegt werden kann. Die hierfür notwendigen Kernfähigkeiten sind entsprechend aufzubauen und vorzuhalten, insbesondere, wenn sich Lieferketten verändern oder im Krisenfall nicht verlässlich sind. Dies ist unverzichtbar für die selbstbestimmte Aufgabenerfüllung der Sicherheitsbehörden und trägt im Sinne einer gesamtstaatlichen Handlungsfähigkeit maßgeblich zur Digitalen Souveränität Deutschlands bei.

Wo stehen wir?

Es ist im Schwerpunkt Aufgabe der ZITiS, für die Sicherheitsbehörden im Geschäftsbereich des BMI Werkzeuge und Methoden zu entwickeln, nachzuvollziehen, zu bewerten und zentral zur Verfügung zu stellen, deren Bündelung aufgrund gleichgelagerter Herausforderungen im Cyberraum bei Polizeien und Nachrichtendiensten erforderlich geworden ist.

Jedoch erfordert die hochdynamische technische Entwicklung für Sicherheitsanwendungen vor dem Hintergrund enormer Investitionen, die im Nicht-EU-Ausland in Zukunftstechnologien erfolgen, eine strategische Neuausrichtung, um auch künftig aus eigener Kraft handlungsfähig zu sein. Die Schwerpunktsetzung im Bereich der Forschung und Entwicklung ist beständig zu überprüfen und je nach technischem Fortschritt erforderlichenfalls anzupassen und dient als Grundlage für den Auftrag der ZITiS als Dienstleister für die Sicherheitsbehörden. Aktuell bestehen bei den eingesetzten und notwendigen technischen Lösungen häufig große Abhängigkeiten, insbesondere vom außereuropäischen Ausland. Ein gravierender Anteil der für die gesetzliche Auftragserfüllung eingesetzten technischen Geräte, Werkzeuge und Methoden der informationstechnischen Überwachung, Datenanalyse und Mustererkennung ist dementsprechend aufgrund fehlender industrieller Basis auf nationaler Ebene oder in der EU nicht im benötigten Umfang verfügbar. Ein selbstbestimmtes, unabhängiges Handeln der Sicherheitsbehörden ist in diesem Bereich trotz eigener Fähigkeiten daher aktuell nicht immer wie gewünscht möglich.

Was wollen wir erreichen?

Die ZITiS wird in die Lage versetzt, Werkzeuge und Methoden zu entwickeln, zu bewerten und zentral zur Verfügung zu stellen, die den Sicherheitsbehörden ein selbstbestimmtes Handeln ermöglichen, eine krisenfeste Versorgungssicherheit gewährleisten und deren Cyberfähigkeiten signifikant stärken.

Die zentrale Forschung und Entwicklung zugunsten eigener Werkzeuge und Methoden für diese Behörden wird bei der ZITiS im Rahmen des geltenden Rechts weiter ausgebaut. Gleichzeitig werden auch die weiteren Behörden anderer Ressorts ihre Vorhaben in Forschung und Entwicklung im Rahmen des jeweils geltenden Rechts weiter intensivieren.

Soweit kommerzielle Produkte zur Erfüllung des gesetzlichen Auftrages bei Polizeien, Nachrichtendiensten und im Geschäftsbereich des BMVg zum Einsatz kommen, sollen diese zur Erhöhung der Einsatzsicherheit möglichst umfassend geprüft werden.

Welche Wirkung erwarten wir?

Die ZITiS wird sich dadurch als wichtiger Baustein für eine gesamtstaatliche Cybersicherheit weiter etablieren sowie Herausforderungen agil und schnell angehen und Zukunftstechnologien als zentraler Dienstleister für die Sicherheitsbehörden insbesondere im Geschäftsbereich des BMI erschließen können.

Durch ein passgenaues Angebot der ZITiS an technischen Lösungen, Werkzeugen und Beratungsleistungen für die Sicherheitsbehörden werden die souveräne Handlungsfähigkeit deutscher Sicherheitsbehörden im digitalen Raum und ihre Unabhängigkeit von Unternehmen aus dem außereuropäischen Ausland gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die durch die ZITiS bereitgestellten Dienstleistungen und Eigenentwicklungen werden durch die Sicherheitsbehörden des Bundes in Anspruch genommen.
- Die Abhängigkeit der Sicherheitsbehörden von außereuropäischen Produkten und Lösungen ist gesunken.
- Die Verfügbarkeit hochspezialisierter Expertinnen und Experten in den Kernthemen ist gestiegen.
- Es wurden ausreichende eigene Fähigkeiten hinsichtlich der Eigenentwicklung kritischer oder risikobehafteter Systeme und Methoden der Sicherheitsbehörden aufgebaut.
- Die ZITiS verfügt über eine zentrale und in Anspruch genommene Evaluierungskompetenz für Produkte und Systeme, die aus globalen Lieferketten bezogen werden.

8.3.12 Das Cybersicherheitsniveau durch gestärkte Vorfeldaufklärung erhöhen

Warum ist das Ziel relevant?

Cyberangriffe werden unter anderem zur Spionage, politischen Einflussnahme oder Sabotage eingesetzt. Auch Deutschland steht im Fokus nachrichtendienstlicher Gruppierungen, die fortgeschrittene Angriffstechniken verwenden (APT). Darüber hinaus nutzen unter anderem extremistische und terroristische Akteure – zum Teil als Dienstleistungen im Internet erwerbbare – Cybertechnologien für ihre Zwecke. Angesichts dieser Bedrohungen gilt es, umfassend für diese Gefahren zu sensibilisieren (Prävention), die Akteure, deren Motive und Fähigkeiten zu identifizieren (Aufklärung), konkrete Angriffe oder deren Vorbereitungen zu entdecken (Detektion), durch Information Maßnahmen zur Abwehr zu ermöglichen (Warnung) und die Urheber der Angriffe zu ermitteln (fachliche Attribuierung).

Die Frühwarnfunktion vor Cyberangriffen wird in der Cybersicherheitsarchitektur primär durch die Nachrichtendienste wahrgenommen.

Wo stehen wir?

Der wachsenden Bedeutung der nachrichtendienstlichen Aufklärung von Angreifern wurde durch organisatorische Maßnahmen in den Nachrichtendiensten des Bundes Rechnung getragen. So wurden beispielsweise mit der personellen Stärkung der Cyberabwehr des BfV und der Cyberauswertung im BND Maßnahmen ergriffen, die die Nachrichtendienste in die Lage versetzen, relevante Cyberakteure intensiver betrachten zu können. Durch die Aufstellung einer Referatsgruppe Cyberabschirmung hat sich auch das BAMAD für die Herausforderungen hinsichtlich der Bedrohungen aus dem Cyberraum gegen den Geschäftsbereich des BMVg besser ausgerichtet.

Was wollen wir erreichen?

Um auch zukünftig wesentliche Beiträge für die Bereiche der Prävention, Aufklärung, Detektion Warnung und fachlichen Attribuierung liefern zu können, ist es notwendig, sowohl die technischen als auch die fachlichen Fähigkeiten der Nachrichtendienste des Bundes zu stärken. Ferner achten wir darauf, dass die Nachrichtendienste des Bundes auch zukünftig, gemessen an der jeweiligen Bedrohungslage, über ausreichende gesetzliche Befugnisse zur Erfüllung ihres jeweiligen gesetzlichen Auftrags verfügen. Die technischen Analysefähigkeiten sollen durch regelmäßige Evaluierung und Anpassung von Analysetools, -umgebungen und Datenhaltungssystemen auf dem erforderlichen Stand gehalten und jeweils durch eine angemessene personelle Ausstattung hinterlegt werden.

Der notwendige Austausch mit anderen Nachrichtendiensten, Sicherheitsbehörden und sonstigen Stellen (einschließlich Wirtschaft) wird weiter verbessert mit dem Ziel, die dafür eingesetzten Ressourcen effektiver zu nutzen sowie die Cyberabwehr zu verbessern und der aktuellen Gefährdungslage anzupassen.

Welche Wirkung erwarten wir?

Durch eine effiziente und der Gefährdungslage angepasste Auftragsumsetzung der Nachrichtendienste des Bundes können Gefahren frühzeitig identifiziert, Risiken minimiert und das Entdeckungsrisiko der Urheber erhöht werden. Dadurch wird erreicht, dass die durch die Digitalisierung

erhöhte Angriffsfläche durch weit im Vorfeld eines Cyberangriffs stattfindende Maßnahmen wieder reduziert wird und sich das nationale Cybersicherheitsniveau in Summe erhöht.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Nachrichtendienste des Bundes verfügen gemessen an der Bedrohungslage über ausreichende gesetzliche Befugnisse zur Wahrnehmung ihrer gesetzlichen Aufgaben.
- Erforderliche technische und personelle Voraussetzungen für die angemessene und effiziente Aufklärung und Abwehr von Cyberangriffen sind ausgebaut.
- Die verbesserte Früherkennung und Aufklärung von Cyberangriffen hat zur Erhöhung gegebener Warnhinweise zur Gefahrenabwehr, zur nachhaltigen Unterstützung der Präventionsarbeit sowie zur politischen Attribuierung von Cyberakteuren ausländischer Provenienz beigetragen.

8.3.13 Verteidigungsaspekte der Cybersicherheit stärken

Warum ist das Ziel relevant?

Cyberverteidigung ist als militärischer Teil der Gesamtverteidigung verfassungsmäßiger Auftrag der Bundeswehr und unterliegt den für Einsätze der Bundeswehr geltenden nationalen wie völkerrechtlichen Regelungen. Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit sind gemäß Weißbuch 2016 originäre Aufgaben des BMVg und der Bundeswehr. Die Verteidigungsfähigkeiten der Bundeswehr im Cyberraum sind dabei auch wesentlicher Teil der Cybersicherheitsarchitektur. Im Spannungs- und Verteidigungsfall sind Cyberabwehr, Cyberaußen- und -Sicherheitspolitik sowie Cyberverteidigung sich ergänzende und etablierte Mittel, um die Risiken, die für Deutschland aus dem Cyberraum erwachsen, auf ein tragbares Maß zu reduzieren. Aufgrund der Charakteristika des Cyberraums und dessen hoher Dynamik gilt es, diese Mittel stets der Entwicklung anzupassen und geeignet weiterzuentwickeln. Dabei ist ein ressortübergreifender Ansatz zur Verteidigung im Cyberraum erforderlich.

Die Bundeswehr ist als hoch technisierte Armee im weltweiten Einsatz den Gefahren des Cyberraums fortlaufend ausgesetzt; gleichzeitig ist die Nutzung des Cyberraums Voraussetzung für die Einsatz- und Durchsetzungsfähigkeit der Streitkräfte.

Wo stehen wir?

Verantwortlichkeiten bei den Themen Cyber und IT sind an zentraler Stelle zusammengelegt und werden durch die Abteilung Cyber/Informationstechnik im BMVg sowie den Militärischen Organisationsbereich Cyber- und Informationsraum wahrgenommen; Cyberoperationsführung obliegt der Abteilung Strategie und Einsatz im BMVg. Neben der Zusammenführung bisher verteilter Fähigkeiten wurden neue Fähigkeiten aufgebaut.

Bereits außerhalb des Verteidigungs- oder Spannungsfalles sowie bei Einsätzen schirmt der MAD die Bundeswehr gegen Spionage und Sabotage sowie Extremismus und Terrorismus im Cyberraum ab. Als Nachrichtendienst im Geschäftsbereich des BMVg verfügt er über entsprechende gesetzliche Befugnisse und trägt so zur Auftragserfüllung der Streitkräfte bei.

Die Konzeption der Cyberverteidigung wird fortlaufend weiterentwickelt und an sich verändernde Gegebenheiten und Herausforderungen angepasst.

Was wollen wir erreichen?

Es gilt, die Wirksamkeit der Strukturen und Fähigkeiten vor dem Hintergrund des sich kontinuierlich und schnell weiterentwickelnden Cyberraumes hinsichtlich der Zielerreichung einer Reduzierung der Risiken im Cyberraum auf ein tragbares Maß zu überprüfen und gegebenenfalls anzupassen. Die Kernfähigkeiten im Cyber- und Informationsraum sind erhalten und ausgebaut. Systeme für die Sicherstellung der Kernführungsfähigkeit und die Erhöhung der Resilienz von Waffen- und Wirksystemen sind als kritische IT-Komponenten identifiziert. Sie sind zielgerichtet als vertrauenswürdige Systeme aufgebaut beziehungsweise durch solche ersetzt.

Die zur Erreichung dieser Ziele erforderlichen IT-Services sind priorisiert aufgebaut beziehungsweise erhalten.

Innerhalb der Bundesregierung ist ein Konzept für die Aufgabenwahrnehmung im Rahmen der Verteidigung im Cyberraum im Spannungs- und Verteidigungsfall ebenso wie in konventionellen Bereichen abgestimmt und wird regelmäßig beübt.

Weiterhin werden die Verteidigungsaspekte der Cybersicherheit im Rahmen der Landes- und Bündnisverteidigung sowie weitere Möglichkeiten der Reaktion auf Bedrohungen im Cyber- und Informationsraum unter Berücksichtigung rechtlicher Fragestellungen und mit dem Ziel der Konkretisierung untersucht.

Welche Wirkung erwarten wir?

Die Cyberverteidigung ist wirksam und passt sich den dynamischen Änderungen im Cyber- und Informationsraum kontinuierlich an.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es existiert ein abgestimmtes Konzept zur Verteidigung im Cyberraum im Spannungs- und Verteidigungsfall, das regelmäßig beübt wird.
- Die Netze und Systeme der Bundeswehr sind so geschützt, dass es durch Cyberangriffe keine wesentlichen Einschränkungen in der Verfügbarkeit gibt.
- Die Bundeswehr ist darauf eingestellt, verfügbare Ressourcen, insbesondere zur Incident Response, gemäß den rechtlichen Vorgaben für Amtshilfe zur Verfügung zu stellen. Dabei werden zum Beispiel im Bereich der Incident Response Teams regelmäßig Übungen durchgeführt.

8.3.14 Das Telekommunikations- und Telemedienrecht und die Fachgesetze an den technologischen Fortschritt anpassen

Warum ist das Ziel relevant?

Die gesetzlichen Befugnisse für die Aufgabenwahrnehmung der Sicherheitsbehörden in den verschiedenen Fachgesetzen und das Telekommunikationsgesetz müssen mit den technologischen Entwicklungen Schritt halten und entsprechend kontinuierlich angepasst werden. Die rasante Entwicklung bei Vernetzung und Kommunikation der Zukunft führt zu erheblichen Veränderungen, insbesondere in den Bereichen mobile Kommunikation, IoT und Automotive IT. Mit der Einführung der 5. Mobilfunkgeneration (5G) steht beispielsweise eine technologische Evolution mit disruptivem Charakter bevor. Die Anzahl der mobil vernetzten Geräte wird erheblich zunehmen, hierzu gehören beispielsweise Drohnen, Roboter, Kommunikations-Endgeräte, smarte Brillen, holographische Displays und vielfältige Sensoren, die jede Art von Alltagsgegenstand digitalisieren.

Diese Entwicklung wird durch fünf Megatrends gefördert, die vor allem die Anforderungen an das Mobilfunknetz der 6. Generation (6G) maßgeblich bestimmen werden:

- Vernetzte Maschinen,
- Mensch-Maschine-Kommunikation,
- Künstliche Intelligenz,
- Öffnung der mobilen Kommunikation durch Einführung offener, standardisierter Schnittstellen zwischen relevanten Netzkomponenten (Open RAN) und
- Nutzung der Mobilfunknetze zur Begegnung sozialer, politischer und gesellschaftlicher Herausforderungen.

Die Vielfalt der verfügbaren Dienste und damit einhergehender neuer Geschäftsmodelle werden weiter erheblich zunehmen. Somit eröffnen die bestehenden und insbesondere die neuen Kommunikationsdienste aber auch vielfältige Möglichkeiten zum Missbrauch dieser Technologien, zum Beispiel in den Phänomenbereichen um Cyberkriminalität, Extremismus oder internationaler Terrorismus beziehungsweise Hass und Hetze im Netz.

Wo stehen wir?

Die Sicherheitsbehörden stehen vor enormen technologischen und methodischen Herausforderungen, um sich an die sich rasant ändernden Gegebenheiten der digitalen Welt anzupassen. Bei der Kommunikation von Straftätern gewinnen zum Beispiel Messengerdienste, die speziell zur Vorbereitung von Straftaten entwickelt werden, sowie gehärtete Mobilfunkgeräte und Chatfunktionen bei Onlinespielen immer mehr an Bedeutung. Die im Jahr 2021 erfolgte umfassende Novellierung des Telekommunikationsgesetzes begegnet diesen Entwicklungen bereits mit gesetzlichen Anpassungen. Jedoch gilt es, fortwährend mit den technologischen Entwicklungen Schritt zu halten. Insofern werden auch nach abgeschlossener Telekommunikationsgesetz-Novelle Regelungsnotwendigkeiten im Telekommunikations- und Telemedienrecht und in den Fachgesetzen geprüft, damit die Sicherheitsbehörden auch in der digitalen Welt ihre Aufgaben wahrnehmen können und gleichzeitig Grundrechte möglichst effektiv schützen. Hierbei muss stets abgewogen werden zwischen den Anforderungen an eine effektive und technisch zeitgemäße Arbeit der Sicherheitsbehörden einerseits und dem Schutz hiervon betroffener Freiheitsrechte andererseits.

Was wollen wir erreichen?

Die gesetzlichen Befugnisse der Sicherheitsbehörden im Telekommunikations- und Telemedienrecht und den Fachgesetzen müssen regelmäßig an die stetigen Veränderungen bei Vernetzung und Kommunikation der Zukunft, insbesondere in den Bereichen mobile Kommunikation, IoT und Automotive IT, angepasst werden, damit keine Lücken in der Gefahrenabwehr und Strafverfolgung entstehen. Die TKÜ als zentrales Aufklärungs-, Ermittlungs- und Fahndungsinstrument der Sicherheitsbehörden des Bundes und der Länder hat eine herausgehobene Bedeutung in allen Phänomenbereichen (speziell in den Bereichen Organisierter Kriminalität und Terrorismus).

Für die Sicherheitsbehörden ist es deshalb von hoher Bedeutung, dieses Instrument auch angesichts der technischen Weiterentwicklung zu erhalten. Durch die Einführung neuer Dienste und Geschäftsmodelle dürfen die Fähigkeiten der Sicherheitsbehörden zur Kriminalitätsbekämpfung und zum Schutz der Bevölkerung vor schweren Straftaten einschließlich des Terrorismus nicht infrage gestellt werden.

Welche Wirkung erwarten wir?

Die Befugnisse der Sicherheitsbehörden in ihren jeweiligen weiteren Fachgesetzen, die mit entsprechenden Erlaubnissen im Telekommunikations- und Telemedienrecht korrespondieren müssen, müssen ihnen gestatten, ihre Aufgaben uneingeschränkt und dem technischen Fortschritt angepasst wahrzunehmen. Dies wird auch bei der Einführung von 6G zu beachten sein. Diese betrifft im Kern die einschlägigen Regelungen des Telekommunikationsgesetzes, Telemediengesetzes, Telekommunikation-Telemedien-Datenschutzgesetzes, der TKÜ-Verordnung sowie die jeweiligen korrespondierenden Gesetze zur Regelung der präventiven und repressiven Eingriffsbefugnisse der Sicherheitsbehörden wie Strafprozessordnung, Bundeskriminalamtgesetz, Zollfahndungsdienstgesetz, Bundesverfassungsschutzgesetz, Gesetz über den Bundesnachrichtendienst und Bundespolizeigesetz.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Es wurde eine Systematik implementiert, die überprüft, ob ausreichende Fähigkeiten zur Wahrnehmung des gesetzlichen Auftrages der Sicherheitsbehörden in der digitalen Welt vorhanden sind.
- Die Erforderlichkeit gesetzlicher Anpassungen wird kontinuierlich geprüft.

8.4 Handlungsfeld 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik

Die zunehmende transnationale Vernetzung lässt auch die digitalisierte Welt stetig weiter zusammenrücken. Die Zusammenarbeit mit unseren internationalen Partnern in EU und NATO sowie mit weiteren Wertepartnern und die Einbindung nationaler Maßnahmen in europäische und internationale Prozesse sind daher für die Gewährleistung eines hohen Niveaus an Cybersicherheit in Deutschland unverzichtbar. Während diese Einbindung in allen Handlungsfeldern mitbedacht werden muss, adressiert das Handlungsfeld 4 diejenigen Ziele, für die sich Deutschland aktiv in die europäische und internationale Cybersicherheitspolitik einbringt.

Eine besondere Rolle spielt dabei das deutsche Engagement im Rahmen der EU mit folgenden übergeordneten Zielen: ein EU-weiter hoher Cybersicherheitsstandard, gemeinsames Agieren mit den EU-Partnern auf der internationalen Bühne sowie ein vertiefter Austausch bei der polizeilichen und justiziellen Zusammenarbeit unter Berücksichtigung bestehender Unionskompetenzen. Die Cybersicherheitsstrategie 2021 fügt sich insoweit in die Europäische Cybersicherheitsstrategie 2020 ein, um die kollektive Abwehrfähigkeit gegen Cyberbedrohungen in Europa gemeinsam zu stärken.

Im Nordatlantischen Bündnis bringt sich Deutschland bei der Weiterentwicklung der Cyberverteidigungspolitik der NATO ein. Maßgeblich sind dabei der Schutz der Netze und Systeme der NATO sowie die Resilienz der IT-Infrastruktur und Kritischen Infrastrukturen der NATO-Mitgliedstaaten in einem sich verändernden Sicherheitsumfeld.

Ebenso verfolgt Deutschland das Ziel, das internationale Regelwerk für Staaten im Cyberraum zu stärken. Die Bundesregierung beteiligt sich an Resolutionen sowie Erklärungen und bringt sich aktiv in internationale Diskussionen, insbesondere in den Vereinten Nationen (VN), ein, um diesen Prozess voranzubringen. Mit Hilfe internationaler Austauschplattformen und vertrauensbildender Maßnahmen, insbesondere im Rahmen der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), will Deutschland ein gegenseitiges Verständnis mit anderen Staaten in Bezug auf Cyberbedrohungen fördern. Durch eine Ausweitung der Unterstützung für den Aufbau von Cyberfähigkeiten in anderen Staaten leistet Deutschland ferner einen Beitrag zur Steigerung der globalen Cybersicherheit.

Gemeinsam mit internationalen Partnern, die unsere Werte teilen, setzt sich Deutschland für ein freies, offenes, sicheres und globales Internet ein. Hierzu wird auf nationaler und internationaler Ebene auch ein regelmäßiger Dialog mit Vertretern aus Zivilgesellschaft, Wissenschaft und Wirtschaft angestrebt.

Mit den folgenden strategischen Zielen wollen wir, die Bundesregierung, diese Aufgaben angehen.

8.4.1 Eine wirksame europäische Cybersicherheitspolitik aktiv gestalten

Warum ist das Ziel relevant?

Die rasant fortschreitende digitale Transformation sowie die zunehmende Vernetzung innerhalb der EU verdeutlichen den Bedarf, bei der Cybersicherheit europäische Lösungen zu finden. Deutschland versteht Cybersicherheit als eine zentrale Gestaltungsaufgabe für die EU (im Rahmen ihrer Kompetenzen) und setzt sich gemeinsam mit den EU-Partnern für eine leistungsfähige Cybersicherheitsarchitektur und einen verbesserten Informationsaustausch im EU-Kreis ein. Erforderlich sind die Fortentwicklung einer gemeinsamen Vision und Strategie im Bereich der Cybersicherheit sowie deren bedarfsbezogene Aktualisierung. Durch Mindeststandards in den Bereichen Prävention, Detektion und Reaktion kann europäische Cybersicherheitspolitik das Cybersicherheitsniveau in der gesamten EU verbessern.

Wo stehen wir?

Wir begreifen Cybersicherheit als Standortvorteil für die europäische Industrie. Sie soll Leitanbieter für sichere IT-Lösungen sein und so die Lebensqualität für die Bürgerinnen und Bürger stärken. Deutschland ist darüber hinaus treibende Kraft in den EU-Gremien im Sinne einer mitgliedstaatenübergreifenden Reaktionsfähigkeit und gesamtheitlichen Positionierung der EU nach außen und fördert ein gemeinsames Auftreten der EU in internationalen Gremien.

Zusammen mit ihren Mitgliedstaaten kann die EU mit der sogenannten „Cyber Diplomacy Toolbox“ in koordinierter Weise auf schädigende Cyberaktivitäten aus dem Ausland reagieren. Im Jahr 2020 verhängte der Rat der Europäischen Union erstmals restriktive Maßnahmen gegen Personen und Einrichtungen aus dem Ausland, die für verschiedene Cyberangriffe gegen EU-Mitgliedstaaten verantwortlich oder daran beteiligt waren.

Außerdem wurde im Jahr 2019 auf EU-Ebene der Cybersecurity Act verabschiedet, der ein neues Mandat für die Europäische Cybersicherheitsagentur ENISA definiert und einen gemeinsamen Zertifizierungsrahmen in der EU einführt.

Seit Anfang 2021 wird eine Überarbeitung der Netzwerk- und Informationssicherheitsrichtlinie im Rat und im Europäischem Parlament verhandelt, die sogenannte NIS-Richtlinie 2.0. Deutschland bringt sich in den Prozess aktiv und gestaltend ein.

Was ist die „Cyber Diplomacy Toolbox“?

Im Juni 2017 nahm der Rat der Europäischen Union die Schlussfolgerungen zum Rahmen für eine gemeinsame diplomatische Reaktion der EU auf schädigende Cyberaktivitäten an. Das Dokument gibt – wie eine Art Werkzeugkasten – der EU und ihren Mitgliedstaaten Instrumente an die Hand, um angemessen und entschlossen auf schädigende Cyberaktivitäten mit einem breiten Spektrum an diplomatischen, politischen und wirtschaftlichen Maßnahmen reagieren zu können. Die Toolbox enthält vorbeugende, kooperative, stabilisierende und restriktive Maßnahmen (Sanktionen) und mögliche Unterstützung der EU für die rechtmäßigen Reaktionen der Mitgliedstaaten.

Die Cyber Diplomacy Toolbox ist abrufbar unter https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

Was wollen wir erreichen?

Deutschland wirkt auf eine aktive Positionierung der EU zusammen mit ihren Mitgliedstaaten in der internationalen Cybersicherheitspolitik sowie die kontinuierliche Weiterentwicklung des cyberaußenpolitischen Instrumentariums der EU hin, um die Handlungsfähigkeit der Union im Angesicht von Bedrohungen im Cyberraum weiter zu verbessern.

Deutschland bringt sich aktiv bei der gemeinsamen Vision und Strategie der EU für Cybersicherheit und europäische Digitale Souveränität ein und entwickelt diese kontinuierlich fort. Hierzu zählen insbesondere die in der EU-Cybersicherheitsstrategie identifizierten drei Handlungsbereiche Resilienz, technologische Souveränität und Führungsrolle, Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion sowie Förderung eines globalen offenen Cyberraums.

Deutschland unterstützt eine verstärkte Kooperation zwischen den EU-Mitgliedstaaten untereinander im Rahmen der rechtlichen Möglichkeiten und macht sich für eine vertiefte Zusammenarbeit auf EU-Ebene stark. Ziel ist es, innerhalb der EU noch stärker voneinander zu lernen und sich in Krisensituationen eng abzustimmen.

Die europäische und internationale operative Zusammenarbeit (wie etwa im Rahmen des EU-CSIRTs-Netzwerkes sowie CyCLO-Netzwerkes) ist als wichtiger Baustein einer wirksamen Cyberabwehr weiterentwickelt. Einzelnen Austauschforen sind jeweils klare Zuständigkeiten zugewiesen und Informations- und Abstimmungswege zwischen den Akteuren stringent gehalten.

Nationale Standards und Best-Practice-Ansätze der Cybersicherheit fließen aktiv in europäische Vorhaben und EU-Regulierungen ein.

Welche Wirkung erwarten wir?

Mit einer gemeinsamen Vision in der EU wird ein notwendiger Orientierungsrahmen geschaffen, der eine Richtung und Orientierung im Bereich Cybersicherheitspolitik vorgibt. Die gemeinsame Vision soll auch dabei helfen, dass alle EU-Mitgliedstaaten vereinbarte Mindeststandards einführen und umsetzen. Somit wird gewährleistet, dass einheitliche, anerkannte und abgestimmte Verfahren eingesetzt werden.

Durch die enge Zusammenarbeit mit der EU beziehungsweise mit den einzelnen Mitgliedstaaten wird der Informationsaustausch auf EU-Ebene verbessert. Die Mitgliedstaaten der EU haben zu allen wichtigen Themen der Cybersicherheitspolitik eine Position und vertreten diese aktiv. Durch den kontinuierlichen Austausch lernen die einzelnen EU-Mitgliedstaaten stärker voneinander. Bei anfallenden Krisensituationen kann somit eine enge Abstimmung erfolgen.

Ein gemeinsames Auftreten der EU-Mitgliedstaaten führt zu einer besseren Wirksamkeit und Stärkung in allen Bereichen der EU, aber auch beim Einbringen europäischer Positionen in internationale Verhandlungen. Botschaften werden durch ein EU-koordiniertes Auftreten verstärkt, der eigene Einfluss auf der Weltbühne gesteigert.

Durch eine gemeinsame Vision, abgestimmte Standards, verbesserten Informationsaustausch, Wissenstransfer, transnationale Vernetzung, klare Rechtsrahmen und größere Resilienz wird erwartet, dass das europäische und deutsche Cybersicherheitsniveau erhöht und vereinheitlicht wird sowie Ressourcen effektiver eingesetzt werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Grundlagen der europäischen Cybersicherheitspolitik werden kontinuierlich und gegebenenfalls anlassbezogen weiterentwickelt.
- Die NIS-Richtlinie wird überarbeitet und diese neue NIS-Richtlinie 2.0 in nationales Recht umgesetzt.
- Die strategischen Initiativen der EU-Cybersicherheitsstrategie 2020 werden gemeinsam mit unseren europäischen Partnern geprüft, konkret ausgestaltet und umgesetzt.
- In Abstimmung mit ihren europäischen Partnern reagiert die Bundesregierung angemessen auf Cybervorfälle[46].
- Die „Cyber Diplomacy Toolbox“ kommt unter Berücksichtigung etablierter Reaktionsmechanismen zur Anwendung und wird kontinuierlich überprüft und gegebenenfalls anlassbezogen weiterentwickelt.

[46] Die Attribuierung von Cyberangriffen bleibt weiterhin eine Kompetenz der Mitgliedstaaten. Darauf aufbauend besteht die Möglichkeit einer koordinierten oder gemeinsamen Attribuierung.

8.4.2 Cybersicherheit und -verteidigung in der NATO mitgestalten

Warum ist das Ziel relevant?

Die NATO ist eine unverzichtbare Grundlage deutscher und euroatlantischer Sicherheit. Die NATO verbindet ihre Mitgliedstaaten in einer gleichermaßen politischen wie militärischen Organisation und bürgt seit über 70 Jahren für deren Souveränität, sicherheitspolitische Stabilität und territoriale Unversehrtheit. Zur Erfüllung ihrer Kernaufgaben ist die NATO auch auf einen ausreichenden Schutz vor Angriffen im und durch den Cyberraum angewiesen. Die Schwerpunkte der NATO in der Dimension Cyber liegen daher auf dem Schutz der NATO-eigenen Netze, der Stärkung der Resilienz der Mitgliedstaaten beim Schutz gegen Cyberbedrohungen sowie der Fähigkeit der Allianz zur Abschreckung und Verteidigung sowie anderer Reaktion auf Cyberbedrohungen.

Wo stehen wir?

Beim NATO-Gipfel 2016 verabschiedeten die NATO-Mitgliedstaaten mit dem „Cyber Defense Pledge“[47] eine politische Selbstverpflichtung zur Steigerung der Resilienz ihrer Netze und Infrastrukturen sowie zur schnellen und effektiven Reaktion auf Cyberangriffe. Zeitgleich wurde der Cyberraum als eine Dimension der Operationsführung anerkannt, in der sich die NATO ebenso wirksam verteidigen können muss wie in der Luft, zu Land und zur See. Beim NATO-Gipfel 2021 wurde eine neue Cyber-Verteidigungspolitik angenommen, die einen überarbeiteten Rahmen für Cyberverteidigung und Resilienzsteigerung in der NATO schafft.

„Cyber Defense Pledge“

Im Juli 2016 bekräftigten die Staats- und Regierungschefs der NATO, im „Cyber Defense Pledge“ die nationalen Cybersicherheitsmaßnahmen zum Schutz von Netzen und Infrastrukturen zu stärken.

Neben einer Stärkung der nationalen Cybersicherheit sieht der Pledge eine Vertiefung der EU-NATO-Kooperation im Bereich Cybersicherheit, eine Verbesserung der Kooperation im Bereich der Cyberverteidigung und einen jährlichen Überprüfungsmechanismus vor.

Was wollen wir erreichen?

Die Cyberverteidigungspolitik der NATO als Eckpfeiler der nationalen und euroatlantischen Sicherheit ist weiterentwickelt und an ein sich veränderndes Sicherheitsumfeld angepasst.

Die Netze und Systeme der NATO sind durch ein hohes Maß an Cybersicherheit und Resilienz gegen Cyberangriffe geschützt.

Die NATO leistet einen wichtigen Beitrag zur Steigerung der Resilienz der NATO-Mitgliedstaaten durch die Umsetzung des „Cyber Defense Pledge“.

Die NATO bietet ein Forum für Austausch und Konsultationen zur Cybersicherheit und zur Reaktion auf bösartiges Verhalten im Cyberraum.

---

[47] Abrufbar unter: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Durch die Weiterentwicklung des Cyberraums als Dimension der Operationsführung – im Rahmen des defensiven Mandats der NATO und im Einklang mit dem Völkerrecht – kann sich die NATO im Cyberraum genauso effektiv verteidigen und Operationen führen wie in den anderen Dimensionen. Hierfür hat Deutschland seine Bereitschaft angezeigt, die NATO in mandatierten Operationen und Missionen mit Cyberoperationen zur Erzielung militärischer Effekte zu unterstützen.

Die EU-NATO-Zusammenarbeit bei der Cyberverteidigung und -resilienz ist weiter gestärkt und es ist auf eine bessere Abstimmung bei der Reaktion auf Cyberbedrohungen hingewirkt, um deren Wirksamkeit zu erhöhen.

Deutschland unterstützt weiterhin die NATO mit nationalem Sachverstand bei der zukunftssicheren Ausgestaltung der Cyberverteidigungspolitik im Rahmen des Mandates der Allianz. Die Balance zwischen bündnisgemeinsamem Handeln und den souveränen Aufgaben der Mitgliedstaaten sowie zwischen den zivilen und militärischen Aspekten von Cybersicherheit wird gewahrt.

Welche Wirkung erwarten wir?

Es wird eine Stärkung der Cybersicherheit der NATO und der NATO-Mitgliedstaaten, eine Verbesserung der Handlungsfähigkeit der NATO bei Operationen des Krisenmanagements und eine Erhöhung der Verteidigungsfähigkeit der NATO erwartet.

Die Aufgaben der nationalen und bündnisgemeinsamen Verteidigung sowie für internationales Krisenmanagement und Stabilisierung können erfüllt werden.

Mit der Umsetzung des NATO „Cyber Defence Pledge“ werden die Cyberabwehr und Cyberverteidigung verstärkt. Im Verbund mit seinen Partnern bleibt Deutschland handlungsfähig.

Durch eine intensive EU-NATO-Zusammenarbeit werden der Informationsaustausch und die Abstimmung von Reaktionen auf schädigendes Verhalten aus dem Ausland verbessert.

Deutschland und die NATO bieten so insgesamt weniger Angriffsfläche für Cyberangriffe.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Grundlagen der NATO-Cyberverteidigungspolitik werden kontinuierlich überprüft und anlassbezogen weiterentwickelt.
- Es sind Verfahren etabliert, mit denen die NATO im Bedarfsfall in angemessenem Umfang mit nationalen Cyberfähigkeiten unterstützt werden kann.
- Die nationale Umsetzung entlang der Ziele des NATO „Cyber Defense Pledge“ wird fortgesetzt und vorangetrieben.
- Die EU-NATO-Kooperation im Bereich der Cybersicherheit und Cyberverteidigungspolitik wird gestärkt.

8.4.3 Völkerrecht und den normativen Rahmen für den Cyberraum stärken und auf verantwortliches Staatenverhalten hinwirken

Warum ist das Ziel relevant?

Cybersicherheit kann nicht einseitig auf nationaler Ebene erreicht werden, sondern muss durch entsprechende Aktivitäten auf internationaler Ebene flankiert werden. Jeder Versuch, den Cyberraum im Alleingang, also ausschließlich auf nationaler Ebene zu regeln, ist angesichts der umfassenden grenzüberschreitenden Interdependenzen nationaler Cybersysteme zum Scheitern verurteilt. Cybersicherheit kann nur durch die enge Zusammenarbeit zwischen Staaten und internationalen Organisationen, Zivilgesellschaft, Wirtschaft und Wissenschaft gewährleistet und gestärkt werden. Für dieses Ziel kommt dem Völkerrecht eine wesentliche Bedeutung zu; dementsprechend bildet die regelbasierte internationale Ordnung auch generell einen Grundpfeiler deutscher Außenpolitik. Daneben können freiwillige Selbstverpflichtungen für verantwortliches Staatenverhalten diesen völkerrechtlichen Rahmen ergänzen und weiter konkretisieren. Deutschland setzt sich daher weltweit dafür ein, das Völkerrecht, dessen Institutionen und auch freiwillige Verpflichtungen im Bereich der Cybersicherheit zu stärken und weiterzuentwickeln. Internationale Normenbildung ist für Vertrauen und Sicherheit im Cyberraum von zentraler Bedeutung.

Wo stehen wir?

Der Großteil der Staatengemeinschaft erkennt an, dass das Völkerrecht im Cyberraum Anwendung findet. In Diskussionen auf Ebene der VN sowie in Expertenkreisen wird weiter konkretisiert, was dies im Einzelnen bedeutet und wie einzelne Normen und Prinzipien des Völkerrechts, etwa jene der VN-Charta, im Cyberraum konkrete Anwendung finden. Weiter diskutiert wird auch, mit welchen freiwilligen Selbstverpflichtungen für verantwortliches Staatenverhalten der normative Rahmen für den Cyberraum weiter ausgebaut werden kann. Gleichzeitig gibt es immer wieder einzelne Staaten, die die Geltung des Völkerrechts ganz oder teilweise durch Erklärungen und Handlungen in Frage stellen.

Im März 2021 hat die Bundesregierung ein Positionspapier[48] veröffentlicht, das einen Beitrag zu den fortdauernden Diskussionen um die konkreten Anwendungsmodalitäten des Völkerrechts im Cyberraum leistet. Mit dem Papier bekräftigt Deutschland die Geltung und Relevanz des Völkerrechts als des zentralen multilateralen Ordnungsrahmens auch für Cyberoperationen und untermauert sein Bekenntnis zu einer völkerrechtsbasierten Cyberaußenpolitik.

Was wollen wir erreichen?

Der völkerrechtliche Rahmen für den Cyberraum und der Acquis rechtlich nicht bindender Normen für verantwortliches Staatenverhalten werden gestärkt. Deutschland wirkt auf ein international gemeinsames Verständnis zur Anwendung von Völkerrecht im Cyberraum und zu verant-

[48] Abrufbar unter: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

wortlichem Staatenverhalten hin. Leitbild der Bundesregierung ist dabei ein freies, offenes, globales und sicheres Internet. Deutschland engagiert sich zu diesen Themen aktiv und stimmt sich zugleich eng mit den EU-Partnern ab. Weiter fördert Deutschland Maßnahmen zur Wahrung internationaler Stabilität im Cyberraum sowie Maßnahmen zum Schutz von Menschenrechten auf nationaler, europäischer und internationaler Ebene.

Welche Wirkung erwarten wir?

Der von den meisten Staaten getragene Konsens, dass das existierende Völkerrecht auch im Cyberraum gilt, wird weiter stabilisiert und ausgebaut. Es wird dafür geworben, dass sich Staaten, die der Geltung des existierenden Völkerrechts beziehungsweise einzelner Völkerrechtsbereiche im Cyberraum bislang zurückhaltend gegenüberstehen, zur umfassenden Geltung des Völkerrechts im Cyberraum bekennen.

Durch eine fortgesetzte Diskussion steigt international das Bewusstsein über den völkerrechtlichen Rahmen sowie über rechtlich nicht bindende Normen für verantwortliches Staatenverhalten im Cyberkontext. Offene Fragen werden identifiziert und auf eine Klärung hingewirkt. Die dadurch verbesserte Rechtssicherheit in Bezug auf die Anwendung des Völkerrechts im Cyberraum ermöglicht es staatlichen, darunter insbesondere auch deutschen, Behörden, unter Beachtung geltender rechtlicher Rahmenbedingungen effektiver auf Cyberbedrohungen zu reagieren.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Bundesregierung beteiligt sich bilateral, multilateral und im Austausch mit der Zivilgesellschaft auf Grundlage des im März 2021 veröffentlichten Positionspapiers an Diskussionen zur Anwendbarkeit des Völkerrechts im Cyberraum sowie zur Implementierung von Selbstverpflichtungen zu verantwortlichem Staatenverhalten.
- Deutschland ist an den relevanten Diskussionen auf VN-Ebene im Kontext der Cybersicherheit beteiligt und vertritt darin aktiv seine Positionen.
- Ein regelmäßiger Dialog auf internationaler und nationaler Ebene mit Gesellschaft, Wissenschaft und Wirtschaft zu Aspekten des normativen Rahmens für den Cyberraum ist etabliert.
- Deutschland beteiligt sich an Resolutionen und Erklärungen zum Thema Menschenrechte online sowie für ein freies, offenes, globales und sicheres Internet.

8.4.4 Vertrauensbildende Maßnahmen fördern

Warum ist das Ziel relevant?

Motivation und Ziele von schadhaftem Cyberverhalten sind häufig ebenso wenig unmittelbar erkennbar wie die Verantwortlichen für einen Cyberangriff. Gleichzeitig ist der Cyberraum international hoch vernetzt. Dadurch entsteht ein erhebliches Potential für Fehlwahrnehmungen und Fehleinschätzungen, die zu Spannungen zwischen Staaten führen können. Vor diesem Hintergrund sind Maßnahmen zur Transparenzsteigerung und Vertrauensbildung wichtig, um Konflikt- und Eskalationsrisiken vorzubeugen.

Wo stehen wir?

Die wichtige Rolle vertrauensbildender Maßnahmen für Sicherheit und Stabilität im Cyberraum wurde 2021 in den VN von allen Staaten anerkannt und bekräftigt. Für Deutschland ist insbesondere die OSZE die relevante regionale Sicherheitsorganisation. Die 57 OSZE-Teilnehmerstaaten haben 2013 und 2016 insgesamt 16 vertrauensbildende Maßnahmen beschlossen, die den Austausch zwischen Staaten fördern, erforderliche Kommunikationskanäle etablieren und Kooperation zu Cybersicherheitsfragen ermöglichen.

Was wollen wir erreichen?

Die Maßnahmen zur internationalen Vertrauensbildung sind gestärkt. Dabei werden bilaterale, regionale und internationale Austauschformate genutzt.

Neben der Weiterentwicklung vertrauensbildender Maßnahmen setzt sich Deutschland für eine Implementierung der vereinbarten Maßnahmen, insbesondere in der OSZE, ein.

Welche Wirkung erwarten wir?

Vertrauensbildenden Maßnahmen kommt sowohl eine präventive als auch eine deeskalierende Rolle zu. Es wird erwartet, dass der regelmäßige Austausch und die internationale Zusammenarbeit bei vertrauensbildenden Maßnahmen das gegenseitige Verständnis zu Bedrohungswahrnehmungen und zu nicht akzeptiertem Verhalten im Cyberraum erhöhen. Im Fall von Konflikten stehen Ansprechpartner zur Verfügung und es kann auf zuvor etablierte, verlässliche Kommunikationskanäle zurückgegriffen werden.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Deutschland informiert in bilateralen, regionalen und internationalen Foren über nationale Bewertungen und Entwicklungen im Cybersicherheitsbereich.
- Deutschland ist an den relevanten Diskussionen zu vertrauensbildenden Maßnahmen im Cybersicherheitsbereich auf internationaler und regionaler Ebene beteiligt und vertritt darin aktiv seine Position, insbesondere zur Anwendbarkeit des Völkerrechts im Cyberraum und zu verantwortlichem Staatenverhalten.

- Deutschland stellt sicher, dass die im Rahmen vertrauensbildender Maßnahmen von Deutschland benannten Ansprechpartnerinnen und -partner und vereinbarten Kommunikationskanäle verlässlich zur Verfügung stehen.

8.4.5 Bilaterale und regionale Unterstützung und Kooperation zum Auf- und Ausbau von Cyberfähigkeiten (Cyber Capacity Building) stärken

Warum ist das Ziel relevant?

Cyber Capacity Building ist angesichts der voranschreitenden digitalen Transformation und der global vernetzten Welt von zentraler Bedeutung. Cyberbedrohungen und -angriffe können bestimmte Staaten und Bevölkerungsgruppen in ihrer wirtschaftlichen, sozialen und politischen Entwicklung stark einschränken oder zurückwerfen. Wo Ressourcen, Infrastruktur und Kapazitäten für Cybersicherheit fehlen, entstehen besondere Bedarfe. Mit dem Auf- und Ausbau von Cyberfähigkeiten in Partnerländern und -regionen können dort Menschenrechte geschützt, Rechtsstaatlichkeit gestärkt und ein nachhaltiges Wirtschaftswachstum gefördert werden. Für die deutsche Entwicklungszusammenarbeit und die Partnerstaaten ist Cyber Capacity Building daher ein wichtiges Instrument, um die Chancen der Digitalisierung zu nutzen und den damit verbundenen Risiken entgegenzuwirken. Insbesondere dort, wo Menschen der Erstzugang zum Cyberraum dank entwicklungspolitischer Maßnahmen ermöglicht wird, müssen die Rahmenbedingungen und Kenntnisse für seine sichere und verlässliche Nutzung unterstützt werden. Hiervon profitiert auch die Cybersicherheit Deutschlands.

Wo stehen wir?

Der Generalsekretär der VN hat im Juni 2020 eine Roadmap zu digitaler Kooperation vorgelegt. Auch in der Cybersicherheitsstrategie der EU wird die Bedeutung von Cyber Capacity Building herausgestellt. Deutschland engagiert sich in bilateralen Projekten sowie darüber hinaus in einzelnen Projekten im multilateralen Rahmen.

Im Rahmen der Entwicklungszusammenarbeit fördert die Bundesregierung bereits eine Vielzahl an digitalen Projekten auf dem afrikanischen Kontinent. Stärkung und Schutz der digitalen Sicherheit ist eine wichtige Zukunftsaufgabe der deutschen Entwicklungszusammenarbeit, da ohne sie das Potenzial des digitalen Wandels nicht (voll) entfaltet werden kann. Cybersicherheit wird daher als Komponente in allen digitalen Projekten der Entwicklungszusammenarbeit mitgedacht.

Was wollen wir erreichen?

Die bilaterale und regionale Zusammenarbeit zum Aufbau von Cyberkapazitäten ist unter Einbeziehung internationaler Partner aus der Politik, Wirtschaft und Zivilgesellschaft weiterentwickelt, um das Potential der Digitalisierung nutzbar zu machen und Vulnerabilitäten zu senken. Cybersicherheit ist in Programmen zur Förderung der Digitalwirtschaft und bei Stabilisierungsmaßnahmen stärker integriert. Das Thema hat international weiter an Bedeutung gewonnen. Die Förderung und Koordinierung nationaler und internationaler Maßnahmen zum Kapazitätsaufbau sind sichergestellt.

Welche Wirkung erwarten wir?

Die bilaterale und multilaterale Zusammenarbeit erhöht die Cybersicherheit in Partnerstaaten nachhaltig. Demokratische und normative Werte und Ideale können weltweit verankert werden. Im Ergebnis vergrößert sich durch Cyber Capacity Building die globale Cybersicherheit insgesamt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Der Cyberkapazitätsaufbau ist in internationalen Gremien als Thema etabliert und wurde in relevanten Policy-Dokumenten verankert.
- Deutschland beteiligt sich an der Durchführung und/oder Unterstützung von Maßnahmen zum Cyberkapazitätsaufbau im nationalen, EU-, NATO- oder internationalen Kontext.

8.4.6 Internationale Zusammenarbeit bei der Strafverfolgung stärken und internationale Cyberkriminalität bekämpfen

Warum ist das Ziel relevant?

Cyberkriminalität ist ein weltweites Phänomen, das nicht an Ländergrenzen haltmacht. Eine effektive Strafverfolgung kann daher oftmals nur im Rahmen international koordinierter Ermittlungsverfahren erfolgen. Durch die Stärkung der internationalen Zusammenarbeit bei der Verfolgung von Cyberkriminalität kann es den zuständigen Stellen gelingen, noch bessere Ermittlungserfolge zu erzielen. Ein höheres Entdeckungsrisiko kann zu einem spürbaren Rückgang von Cyberkriminalität beitragen.

Wo stehen wir?

Die Fallzahlen im Bereich Cyberkriminalität nehmen weiter zu und gehen mit der wachsenden Verlagerung wirtschaftlicher und sozialer Aktivitäten in den digitalen Raum einher. Dies belegen die polizeilichen Fallzahlen sowie zahlreiche Studien und Phänomenanalysen. Darüber hinaus wird ein überdurchschnittlich großes Dunkelfeld vermutet, da nicht alle Angriffe angezeigt werden. Deutschland nimmt bei der Bekämpfung grenzüberschreitender Cyberkriminalität bereits heute eine bedeutende Rolle ein. Diese Rolle gilt es zu sichern und kontinuierlich auszubauen. Als Beispiel für eine erfolgreiche, international koordinierte Maßnahme ist die durch Deutschland initiierte Zerschlagung der Infrastruktur der „Emotet-Schadsoftware“ im Januar 2021 zu nennen.

Bei der internationalen Zusammenarbeit spielt das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität (European Cyber-Crime Centre – EC3) eine multilateral unterstützende Rolle. Das EC3 unterstützt die EU-Mitgliedstaaten bei der Analyse und Auswertung von Cyberkriminalität und koordiniert die grenzübergreifende Strafverfolgung.

Deutschland ist Unterzeichner des Übereinkommens des Europarates über Computerkriminalität („Budapest-Konvention“[49]), das mittlerweile 65 Vertragsstaaten zählt. Der völkerrechtliche Vertrag ist das erste internationale Übereinkommen, das Cyberkriminalität zum Gegenstand hat.

Im April 2018 hat die Europäische Kommission unter der Bezeichnung „E-Evidence“ ein Legislativpaket[50] auf den Weg gebracht, durch das es den EU-Mitgliedstaaten erstmals ermöglicht werden soll, grenzüberschreitend elektronische Beweismittel ohne Rückgriff auf den traditionellen Weg der Rechtshilfe zu erheben. Das Vorhaben wird derzeit auf EU-Ebene verhandelt.

Um die im E-Evidence-Dossier vorgesehenen Instrumente auch im Verhältnis zu den USA einsetzbar zu machen, führt die Europäische Kommission parallel zu den Beratungen auf EU-Ebene Verhandlungen mit dem US-Justizministerium zum Abschluss eines entsprechenden Verwaltungsabkommens.

---

[49] Abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185

[50] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52018PC0225

Was wollen wir erreichen?

Deutschland unterstützt ausländische Strafverfolgungsbehörden mittels der polizeilichen Aufbauhilfe mit dem Ziel, grenzüberschreitender Cyberkriminalität, insbesondere mit ihren Auswirkungen auf Deutschland und Europa, frühzeitig entgegenzuwirken. Die effektive Bekämpfung internationaler Cyberkriminalität ist dadurch gestärkt und Möglichkeiten der grenzüberschreitenden Strafverfolgung sind verbessert.

Deutschland beteiligt sich an international koordinierten Ermittlungsverfahren. Europol und das EC3 übernehmen dabei eine multilateral unterstützende Rolle. Zum deutschen Engagement gehört ebenfalls die Teilnahme an und Ausrichtung von internationalen Erfahrungsaustauschen und Lösungsentwicklungen.

Deutschland wirbt bei Nicht-Vertragsstaaten für die Unterzeichnung der „Budapest-Konvention“ und setzt sich für ihre Umsetzung in nationales Recht ein. Ferner bringt sich Deutschland aktiv bei ihrer Fortentwicklung ein.

Welche Wirkung erwarten wir?

Durch den Austausch strategischer und operativer Informationen und das gemeinsame Arbeiten mit internationalen Partnern verbessert Deutschland seine Fähigkeiten bei der wirksamen Bekämpfung von Cyberkriminalität.

Durch den generalpräventiven Ansatz wird Deutschland ein weniger attraktives Ziel für Cyberangriffe. Mittels international koordinierter Ermittlungsverfahren und Strafverfolgung wird sichergestellt, dass Kritische Infrastrukturen sowie allgemein staatliche Einrichtungen, Unternehmen und Bürgerinnen und Bürger in Deutschland besser geschützt werden.

Die Möglichkeiten der internationalen Strafverfolgung werden durch eine zunehmende Anzahl an Beitrittsstaaten zur „Budapest-Konvention“ sowie einen zeitnahen Abschluss des E-Evidence-Dossiers gestärkt.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Die Anzahl und Wertigkeit international koordinierter Auswerte- und Ermittlungsverfahren ist gestiegen.
- Die Anzahl der polizeilichen Aufbauhilfemaßnahmen Deutschlands für ausländische Sicherheitsbehörden ist gestiegen.
- Die Anzahl der Teilnahmen und Ausrichtungen Deutschlands von Konferenzen und Workshops zu den Themen international koordinierte Strafverfolgung und Cyberkriminalität ist gestiegen.
- Die „Budapest-Konvention“ wird durch weitere Staaten ratifiziert.

8.4.7 Gemeinsam in der EU an innovativen Lösungen für eine effektivere Bekämpfung von Kriminalität arbeiten

Warum ist das Ziel relevant?

Zur wirksamen Strafverfolgung von Kriminalität haben Ermittlerinnen und Ermittler hohen Bedarf an technischen Lösungen, die im operativen Bereich möglichst schnell zur Verfügung stehen müssen. Diese Lösungen basieren oft auf neuen und kombinierten Technologien. Ihre Erarbeitung benötigt einen hohen Einsatz an Fachexpertise und technischer Ausrüstung. Diese Ressourcen sind bei den europäischen Strafverfolgungsbehörden nicht gleichmäßig verteilt, der EU-Raum ist aber gleichmäßig von diesen Straftaten und der Notwendigkeit der technischen Unterstützung bei der Aufklärung und Strafverfolgung betroffen.

Die Erarbeitung innovativer Lösungen für eine effektivere internationale Zusammenarbeit der Strafverfolgungsbehörden liegt im gemeinsamen Interesse der EU-Mitgliedstaaten. Neben der tatsächlichen Erarbeitung von Methoden und Tools sind die Koordinierung von Bedarfen sowie der Expertenaustausch zentrale Punkte in diesem Aufgabenfeld.

Wo stehen wir?

Im Rahmen der deutschen EU-Ratspräsidentschaft ist es gelungen, ein Clearing Board auf europäischer Ebene (EuCB) einzurichten. Das Clearing Board, soll die Kommunikation und ad-hoc-Abstimmung zu kurzfristigen Bedarfen an Tools und Methoden zwischen der Arbeitsebene der Sicherheitsbehörden in den Mitgliedstaaten untereinander, auf EU-Ebene sowie mit Europol herstellen und kanalisieren.

Relevante Partner und Nachbarnetzwerke wie die ZITiS, das European Network of Forensic Science Institutes (ENFSI) und das European Network of Law Enforcement Technology Services (ENLETS) sind eingebunden.

Was wollen wir erreichen?

Das EuCB bietet einen tatsächlichen Mehrwert für Ermittler und ist operativ ausgerichtet. Insbesondere soll es:

- operative Bedarfe und Anforderungen für technische Lösungen unter Verwendung emergenter Technologien direkt von Anwendern (das heißt Strafverfolgungsbehörden) identifizieren und bündeln;
- im Europol Innovation Lab projektbezogene Zusammenarbeit von Expertinnen und Experten zu spezifischen, klar umrissenen operativen Fragestellungen mit technischem Bezug initiieren;
- Arbeitsergebnisse des Europol Innovation Lab und seiner Kerngruppen innerhalb der Strafverfolgungsbehörden verbreiten und als Forum für fachlichen Austausch von Experteninnen und Experten und Ermittlerinnen und Ermittlern der EU-Mitgliedstaaten dienen.

Welche Wirkung erwarten wir?

Durch die Zusammenarbeit bei der gemeinsamen Entwicklung innovativer Lösungen und dem Austausch mit europäischen Partnern verbessert Deutschland seine Fähigkeiten bei der wirksamen Bekämpfung von Kriminalität. Auch die europäischen Partner können von der deutschen Expertise profitieren und damit ihre Fähigkeiten bei der Bekämpfung von Kriminalität verbessern.

Woran lassen wir uns messen?

Die Bundesregierung wird die Erreichung des Ziels anhand folgender Kriterien überprüfen:

- Das EuCB ist eingerichtet.
- Das EuCB hat wertige, europäische Projekte zur wirksameren Bekämpfung von Kriminalität gebündelt, initiiert beziehungsweise koordiniert.
- Zwischen den Mitgliedern des EuCB, des Europol Innovation Labs sowie des EU Innovation Hub findet ein regelmäßiger Erfahrungsaustausch statt.

9 Umsetzung, Berichtswesen, Controlling und Evaluierung der Cybersicherheitsstrategie

Im folgenden Kapitel werden grundlegende Festlegungen zur Ausgestaltung der Leitlinie: „Ziele messbar und transparent ausgestalten“ beschrieben. Sie dienen als Rahmen für die Umsetzung der Strategie, das noch einzurichtende Berichtswesen, das neu einzurichtende Strategische Controlling und die systematische Vorbereitung zukünftiger Evaluierungen.

Im Rahmen der Cybersicherheitsstrategie 2021 wird zwischen zwei Ebenen unterschieden:

- Strategische Ebene: Diese umfasst die strategischen Ziele und die Strategie selbst. Sie beinhaltet die Koordination und Einbindung der Ressorts durch das BMI.
- Operative Ebene: Diese umfasst die Maßnahmen unterhalb der strategischen Ziele und die Umsetzung in den Ressorts. Die Verantwortung obliegt den einzelnen Ressorts.

9.1 Umsetzung

Die zuständigen Ressorts verantworten die Umsetzung der Strategie auf operativer Ebene. Das heißt, sie sind gemäß Ressortprinzip für die Operationalisierung verantwortlich. Hierzu definieren die Ressorts Maßnahmen unterhalb der strategischen Zielebene der Strategie, verfolgen eigenverantwortlich deren Umsetzung und verantworten deren Kosten, Aufwände und Effektivität eigenständig.

Die konkrete Operationalisierung erfolgt durch Ressorts oder durch Geschäftsbereichsbehörden. Für das BMI sind die jeweiligen Ressorts die verantwortlichen Ansprechpartner.

Zur Umsetzung werden durch die Strategie keine verbindlichen Vorgaben gemacht. Im Ergebnis sollen die für das Strategische Controlling (siehe Kapitel 9.3 „Controlling“) notwendigen Informationen bereitgestellt werden. Für eine Vereinheitlichung wird das BMI „Best Practices“ zur Verfügung stellen.

Maßnahmen werden der Strategie nachgelagert erhoben und umgesetzt. Sie werden nach abgeschlossener Erhebung in Form eines fortzuschreibenden Maßnahmenkatalogs der Strategie beigefügt. Die Maßnahmen werden den verantwortlichen Ressorts zugeordnet.

Die Maßnahmenplanung kann in der Laufzeit der Strategie durch die Ressorts angepasst werden, beispielsweise um geänderten Rahmenbedingungen Rechnung zu tragen.

Die Umsetzung der Cybersicherheitsstrategie steht unter dem Vorbehalt der Verfügbarkeit entsprechender, im Haushaltsplan veranschlagter Haushaltsmittel.

9.2 Berichtswesen

Die zuständigen Ressorts übermitteln dem BMI eine Zusammenfassung nebst Bewertung des aktuellen Standes der erreichten Ziele anhand der definierten Indikatoren bis 31. März eines Jahres.

Zusätzlich werden dem BMI Haushaltsmittel- und Personalbedarf sowie Ausgaben und Personalaufwand für die Cybersicherheitsstrategie 2021 mitgeteilt. Im Sinne eines einheitlichen Vorgehens stellt das BMI Berichtsformate (Templates) zur Verfügung.

Das BMI konsolidiert die Einzelberichte der Ressorts in einem Gesamtbericht über den Umsetzungsstand der Cybersicherheitsstrategie 2021. Das BMI legt acht Wochen nach Erhalt der Einzelberichte einen Entwurf des Gesamtberichtes zur Ressortabstimmung vor.

Das BMI bewertet gemeinsam mit den betroffenen Ressorts auf Basis des Gesamtberichtes den Umsetzungsstand der Cybersicherheitsstrategie 2021 und prüft, ob sich aus Änderungen der Bedrohungslage beziehungsweise geänderter Risikobewertung ein Anpassungsbedarf für die Cybersicherheitsstrategie ergibt. Die Umsetzung soll hinsichtlich Effektivität und Zielerreichung überprüft werden. Anpassungsbedürfnissen ist zunächst durch Änderungen in der Umsetzung Rechnung zu tragen. Einzelne Indikatoren können bei Einvernehmen der Ressorts hinzugefügt werden. Ist eine Änderung der Strategie selbst erforderlich, wird eine Evaluierung angestoßen.

9.3 Controlling

Im Rahmen seiner Koordinierungsrolle führt das BMI ein Controlling auf strategischer Ebene ein, im Folgenden mit Strategischem Controlling bezeichnet.

Das Strategische Controlling wird auf Ressort-Ebene etabliert. Das BMI übernimmt die Koordinierungsfunktion und bindet die betroffenen Ressorts ein. Das Strategische Controlling umfasst eine dauerhafte Überprüfung der Zielerreichung und eine Risikobewertung. Um das Strategische Controlling möglichst effizient zu gestalten, sollen geeignete und bereits bestehende Erhebungen, Prüfungen und Kennzahlen zum Stand der Cybersicherheit in Bund und Ländern in die Indikatoren der Cybersicherheitsstrategie 2021 einfließen und gegebenenfalls ergänzt und vereinheitlicht werden.

Das BMI erstellt und stimmt mit den Ressorts ein Controlling-Konzept ab. In Folge wird die Koordinierungsfunktion systematisiert und verstetigt.

9.4 Evaluierungen der Cybersicherheitsstrategie 2021

Mit der Cybersicherheitsstrategie 2021 werden grundlegende Prozesse beschrieben und etabliert, die die Cybersicherheitsstrategie und zukünftige Strategien dauerhaft begleiten. Ziel ist es, die Umsetzung, zukünftige Evaluierungen und zukünftige Fortschreibungen systematisch vorzubereiten.

Evaluierungen sollen spätestens nach vier Jahren erfolgen. Evaluierungen sollen derart vorbereitet werden, dass Ziele mit nachvollziehbaren Indikatoren hinterlegt werden, die eine objektive Zielerreichung überprüfbar machen. Die strategischen Ziele sollen SMART (spezifisch, messbar, aktiv beeinflussbar, realistisch und terminiert) definiert sein. Die Indikatoren können auf geeignete Instrumente (Output) oder die zu erzielende Wirkung (Outcome) auf Staat, Wirtschaft und Gesellschaft abstellen. Grundsätzlich stellt eine Wirksamkeitsmessung die höherwertige Evaluierungsmethode dar. Gleichzeitig gilt es, den Aufwand der Evaluierung in einem angemessenen Verhältnis

zum Aufwand der Maßnahme selbst und deren Optimierungspotenzial durch eine höherwertige Evaluierungsmethode zu halten.

Aktuelle Empfehlungen, wie zum Beispiel das „National Capabilities Assessment Framework“ der ENISA, werden bei einer Evaluierung berücksichtigt.

Zusätzlich erfolgen in Abhängigkeit der laufenden Legislaturperiode anlassbezogene Evaluierungen oder anlassbezogene Sachstandserhebungen, zum Beispiel bei Prüfungen durch den Bundesrechnungshof.

Insbesondere muss die Zielerreichung anhand definierter Indikatoren gemessen werden können. Für Evaluierungen kann es sinnvoll sein, Akteure außerhalb des Staates, zum Beispiel Hersteller, Dienstleister oder Hochschulen, einzubeziehen. Deshalb sollen hierfür Kommunikationsprozesse zwischen den Ressorts abgestimmt und implementiert werden.

Fortschreibungen sollen unter Berücksichtigung der laufenden Legislaturperiode nach vier bis sechs Jahren vorgenommen werden. Ergeben Evaluierungen bereits vorher wesentlichen Änderungsbedarf, kann eine Fortschreibung vorgezogen werden.

Nach Bewertung der Ergebnisse einer Evaluierung kann eine Fortschreibung der Strategie angestrebt werden. Besteht nur geringer Änderungsbedarf, kann das BMI die Fortschreibung bis zur nächsten Evaluierung aussetzen.

10 Glossar

Vorbemerkung: Die nachfolgenden Begriffsbestimmungen gelten für diese Cybersicherheitsstrategie und sollen deren inhaltliche Klarheit und Schlüssigkeit fördern. Die Gültigkeit von in anderen Zusammenhängen im Bereich Cybersicherheit gefundenen Definitionen bleibt hiervon unberührt.

Begriff	**Erläuterung**
Anwenderfreundlichkeit	Anwenderfreundlichkeit als Teil der Nutzererfahrung (englisch User Experience) umschreibt das Erlebnis beziehungsweise die Eindrücke einer Nutzerin oder eines Nutzers in der Interaktion mit einem Produkt oder einer Dienstleistung. Ziel des dahinterstehenden Produktdesigns ist es, die Nutzererwartung in die Interaktion zu erfüllen oder zu übertreffen.
Attribuierung	Attribuierung bezeichnet den Vorgang, den Urheber eines Cyberangriffs zu benennen.
Budapest-Konvention	Die „Budapest-Konvention“ ist ein internationales Übereinkommen des Europarates, welches Cyberkriminalität zum Gegenstand hat. Sie beinhaltet (i) die Kriminalisierung von Verhaltensweisen, die von illegalem Zugriff, Daten- und Systemeingriffen bis hin zu computerbezogenem Betrug und Kinderpornografie reichen; (ii) verfahrensrechtliche Instrumente zur Untersuchung von Cyberkriminalität und zur Sicherung elektronischer Beweismittel im Zusammenhang mit jeglicher Straftat; und (iii) eine effiziente internationale Zusammenarbeit. Das Übereinkommen wird durch ein Zusatzprotokoll ergänzt, das die Kriminalisierung von Handlungen rassistischer und fremdenfeindlicher Natur, die mit Hilfe von Computersystemen begangen werden, zum Gegenstand hat. Die Verhandlungen eines zweiten Zusatzprotokolls dauern derzeit noch an. Ziel des zweiten Zusatzprotokolls ist eine verstärkte internationale Zusammenarbeit bei der Sicherung und betreffend den Zugriff auf elektronische Beweismittel im Strafverfahren durch Behörden in anderen Ländern.
Cloud	Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.
Common Criteria	Mit den Common Criteria for Information Technology Security Evaluation (kurz: Common Criteria) wurde ein internationaler Standard (ISO 15408) für die Bewertung und Zertifizierung der Sicherheit von Computersystemen geschaffen, so dass Komponenten oder Systeme nicht in verschiedenen Ländern mehrfach zertifiziert werden müssen.

Cyberabwehr	Cyberabwehr umfasst alle Maßnahmen mit dem Ziel, den Erfolg von tatsächlichen oder geplanten Cyberangriffen zu verhindern oder abzuschwächen.
Cyberangriff	Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen. Ein besonders schwerer und bedeutender Cyberangriff liegt vor, wenn deren potenzielle Auswirkungen geeignet sind, überregionalen oder in seiner Konsequenz weitreichenden Schaden oder eine Störung des staatlichen Handelns zu verursachen. Indikatoren hierfür können die Betroffenheit Kritischer Infrastrukturen oder anderer systemrelevanter Einrichtungen, die Einbettung in hybride Einflussnahmen oder der sich abzeichnende Bedarf eines gesamtstaatlichen Handelns sein.
Cyberkriminelle	Cyberkriminelle sind Akteure, die auf informationstechnischem Wege oder unter Zuhilfenahme von IT kriminelle Handlungen vornehmen (beispielsweise Erpressung).
Cyberraum	Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.
Cybersicherheit	Cybersicherheit ist die IT-Sicherheit der im Cyberraum auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme.
Cyberterroristen	Cyberterroristen sind ideologisch motivierte Akteure, die Cyberangriffe nutzen, um Ziele zu beschädigen oder zu zerstören, ihre Ideologie zu verbreiten oder ihren Einfluss auszuweiten.
Cyberverteidigung	Cyberverteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und der vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyberraum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyberangriffen und damit dem Schutz eigener Informationen, IT, sowie Waffen- und Wirksysteme dienen. Dazu gehören auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyberabwehr unter verteidigungsrelevanten Aspekten und Situationen.
Datenschutz	Mit Datenschutz wird der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten bezeichnet (nicht zu verwechseln mit Datensicherheit).
Denial of Service	Der englische Fachbegriff Denial of Service (DoS) bedeutet „außer Betrieb setzen“. Technisch wird von einem Angreifer hierbei durch das Absetzen massenhafter

	Anfragen an ein IT-System dieses zur Überlastung gebracht und so deren Verfügbarkeit ganz oder teilweise eingeschränkt.
Distributed Denial of Service	Bei einem „verteilten“ DoS-Angriff (DDoS) werden von Angreifenden anstelle von einzelnen Systemen eine Vielzahl von IT-Systemen zum Angriff genutzt. Die hohe Anzahl der gleichzeitig angreifenden IT-Systeme macht diese Art von Angriffen schwer mitigierbar und damit besonders wirksam.
Desinformation	Desinformation ist gezielt verbreitete falsche oder irreführende Information. Sie ist zu unterscheiden von falscher oder irreführender Information, die ohne Täuschungsabsicht erfolgt.
Detektion	Unter Detektion versteht man das Erkennen von cybersicherheitsrelevanten Ereignissen, wie etwa Indikatoren von Cyberangriffen, in den eigenen IT-Systemen und -Netzen beziehungsweise im Rahmen der Vorfeldaufklärung. Die Angriffserkennung erfolgt beispielsweise durch den Abgleich der verarbeiteten Daten mit Informationen und technischen Mustern, die auf maliziöses Verhalten hindeuten. Moderne Detektion setzt zur Bewältigung hoher Angriffsintensität verstärkt auf technisch gestützte Angriffserkennung, aber auch organisatorische und personelle Maßnahmen spielen weiter eine wichtige Rolle.
Digitale Souveränität	Digitale Souveränität beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.
Digitale Wirtschaft	Die digitale Wirtschaft (Digitalwirtschaft) beschreibt den Umbruch, der heutzutage durch die Technologisierung in der Wirtschaft stattfindet. Neben einer angestrebten effizienteren und effektiveren Ausgestaltung bestehender Geschäftsprozesse ermöglicht Digitalisierung vor allem Innovation bei der Erschließung und Entstehung völlig neuer Geschäftsfelder und -modelle.
E-Government	Der englische Begriff E-Government (Elektronische Verwaltung) meint das Dienstleistungsangebot der öffentlichen Verwaltung im Internet, das es den Kundinnen und Kunden der Verwaltung erlauben soll, Behördengänge so weit wie möglich elektronisch abzuwickeln.
Ende-zu-Ende-Verschlüsselung	Die Ende-zu-Ende-Verschlüsselung ist eine durchgängige Verschlüsselung zwischen Absender und Empfänger.
Exploit	Ein Exploit (englisch to exploit: ausnutzen) ist ein Werkzeug oder eine systematische Möglichkeit (auch Beschreibung), um Schwachstellen und Fehlfunktionen von Hard- oder Software auszunutzen, um sich Zugriff auf die Daten oder Ressourcen zu verschaffen.

EU-Cybersecurity Act	Der europäische Rechtsakt zur Cyber-Sicherheit (Cybersecurity Act, CSA) ist am 27. Juni 2019 in Kraft getreten. Kernelemente der Verordnung sind ein permanentes Mandat für die europäische Cyber-Sicherheitsagentur ENISA sowie die Einführung eines einheitlichen europäischen Zertifizierungsrahmens für IKT-Produkte, -Dienstleistungen und -Prozesse.
European Cybercrime Centre	Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (European Cybercrime Centre, EC3) wurde im Jahr 2013 bei Europol eingerichtet, um die Strafverfolgungsmaßnahmen gegen Cyberkriminalität in der EU zu stärken und so zum Schutz der europäischen Bürgerinnen und Bürger, Unternehmen und Regierungen vor Online-Kriminalität beizutragen.
Europol	Das Europäische Polizeiamt (Europol) ist eine Agentur der EU, die die Strafverfolgungsbehörden der EU-Mitgliedstaaten bei der Bekämpfung organisierter und schwerer internationaler Kriminalität sowie Terrorismus unterstützt.
Hybride Bedrohung	Die Bundesregierung versteht unter hybriden Bedrohungen verschiedene Formen illegitimer Einflussnahme fremder Staaten, die sich insbesondere gegen die Sicherheitsinteressen oder die souveräne politische Willensbildung der Bundesrepublik Deutschland richten.
Informationssicherheit	Informationssicherheit hat den Schutz von Informationen zum Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.
Informationstechnik	Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.
IT-Grundschutz	IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen und Institutionen mit normalem Schutzbedarf hinreichend absichern.
IT-Sicherheit	IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationen und IT durch angemessene Maßnahmen geschützt sind.

Kritische Infrastrukturen	Kritische Infrastrukturen (KRITIS) sind Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
Kryptografie	Kryptografie ist die Wissenschaft der Verschlüsselung von Informationen in „Geheimschriften". Damit soll verhindert werden, dass Dritte Informationen einsehen können, die nicht für sie bestimmt sind.
Nationaler Pakt Cybersicherheit	Mit dem Koalitionsvertrag der aktuellen Legislaturperiode wurde der Nationale Pakt Cybersicherheit ins Leben gerufen. Ziel dieses Paktes ist es, alle gesellschaftlich relevanten Gruppen, Hersteller, Anbieter und Anwendenden sowie die öffentliche Verwaltung in gemeinsamer Verantwortung für digitale Sicherheit in einen Nationalen Pakt einzubinden.
Open RAN	Open RAN ist ein Standardisierungsprojekt, das von privatwirtschaftlichen Initiativen wie der O-RAN Alliance und dem Telecom Infra Project entwickelt und vorangetrieben wird. Beteiligt sind eine Vielzahl von Firmen aus der gesamten Wertschöpfungskette der IKT, wie Netzbetreiber, Komponentenhersteller oder Softwarefirmen, die in den diversen Arbeitsgruppen dieser beiden Organisationen tätig sind. Ziel ist es unter anderem, technische Spezifikationen zu erstellen, die es auch anderen Ausrüstern erlauben beziehungsweise erheblich erleichtern, ihre Produkte einzubringen, um mehr Wettbewerb und offene Schnittstellen zwischen den Komponenten zu ermöglichen. Schwerpunkte liegen beispielsweise in der Entwicklung eines Referenzdesigns für sogenannte White-Box Hardware sowie in der Entwicklung der Software für die einzelnen RAN-Komponenten. Ferner soll mittels Labor- und Feldversuchen sichergestellt werden, dass die Hard- und Softwarekomponenten der verschiedenen Hersteller auch in der Realität interoperabel sind. Als weiteren Schritt strebt die Bundesregierung an, die erstellten Spezifikationen für offene Schnittstellen durch Überführung in eine anerkannte Standardisierungsorganisation (ETSI, European Telecommunications Standards Institute) aufwerten zu lassen.
Patch	Ein Patch ist ein Software-Programm, das unter anderem Programmierfehler oder Schwachstellen in Anwendungs- oder Systemsoftware oder Firmware behebt.
Post Quantenkryptografie	Unter Post-Quanten-Kryptografie versteht man kryptografische Verfahren, von denen angenommen wird, dass sie auch mit Hilfe eines Quantencomputers nicht in realistischer Zeit zu brechen sind. Im Gegensatz zur Quantenkryptografie können diese Verfahren auf klassischer Hardware implementiert werden. Alternativ werden mit der Quantenkryptografie Sicherheitsmechanismen vorgeschlagen, die selbst auf quantenmechanischen Prinzipien basieren. Insgesamt sind Quantenkryptografie und Post-Quanten-Kryptografie auf verschieden Prinzipien beruhende Verfahren, die nicht als Konkurrenten, sondern als gegenseitige Ergänzungen gesehen werden können.

Provider	Provider ist ein Dienstanbieter mit verschiedenen Schwerpunkten, zum Beispiel Netz-Provider, der als Mobilfunkprovider, Internet-Service-Provider oder Carrier die Infrastruktur für den Daten- und Sprachtransport bereitstellt, oder Service Provider, der über die Netzzugangs-Bereitstellung hinausgehende Dienstleistungen erbringt.
Quantencomputing	Quantencomputer sind Rechner, die gezielt quantenmechanische Prinzipien ausnutzen, um damit bestimmte Berechnungen deutlich schneller als mit herkömmlichen Computern ausführen zu können. Diese sogenannte „Quantenüberlegenheit" (englisch „Quantum Supremacy“) konnte mittlerweile für einige spezifische Problemstellungen demonstriert werden.
Quantenkommunikation	Quantenkommunikation, insbesondere die Verteilung kryptografischer Schlüssel mithilfe quantenmechanischer Effekte (englisch Quantum Key Distribution, QKD), ist eine Technologie, die eine sichere Datenübertragung auf Basis physikalischer Prinzipien anstelle mathematischer Vermutungen verspricht. QKD benötigt einen zusätzlichen klassischen Kommunikationskanal.
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „Ransom") wieder freigeben.
Schwachstelle	Eine Schwachstelle (englisch Vulnerability) ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution.
UP KRITIS	Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und staatlichen Stellen wie dem BSI.
Update	Ein Update ist eine neue Version beziehungsweise Ergänzung einer Software oder Firmware, die Programm- oder Funktionsmängel korrigiert oder Programm- oder Funktionsverbesserungen enthält.
Verschlüsselung	Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit einer Zusatzinformation, die „Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.
Völkerrecht	Das Völkerrecht ist das zentrale Element der regelbasierten internationalen Ordnung. Beim Völkerrecht handelt es sich um eine Rechtsordnung, welche durch die Kooperation souveräner, gleichberechtigter Staaten sowie gegebenenfalls anderer Völkerrechtssubjekte auf Grundlage gegenseitiger Übereinstimmung geschaffen wurde und fortgebildet wird. Anders als bei innerstaatlichen Rechtsordnungen gibt es keinen übergeordneten zentralen Gesetzgeber, der allgemeingültige Rechte und Pflichten schafft, an die sich alle Staaten zu halten haben. Vielmehr geschieht dies durch Selbstbindung, da die Akzeptanz und Geltungskraft des Völkerrechts insgesamt auf ein zwischenstaatliches Konsensprinzip zurückgeführt

	werden kann. Dementsprechend sind internationale Übereinkünfte (das so genannte Völkervertragsrecht) oder eine Staatenpraxis, die von einer entsprechenden Rechtsüberzeugung getragen wird (das sogenannte Völkergewohnheitsrecht) sowie die von den meisten Staaten innerstaatlich anerkannten Regeln, die auch auf zwischenstaatliche Ebene übertragbar sind (so genannte allgemeine Rechtsgrundsätze), verbindliche Rechtsquellen der Völkerrechtsordnung.
Zentralstelle	Als Zentralstellen ausgestaltete Bundesbehörden erlauben organisatorische Verbindungen verschiedener Bundes- und Landesbehörden zur dauerhaften gegenseitigen Information, Abstimmung und Unterstützung. Dies ermöglicht, den Aufbau von Doppelstrukturen in Bund und Ländern zu vermeiden.
Zero-Day-Schwachstelle	Eine Zero-Day-Schwachstelle ist eine dem Hersteller unbekannte Schwachstelle in informationstechnischen Systemen.
5G beziehungsweise 6G	5G beziehungsweise 6G bezeichnen Netzstandards der fünften beziehungsweise sechsten Mobilfunkgeneration und sind damit direkte Nachfolger von LTE (4G) und UMTS (3G). Die neuen Standards zielen insbesondere auf höhere Datenraten und geringe Latenz, verbesserte Kapazität und ein intelligentes Netz ab. Für Unternehmen eröffnen sich neue Möglichkeiten bei der Digitalisierung. So können 5G- beziehungsweise 6G-Netze beispielsweise den Datenaustausch innerhalb und zwischen Firmen verbessern oder die Anlagensteuerung mittels Maschine-zu-Maschine-Kommunikation revolutionieren. Für Verbraucherinnen und Verbraucher bedeutet die Technik ein in Zukunft deutlich schnelleres mobiles Netz und eine wachsende Zahl vernetzter Gegenstände im alltäglichen Umfeld.

11 Abkürzungsverzeichnis

Abkürzung	Erläuterung
APT	Advanced Persistent Threat
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BDI	Bundesverband der Deutschen Industrie
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern, für Bau und Heimat
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BPOL	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSOC	Bundes Security Operations Center
CERT	Computer Emergency Response Team
CVD	Coordinated Vulnerability Disclosure
Cyberagentur	Agentur für Innovation in der Cybersicherheit GmbH
Cyber-AZ	Nationales Cyber-Abwehrzentrum
DDoS	Distributed Denial of Service
DsiN	Deutschland sicher im Net
EC3	Europäische Zentrum zur Bekämpfung der Cyberkriminalität (European Cyber-Crime Centre)

eID	Elektronische Identität
ENISA	Agentur der Europäischen Union für Cybersicherheit
EU	Europäische Union
EuCB	Clearing Board auf europäischer Ebene
IoT	Internet of Things
IKT	Informations- und Kommunikationstechnik
ISO	International Organization for Standardization
IT	Informationstechnik
KdoCIR	Kommando Cyber- und Informationsraum
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
KMU	Kleine und mittlere Unternehmen
MAD	Militärischer Abschirmdienst
MIRT	Mobile Incident Response Team
NATO	North Atlantic Treaty Organization oder Nordatlantisches Bündnis
NCSR	Nationaler Cybersicherheitsrat
NIS-Richtlinie	Europäische Richtlinie zur Netzwerk- und Informationssicherheit
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OZG	Onlinezugangsgesetz
QKD	Quantum Key Distribution oder Quantenschlüsselaustausch
PKI	Public-Key-Infrastruktur
SOC	Security Operations Center
TISiM	Transferstelle „IT-Sicherheit im Mittelstand“

TKÜ	Telekommunikationsüberwachung
UP Bund	Umsetzungsplan Bund 2017
VCV	Verwaltungs-CERT-Verbund
VN	Vereinte Nationen
VPN	Virtual Private Network
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Erläuterungen zum Kostenverrechnungsmodell für die Nachnutzung von „EfA“-Antragsdiensten

Mit der Einstellung eines EfA-Dienstes in den FIT-Store müssen den an der Nachnutzung interessierten Ländern die Kosten des EfA-Dienstes bekannt gemacht werden („Preisschild“), um eine Wirtschaftlichkeitsbetrachtung anstellen zu können. Alle EfA-Dienste erstellenden Länder benötigen dafür ein Kostenmodell. Dieses besteht aus der Bestimmung der Kostenarten (vgl. 1.) und der Wahl eines Verteilungsschlüssels (vgl. 2.).

Länder und Kommunen stellen EfA-Leistungen zum Selbstkostenpreis zur Verfügung.
Hierbei sind folgende Grundprinzipien anzuwenden:

a) Selbstkostenpreise mit Vollkostendeckung im Dauerbetrieb,
b) Einfachheit in der Anwendung,
c) hohe Kostentransparenz und
d) Nichtberücksichtigung von Kosten, die - z.B. durch Mittel des Konjunkturpakets - anderweitig finanziert werden („*keine Doppelfinanzierung*“)

1 Erläuterungen zur Definition der Kostenarten und der hierzu jeweils zählenden Einzelkosten

Keine berücksichtigungsfähigen Kosten sind all jene, die für die Herstellung, Bereitstellung, Wartung und Weiterentwicklung von elektronischen Verfahren zur Bearbeitung verwaltungsinterner Vorgänge wie z.B. Fachverfahren anfallen, es sei denn, das Fachverfahren wird als Teil des EfA-Dienstes umgesetzt, beispielsweise, weil bislang noch kein Fachverfahren im Einsatz ist.

Zu den berücksichtigungsfähigen Kosten gem. Ziff. 1 des Beschlussvorschlages zählen ausschließlich

a) die Kosten des Betriebs der technischen Infrastruktur

Aufwände für den Betrieb dedizierter **technischer Infrastruktur**, die ausschließlich dem jeweiligen IT-System der EfA-Online-Dienst-Anwendung zuzurechnen ist. Ausgenommen sind Aufwände, die unter c) fallen, wenn der EfA-Dienst auf Verfahrensinfrastruktur einer Plattform betrieben wird.
Folgende Aufwände für den technischen Betrieb sind berücksichtigungsfähig:

- Gemeinkostenanteil an Rechenzentrumsinfrastruktur (Fläche, Klima, Strom, Notstrom etc.)
- Hardware und virtuelle Infrastruktur (Server, Netzwerk-/Netzwerk-Security-Komponenten, Middleware)
- Betriebssystem sowie betriebssystemnahe Dienste (z.B. Virenscanner, Monitoring-Agent)
- Datenbankmanagement-Systeme
- Web-Server Komponenten
- Registrierung und Pflege der Server und Infrastrukturkomponenten in den zentralen Managementsystemen
- Datenspeicher (Storage) und Einbindung des beauftragten Datenspeichers (physisch und logisch)
- Datensicherung- und Wiederherstellungsmanagement (Backup-/Disaster-Recovery-Management, Backup-Storage)
- Management von Korrektur- und Vorbeugemaßnahmen (CAPA Management)
- Einrichtung und Administration der Verfahrensinfrastruktur (bspw. Einrichtung und Pflege administrativer Konten)
- Bereitstellung versionierter und standardisierter APIs, Release-Support für definierte Zeitspannen für diese Komponenten
- 2nd und 3rd Level-Bearbeitung von Incidents für die vorgenannten Komponenten
- Wartung inkl. Patchmanagement für vorgenannte Komponenten

b) die Kosten der fachlichen Weiterentwicklung der Software und des Change-managements

Die Aufwände für die Veränderung der Software des EfA-Dienstes nach Beendigung der Phase 3 „Rollout in andere Länder“, um Eigenschaften und Funktionen zu verbessern oder Anpassungen an veränderte Rahmenbedingungen vorzunehmen. Ferner das Management dieser Änderungen (Changemanagement, Anforderungsmanagement, Releasemanagement). Folgende Aufwände sind berücksichtigungsfähig:

- den Weiterentwicklungsvorhaben direkt zuzuordnende Personalaufwände
- dem Veränderungsmanagement direkt zuzuordnende Personalaufwände
- den Weiterentwicklungsvorhaben direkt zuzuordnende Sachaufwände wie für die Softwareentwicklung, Testen und Inbetriebnahme erforderliche Hardware (z.B. Entwicklungsrechner,) und Software (Entwicklungsumgebungen, Modellierungs- und Entwicklungswerkzeuge, Testwerkzeuge usw.)
- dem Veränderungsmanagement direkt zuzuordnende Sachaufwände

c) die Nutzungsentgelte und Kosten für die vom EfA-Dienst genutzte Plattform in Höhe des Anteils, der EfA-Zwecken zuzurechnen ist

Anteilige Aufwände für den Betrieb von **Plattformen**, die für den Betrieb des EfA-Dienstes eingesetzt werden (in Abgrenzung zu den Kosten für den Betrieb von dedizierter technischer Infrastruktur nach a)).
Ebenfalls ausgenommen sind Aufwände für Plattform-Basisdienste, die querschnittliche Funktionen für herkömmliche und EfA-Dienste bereitstellen (Nutzerkonten, Nutzerkonto-Postfächer, Payment, Zuständigkeitsfinder etc.).
Ausgenommen sind auch die Softwarewartung und fachliche Weiterentwicklung der Plattform.
Folgende Aufwände von Plattformen sind anteilig berücksichtigungsfähig:

- die für den technischen Betrieb des EfA-Dienstes erforderliche Plattform-Verfahrensinfrastruktur mit den unter a) aufgeführten Arten von berücksichtigungsfähigen Aufwänden
- die für die Inbetriebnahme von Releases des EfA-Dienstes auf der Plattform erforderlichen Aufwände (Hard- und Software für Softwareverteilungssystem)

Der Anteil der auf den EfA-Dienst anzurechnenden Kosten entspricht dem Anteil der *Anzahl der tatsächlichen Nutzungen des EfA-Dienstes* (s. u. Abschnitt 2 Nr. b) an der Gesamtsumme der tatsächlichen Nutzungen aller herkömmlichen und EfA-Online-Dienste auf der miteinander geteilten Plattform.

Zum Beispiel: Auf einer Plattform werden eine Reihe von Online-Diensten (sowohl EfA als auch Nicht-EfA) betrieben. Pro Jahr werden über alle Online-Dienste insgesamt N_{gesamt} = 6,0 Mio. tatsächliche Nutzungen registriert. Die im oben genannten Sinne anrechenbaren Kosten belaufen sich auf $K_{Plattform\ anrechenbar}$ = 700,0 TSD EUR pro Jahr. Auf einen bestimmten EfA-Dienst entfallen $N_{EfA\text{-}OD}$ = 1,2 Mio. tatsächliche Nutzungen pro Jahr. Die in der EfA-Kooperation berücksichtigungsfähigen Kosten für diesen EfA-Dienst betragen

$$\frac{N_{EfA-OD}}{N_{gesamt}} \times K_{Plattform\ anrechenbar} = \frac{1{,}2\ \text{Mio.}}{6{,}0\ \text{Mio.}} \times 700{,}0\ TSD\ EUR = 140{,}0\ TSD\ EUR$$

d) die Kosten, die unmittelbar dem Betrieb des Online-Dienstes (inkl. Wartung und Support) zuzurechnen sind

Aufwände für den Betrieb der **Online-Dienst-Anwendung**. Aufwände für die korrektive und optimierende Wartung des EfA-Dienstes nach Beendigung der Phase 3 „Rollout in andere Länder“, um Fehler zu beheben oder die Wartbarkeit und Performanz zu erhöhen. Aufwände für den Support von Endanwendern sofern Bestandteil der für die Kooperation erbrachten Leistungen. Folgende Aufwände sind berücksichtigungsfähig:

- direkt zuzuordnende Personal- und Sachaufwände von fachlichen Leitstellen[1]

[1]Die Fachliche Leitstelle nimmt die fachliche Verantwortung für den Gesamtbetrieb wahr, insbesondere die Auftraggeberrolle gegenüber IT-Dienstleistern. Zu den Aufgaben in Bezug auf den Betrieb der Online-Dienst-Anwendung gehören

- Entscheidungen über das geeignete Vorgehen bei Betriebsstörungen,
- Verantwortung für die Klärung technischer Fragestellungen und Fehlerbehebungen,

- Registrierung und Pflege der Anwendungen in den zentralen Managementsystemen
- Einrichtung, Konfiguration und Administration des EfA-Dienstes
- Incidentmanagement und Problemmanagement
- 1st Level Bearbeitung von Incidents des EfA-Dienstes, sofern Bestandteil der für die Kooperation erbrachten Leistungen
- 2nd und 3rd Level Bearbeitung von Incidents des EfA-Dienstes
- Applikationsmonitoring
- Performancemanagement inkl. Last- und Performancetests
- für die korrektive und optimierende Softwarewartung erforderlichen Sachkosten wie Hardware (Entwicklungsrechner) und Software (Entwicklungsumgebungen, Modellierungs- und Entwicklungswerkzeuge, Testwerkzeuge usw.)
- für die korrektive und optimierende Softwarewartung Personalaufwände
- Patchmanagement für den Online-Dienst
- Datensicherung- und Wiederherstellungsmanagement des EfA-Dienstes (Backup-/Disaster-Recovery-Management)
- Management von Korrektur- und Vorbeugemaßnahmen (CAPA Management)

e) soweit fachlich relevant: Die der Inanspruchnahme des EfA-Dienstes direkt zuordenbare Kosten (z.B. Druck und Versand von Briefpost)

Aufwände für Leistungen, die für die Kooperationspartner der EfA-Dienst-Allianz in Zusammenhang mit dem EfA-Dienst erbracht werden und nicht unter a)-d) berücksichtigt sind. Berücksichtigungsfähig sind auch Aufwände nachgelagerter Verfahrensschritte wie Druck und Versand von Briefpost im Anschluss an die Nutzung des EfA-Dienstes, unter der Bedingung, dass sie der Inanspruchnahme des EfA-Dienstes direkt zuzuordnen sind.

Den an der Nachnutzung interessierten Ländern stellt jedes umsetzende Land für die von ihm zur Nachnutzung bereitgestellten EfA-Dienste eine transparente Darstellung der Zusammensetzung der Kosten zur Verfügung. Mindestens muss die Aufteilung der Kosten dabei der Differenzierung nach Kostenarten gem. Ziff. 1 entsprechen.

- Abstimmung mit dem Dienstleister zur technischen Umsetzung,
- Finanzplanung,
- Wirtschaftlichkeitsbetrachtungen, Berechnung von Kostenverrechnungsmodellen,
- Vorbereitung von Vertragsschlüssen mit IT-Dienstleistern und Kooperationspartnern,
- Erstellung von Risikoanalysen und Bewertung von Datenschutzfragen,
- Beauftragung und Freigabe neuer Releases,
- Stakeholdermanagement

2 Wahl eines Verteilungsschlüssels bzw. einer Kombination von Verteilungsschlüsseln

Der konkrete Preis der Nachnutzung eines bestimmten EfA-Dienstes ergibt sich aus der Verteilung der nach Ziff. 1 berücksichtigungsfähigen Kosten.

Für diese Kostenverteilung können folgende Verteilungsschlüssel angewendet werden:

a) die Anzahl Einwohner je teilnehmende Organisation

b) die Anzahl der tatsächlichen Nutzungen des EfA-Dienstes

c) die Anzahl der Angehörigen je Zielgruppe je teilnehmende Organisation (z.B. Anzahl Drittstaatsangehörige, Studenten, Kinder, Senioren, Behörden, Unternehmen)

Zusätzlich steht der (angepasste) Königsteiner Schlüssel zur Verfügung.

Soweit sachgerecht kann für einen EfA-Dienst auch eine Kombination von verschiedenen Verteilungsschlüsseln angewendet werden. So kann es etwa sachgerecht sein, Grundkosten (Fixkosten) nach (angepasstem) Königsteiner Schlüssel umzulegen, während variable Kosten nach der Anzahl der tatsächlichen Nutzungen des EfA-Dienstes (b) aufgeteilt werden.

Die Festlegung des Verteilungsschlüssels erfolgt einzeln oder insgesamt für die EfA-Dienste eines bestimmten Umsetzungsvorhaben durch Beschluss der für das Umsetzungsvorhaben zuständige Steuerungsgruppe.

IT-Planungsrat
Digitale Zukunft gestalten

Föderale Architekturrichtlinien

Version 0.99

Stand: 09.09.2021

Änderungshistorie

Version:	Datum:	Geändert von:	Änderungen:	Dokumentenstatus:
0.1	31.03.2021	Lars Santesson (i. A. BMI)	Erste Gliederung	Entwurf
0.2	07.04.2021	Jörg Kremer (FITKO)	Ergänzung Entscheidungsprozess	Entwurf
0.3	13.04.2021	Dr. Günther Diederich (KoSIT), Jörg Kremer (FITKO), Dirk Mehring (HE)	Überarbeitung in gemeinsamer Sitzung	Entwurf
0.4	15.04.2021	Dirk Mehring (HE), Lars Santesson (i. A. BMI)	Ergänzung und Qualitätssicherung nach gemeinsamer Sitzung	Entwurf
0.5	18.04.2021	Jörg Kremer (FITKO)	Ergänzungen, Überarbeitung, Review	Entwurf
0.6	21.04.2021	Dirk Mehring (HE)	Überarbeitung, Review	Entwurf
0.7	18.05.2021	Lars Santesson (i. A. BMI)	Überarbeitung nach Arbeitssitzung am 07.05.2021	Entwurf
0.8	20.05.2021	Dr. Günther Diederich (KoSIT)	Überarbeitung, Review	Entwurf
0.9	27.05.2021	Jörg Kremer (FITKO)	Überarbeitung, Review	Entwurf
0.91	01.06.2021	Lars Santesson (i. A. BMI)	Feedback zu Review-bemerkungen	Entwurf
0.95	02.06.2021	Dr. Günther Diederich (KoSIT), Jörg Kremer (FITKO) Dirk Mehring (HE), Lars Santesson (i. A. BMI)	Überarbeitung in gemeinsamer Arbeitssitzung	Schlussentwurf
0.96	12.06.2021	Lars Santesson (i. A. BMI)	Prüfung Kommentare von Herrn Streicher und Frau Dittmar sowie Anpassung des Dokuments	Schlussentwurf

0.99	09.09.2021	Jörg Kremer (FITKO)	Finales Review, kleinere Anpassungen an Inhalt und Struktur des Dokuments	Freigegeben
1.00	29.10.2021	IT-Planungsrat	Beschluss	Final

Tabelle 1: Änderungsverzeichnis

Inhalt

Abbildungen

1 Management Summary

Die vorliegende Version dieses Dokuments enthält eine erste Fassung übergreifender strategischer Architekturrichtlinien. Diese können ab sofort für ausgewählte Infrastrukturprojekte und -anträge verprobt werden. Es ist beabsichtigt bei der weiteren Fortschreibung die strategischen Architekturrichtlinien um weitere domänenspezifische Architekturrichtlinien zu ergänzen. Diese Architekturrichtlinien leiten sich aus strategischen föderalen Zielen und Gesetzen/Verordnungen ab. Sie sind für eine Vielzahl von föderalen Szenarien einsetzbar, auch wenn sie voraussichtlich zunächst bei der Umsetzung des Onlinezugangsgesetzes und der Registermodernisierung genutzt werden. Die vorliegende Version der Architekturrichtlinien kann ab sofort für ausgewählte Infrastrukturprojekte und -anträge verprobt werden.

Das Architekturboard überprüft anhand der Architekturrichtlinie alle architekturrelevanten Entscheidungsvorlagen hinsichtlich der Einhaltung der beschlossenen Architekturrichtlinien. Hierfür müssen Infrastrukturanträge aus dem Konjunkturpaket entsprechende Beschreibungen umfassen und aufzeigen, wie die Projekte beabsichtigen, die strategischen Architekturrichtlinien zu berücksichtigen. Evtl. Abweichungen zu diesen Architekturrichtlinien sind zu begründen und können maximal als Übergangslösungen vom föderalen Architekturboard akzeptiert werden.

Die Architekturrichtlinien können auf Antrag der Abteilungsleiterrunde/ des IT-Planungsrates angepasst und ergänzt werden. Das Architekturboard kann ebenfalls Änderungen an den Architekturrichtlinien vorschlagen und diese weiterentwickeln. Die Prüfung der Anträge wird innerhalb des Architekturboards erfolgen. Sobald die vorliegende Fassung über die notwendige Reife verfügt, werden die Architekturrichtlinien gemäß dem Dokument „Zusammenwirken im föderalen Architekturboard (Organisation)“ der AL-Runde zur Beschlussfassung vorgelegt.

2 Einleitung

Mit Beschluss der AL-Runde wurde zum 22.02.2021 das föderale IT-Architekturboard[1] als neues Steuerungsgremium des IT-Planungsrats errichtet[2]. Das Architekturboard setzt sich zum Ziel, die föderale Digitalisierungsinfrastruktur ganzheitlich und planvoll weiterzuentwickeln. Die in diesem Dokument aufgeführten Architekturrichtlinien sind ein wesentliches Instrument, diese Weiterentwicklung zu steuern.

Unter Architekturrichtlinien werden Leitlinien verstanden, die bei der Entwicklung und dem Betrieb der föderalen IT-Architektur Orientierung geben.

[1] In diesem Dokument wird der Begriff „Architekturboard“ verwendet.
[2] Siehe https://www.it-planungsrat.de/SharedDocs/Startseitenmeldungen/DE/Startseite_IT_Architekturboard.html

Begriffsbestimmung:

Architekturrichtlinien sind Entscheidungshelfer für den Entwurf und die Entwicklung von IT-Architekturen. Sie orientieren sich an Zielen, rechtlichen Vorgaben und Nutzen für die Verwaltung. Sie bilden die Basis für einheitliche und nachvollziehbare Entscheidungsprozesse.

Architekturrichtlinien helfen Architekturentscheidungen effizient zu treffen und wiederkehrende Grundsatzdiskussionen zu vermeiden. Somit werden Auswahlprozesse beschleunigt, Fehlentscheidungen reduziert und Beschlussergebnisse vereinheitlicht.

Das Architekturboard befasst sich mit der Gestaltung der föderalen IT-Architektur und nicht mit der internen IT-Architektur der Beteiligten (Bund, Länder und Kommunen). Dementsprechend wird sich das Architekturboard mit föderalen Architekturrichtlinien befassen. Das Dokument enthält im Kapitel 3.1 eine Konkretisierung, was unter dem Begriff „föderal relevant“ verstanden wird.

2.1 Zielgruppe

Das vorliegende Dokument richtet sich an folgende Personen:

- Mitglieder des Architekturboards als Entscheidungshilfe bei der Gestaltung der föderalen IT-Architektur und bei der Bewertung von Vorschlägen und Anträgen, die an das Architekturboard gerichtet sind.
- Vom Architekturboard benannte Experten, die bei der Gestaltung der föderalen Architektur unterstützen.
- Antragssteller, die Mittel aus dem Konjunkturpaket beantragen, um die föderale Infrastruktur durch gemeinsame Dienste oder Interoperabilität zu verbessern[3]
- Personen (Bund, Land, Kommunen), die Anträge und Vorschläge unterschiedlicher Art an das Architekturboard richten.
- Projektleiter und Chefarchitekten, die föderale Infrastrukturprojekte verantworten und diese konform zu den IT-Architekturrichtlinien gestalten.
- Produktverantwortliche für Anwendungen des IT-Planungsrats, die beabsichtigen diese Anwendungen auf eine Konformität zu den Architekturrichtlinien zu ertüchtigen.

[3] Siehe Entscheidung IT-Planungsrat 2020/39 – „OZG-Umsetzung (Digitalisierung von Verwaltungsleistungen): Konjunkturpaket“

2.2 Vorgehen

Die vorliegende Version des Dokuments wurde durch eine Arbeitsgruppe des föderalen Architekturboards erarbeitet. Sie basiert auf bestehenden Architekturrichtlinien des Bundes und der Länder, z. B. der Architekturrichtlinie des Bundes und der „Referenzarchitektur zur Umsetzung des OZG“ der ALD (Arbeitsgemeinschaft, Leiter der Datenzentralen).

2.3 Aufbau des Dokuments

Die Architekturrichtlinien liegen mit der aktuellen Fassung in einer ersten Version vor. Es ist beabsichtigt die Architekturrichtlinien laufend, kooperativ und bedarfsorientiert anzupassen, siehe dazu Kapitel 8 .

Die Inhalte des vorliegenden Dokuments sind wie folgt gegliedert:

- Kapitel 3 beschreibt den Umfang (Geltungsbereich) der Architekturrichtlinien aus unterschiedlichen Perspektiven und legt wesentliche Rahmenbedingungen für deren Verwendung fest.
- Kapitel 4 enthält ein Metamodell zur Strukturierung der Architekturrichtlinien, eine Vorlage für deren Dokumentation sowie eine Klassifizierung unterschiedlicher Verbindlichkeitsgrade.
- Kapitel 5 enthält eine Auflistung der übergreifenden, strategischen Architekturrichtlinien
- Kapitel 6 beschreibt, wie die Architekturrichtlinien in der operativen Arbeit im Architekturboard von IT-Architekten und Projektleitern angewendet werden können.
- Kapitel 7 schließlich beschreibt, wie die vorliegenden Architekturrichtlinien fortgeschrieben und wie Anträge für Anpassungen der Architekturrichtlinien gestellt werden können.

3 Umfang und Rahmenbedingungen

Dieses Dokument beschreibt in einer ersten Fassung strategische Architekturrichtlinien. Sie basieren auf der Zielsetzung, alle Verwaltungsleistungen bis 31.12.2022 Bürger:innen und der Wirtschaft auch digital anzubieten.

Das föderale IT-Architekturboard achtet auf die Einhaltung dieser Richtlinien. Die Zusammenarbeit des Architekturboards mit Gremien und föderalen Infrastrukturprojekten zeigt Abbildung 1:

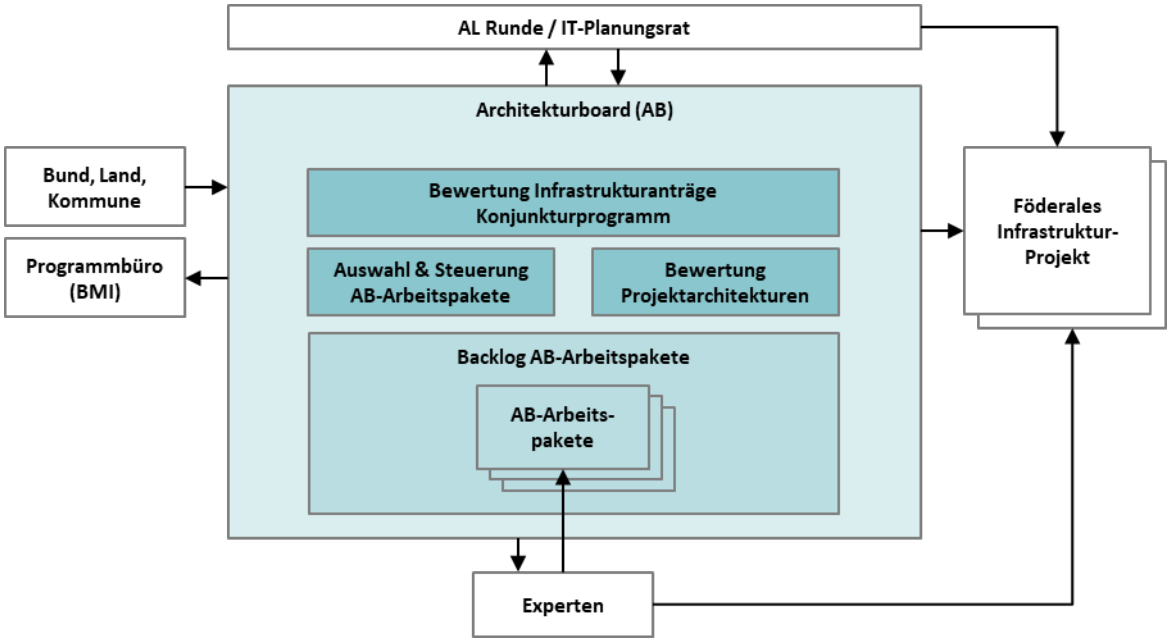


Abbildung 1: Die Organisation des föderalen Architekturboards

Das Architekturboard ist mit umfassenden Kompetenzen versehen. Aufgaben und Organisation des Architekturboards sind ausführlich im Dokument „Zusammenwirken im föderalen Architekturboard (Organisation)“[4] beschrieben.

Der IT-Planungsrat legt für einen definierten Zeitraum Ziele fest. Diese Ziele beziehen sich auf die Digitalisierung der öffentlichen Verwaltung auf föderaler Ebene. Zur Erreichung dieser Ziele wird eine strategische Vorgehensweise festgelegt. Diese Strategie wird von der Runde der Abteilungsleiter verfolgt. Entsprechend den Vorgaben der Strategie entscheidet die Abteilungsleiterrunde über Projekte, Produkte und über neue Standardisierungsvorhaben.

Das Architekturboard richtet die strategischen Architekturrichtlinien an den Ziel- und strategischen Vorgaben aus. Es unterstützt den IT-Planungsrat bzw. die Runde der Abteilungsleiter bei Architekturentscheidungen, gibt Empfehlungen ab, begleitet Projekte und berät das Produktmanagement zu Weiterentwicklungen bestehender Produkte. Das Architekturboard sorgt für die Einhaltung der Architekturrichtlinien und ist insofern als ein strategisches Instrument anzusehen, welches wesentlich zur Erreichung der festgelegten Ziele beiträgt.

Das bei der FITKO eingerichtete Portfolio-Board führt das strategische Controlling aus. Hierzu werden die Daten aus den Bereichen Standards, Projekte und Produkte erhoben, ausgewertet und der Abteilungsleiterrunde/ dem IT-Planungsrat zur Verfügung gestellt.

[4] Siehe Ablage Architekturboard Ordner 01_Organisation/01_Organisationsdokument

3.1 Betrachtete Dimensionen

Der Zielkorridor für die Anwendung der föderalen Architekturrichtlinien ergibt sich aus der additiven Betrachtung der folgenden Dimensionen, siehe Abbildung 2.

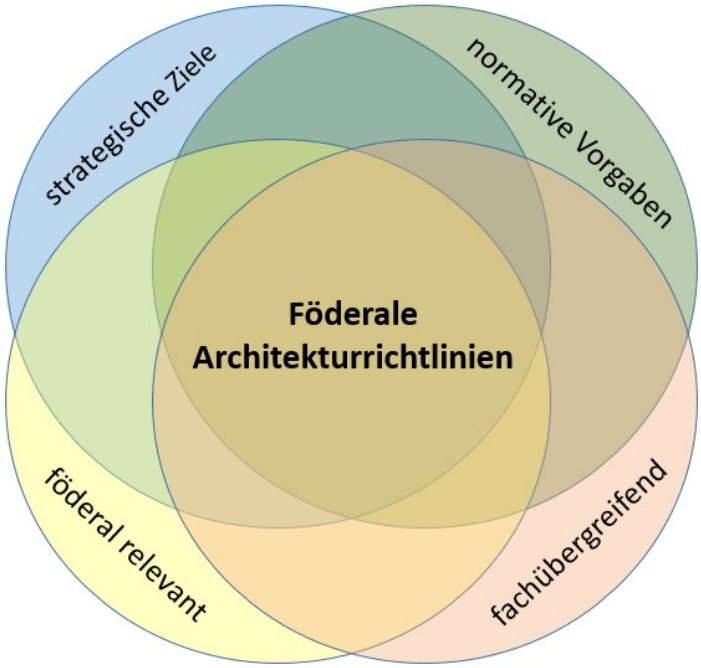


Abbildung 2: Dimensionen mit Einfluss auf die föderalen Architekturrichtlinien

Strategische Ziele:

- S1 Digitale Souveränität: Der IT-Planungsrat hat am 17. März 2021 die „Strategie zur Stärkung der Digitalen Souveränität für die IT der öffentlichen Verwaltung“ beschlossen (Beschluss 2021/09). Digitale Souveränität wird hier definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“. Dabei werden drei strategische Ziele verfolgt:
    - Wechselmöglichkeit: Die Öffentliche Verwaltung hat die Möglichkeit einer freien Wahl bzw. eines flexiblen Wechsels zwischen IT-Lösungen, IT-Komponenten und Anbietern
    - Gestaltungsmöglichkeit: Die Öffentliche Verwaltung hat die Fähigkeit ihre IT (mit-)gestalten zu können und
    - Einfluss auf Anbieter: Die Öffentliche Verwaltung kann ihre Anforderungen und Bedarfe (z. B. hinsichtlich Produkteigenschaften, Verhandlung und Vertragsgestaltung) gegenüber Technologieanbietern artikulieren und durchsetzen.
- S2: Green-IT: Der IT-Planungsrat hat eine Koordinationsgruppe Green-IT eingerichtet, mit dem Ziel eine Green-IT-Strategie zu erarbeiten. Über die KG Green-IT sollen entsprechend

bundesweite Mindestanforderungen an einen nachhaltigen und ressourcenschonenden IT-Einsatz definiert werden (Beschluss IT-PLR 2021/11).

- S3: Digitale Verwaltung: Die Digitalisierung der Verwaltungsleistungen folgt grundsätzlich den im Eckpunktepapier des Konjunkturprogramms formulierten sechs Grundprinzipien „Relevanz“, „Nutzerfreundlichkeit“, „Geschwindigkeit“, „Einer für Alle/Wirtschaftlichkeit“, „Innovation und nachhaltige technische Qualität“, „Offene Standards und Open Source“, siehe Beschluss IT-PLR 2020/39.
- S4: Verwaltung als Plattform: Ziel ist es, eine funktionierende föderale Plattform (Infrastruktur) für die flächendeckende Digitalisierung zu schaffen. Diese Plattform(en) stellen Services zur Verfügung, die Bund und Länder nutzen können. Dabei steht die Verbindung bestehender Systeme und Plattformen in Bund und Ländern im Vordergrund. Dieses Zusammenspiel wird auf der Grundlage von Interoperabilität sichergestellt. Das European Interoperability Framework betrachtet Interoperabilität auf rechtlicher, organisatorischer, semantischer und technischer Ebene. Um eine funktionierende Interoperabilität aller Plattformen zu ermöglichen, müssen alle Ebenen berücksichtigt werden. Auf Grundlage der föderalen Plattform sollen Verwaltungsleistungen (Online-Dienste) nach dem „Einer für Alle Paradigma“ zentral entwickelt und betrieben werden können und zur direkten Nachnutzung bereitgestellt werden. Es soll die Möglichkeit für externe Akteure (Wirtschaft) bieten, Zusatzleistungen anzubieten, ohne dabei die digitale Souveränität Deutschlands zu gefährden.
- S5: Open Data fördern: Daten sind der Rohstoff der Digitalisierung. Open Data liegt die Idee zugrunde, dass die Erhebung dieser Daten durch öffentliche Stellen im Auftrag der Bürger erfolgt und somit der Zugang und die Nutzung diesen frei stehen. Darin ist auch ein Gewinn an Transparenz von staatlichem Handeln zu sehen. Das E-Government Gesetz des Bundes und die E-Government Gesetze bzw. Transparenzgesetze vieler Länder legen fest, dass Behörden Daten zum Abruf über öffentliche Netze bereitzustellen haben, sofern diese nicht geschützt werden müssen. Für die Veröffentlichung der Daten wurde GovData als Anwendung des IT-Planungsrat eingeführt (siehe Beschluss IT-PLR 2014/20 und 2021/18). Verantwortlich für das Portal ist die Geschäfts- und Koordinierungsstelle GovData mit Sitz in Hamburg.

Normative Vorgaben (Gesetze und Verordnungen):

Im Folgenden werden die wesentlichen normativen Vorgaben (Gesetze und Verordnungen) genannt. Aufgeführt werden Vorgaben mit unmittelbarem Bezug zur Digitalisierung der Verwaltung des Bundes und der Länder genannt. Weitere Gesetze ohne unmittelbaren Bezug, wie z. B. die Datengrundschutzverordnung (DGSVO) die für alle IT-Umsetzungsprojekte von Relevanz ist, werden aus Gründen der Übersichtlichkeit nicht aufgeführt.

- R1: Onlinezugangsgesetz (OZG) - Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten.

- R2: Single Digital Gateway Verordnung (SDG) - Das Europäische Parlament und der Europäische Rat haben im Jahr 2018 beschlossen, mit dem Single Digital Gateway (SDG) ein einheitliches digitales Zugangstor zur Verwaltung in der EU zu schaffen.
- R3: Registermodernisierungsgesetz - Das Registermodernisierungsgesetz umfasst die Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze. Mit dem Registermodernisierungsgesetz kann das "Once-Only"-Prinzip verwirklicht werden. Bereits in Registern gespeicherte Angaben und Nachweise müssen dann nicht erneut vorgelegt werden. Zudem wird die Qualität der Registerdaten nachhaltig gesteigert.
- R4: E-Government-Gesetze: Bund und Länder haben E-Government-Gesetze verabschiedet. Die Inhalte der E-Government-Gesetze variieren je Bundesland. Grundsätzliches Ziel ist es, einen einfachen digitalen Zugang zur öffentlichen Verwaltung zu schaffen sowie interne Verwaltungsabläufe zu digitalisieren.
- R5: Verwaltungsverfahrensgesetze: Die Verwaltungsverfahrensgesetze des Bundes und der Länder regeln alles, was die Verwaltung tut und wie sie es tun darf. Es enthält allgemeine Verfahrensgrundsätze, die für alle Behörden gelten. Hierunter fallen z. B. die Tätigkeiten einer Behörde, die erforderlich sind, um einen Verwaltungsakt[5] zu erlassen.

Fachübergreifende Dienste:

Für eine Festlegung des Umfangs der föderalen IT ist es sinnvoll die IT entsprechend des länderübergreifenden Wiederverwendungspotenzials aufzuteilen. Für diesen Zweck wird der Begriff Dienst verwendet. Unter Dienst wird eine logische Einheit verstanden, die einen definierten Umfang an funktionalen Anforderungen erfüllt. Mit Hilfe des Dienstebegriffs kann die föderale IT beschrieben werden, ohne konkret auf die spezifischen IT-Lösungen von Bund und Ländern einzugehen. So gibt es z. B. deutschlandweit mehrere IT-Lösungen, die den Dienst „Nutzerkonto“ realisieren. Die nachfolgende Aufteilung ist angelehnt an das das IT-Rahmenkonzept Bund[6]:

- Fu1: Fachdienste unterstützen eine ressortspezifische Fachlichkeit. Fachdienste können nicht ressortübergreifend wiederverwendet werden.
- Fu2: Querschnittsdienste unterstützen eine ressortübergreifende Fachlichkeit. Beispiele: E-Rechnung und Beschaffungsplattformen. Eine ressortübergreifende Wiederverwendung ist möglich.

[5] Siehe z. B. https://www.bmi.bund.de/SharedDocs/glossareintraege/DE/v/verwaltungsakt.html
[6] Diese Definitionen sind angelehnt an das IT-Rahmenkonzept Bund, siehe https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/rahmenarchitektur_itsteuerung_bund_grundlagen_download.pdf?__blob=publicationFile

- Fu3: Basisdienste bieten Funktionen an, die übergreifend und unabhängig vom spezifischen fachlichen Kontext eingesetzt werden können. Obwohl die Basisdienstfunktionalität nach fachlichen Gesichtspunkten konfiguriert werden kann, wird die Lösung ohne spezifische fachliche (ressortspezifische) Kenntnisse betrieben und weiterentwickelt. Beispiele: Kollaborationswerkzeuge und E-Mail-Server. Das Wiederverwendungspotential ist höher als bei Querschnittsdiensten, da die Basisdienste nicht nur einen spezifischen fachlichen Prozess unterstützen können.
- Fu4: Infrastrukturdienste bieten Funktionen an, die als Fundament für Entwicklung und Betrieb von Anwendungen und den Datenaustausch dienen. Beispiele: Server-, Netzinfrastrukturen, Betriebssysteme und Applikationsserver. Das Wiederverwendungspotenzial ist höher als bei Basisdiensten, da sie eine Unterstützung für beliebig viele Funktionen anbieten. So kann z. B. der gleiche Applikationsserver für Kollaborationswerkzeuge und E-Mail verwendet werden.

Der primäre Fokus liegt auf den Querschnittsdiensten, Basisdiensten und Infrastrukturdiensten, da hier das Wiederverwendungspotenzial am höchsten ist. Fachdienste werden nur teilweise behandelt. Für Fachdienste liegt der Fokus auf der verwendeten Plattform und auf generischen Vorgaben. Die realisierte Fachlichkeit wird nicht betrachtet, wie etwa die Gestaltung einzelner Online-Dienste. Plattformen für Fachdienste sollten ressortübergreifende Querschnittsdienste, Basisdienste und Infrastrukturdienste wiederverwenden und keine konkurrierenden IT-Lösungen einsetzen, wie z. B. ressortspezifische Nutzerkonten.

Föderal relevant:

Der Umfang des föderalen Architekturboard ist auf föderal relevante Dienste begrenzt. Diese sind:

- Fö1: Zentrale Dienste, die länderübergreifend eingesetzt werden. Beispiele: Portalverbund Online-Gateway, einheitliches Unternehmenskonto und NdB-Verbindungsnetz
- Fö2: Interoperabilitätskonzepte und -lösungen zur Verknüpfung von regionalen Diensten. Die Festlegungen zur Interoperabilität können Prozesse, Semantik und Technologien umfassen, vgl. das European Interoperability Framework (EIF)[7]. Beispiele: Standardisierte Schnittstellen zu E-Payment-Diensten und zentrales Verzeichnis mit Information über regionale E-Payment-Dienste.

3.2 Ganzheitliche Architekturbetrachtung

Für die Gestaltung der föderalen IT-Architektur in Deutschland ist eine ganzheitliche Betrachtung notwendig. Die folgenden Architekturdomänen orientieren sich am Architekturframework

[7] European Interoperability Framework, siehe https://ec.europa.eu/isa2/eif_de

TOGAF[8], siehe auch Abbildung 3. Alle Architekturdomänen müssen bei einer Architekturgestaltung berücksichtigt werden:

- Geschäftsarchitektur, d. h. fachliche Prozesse, Akteure und Organisationseinheiten
- Informationssystemarchitektur, d. h. Anwendungen und Daten von Informationssystemen
- Technische Architektur, d. h. die unterstützende technische Infrastruktur

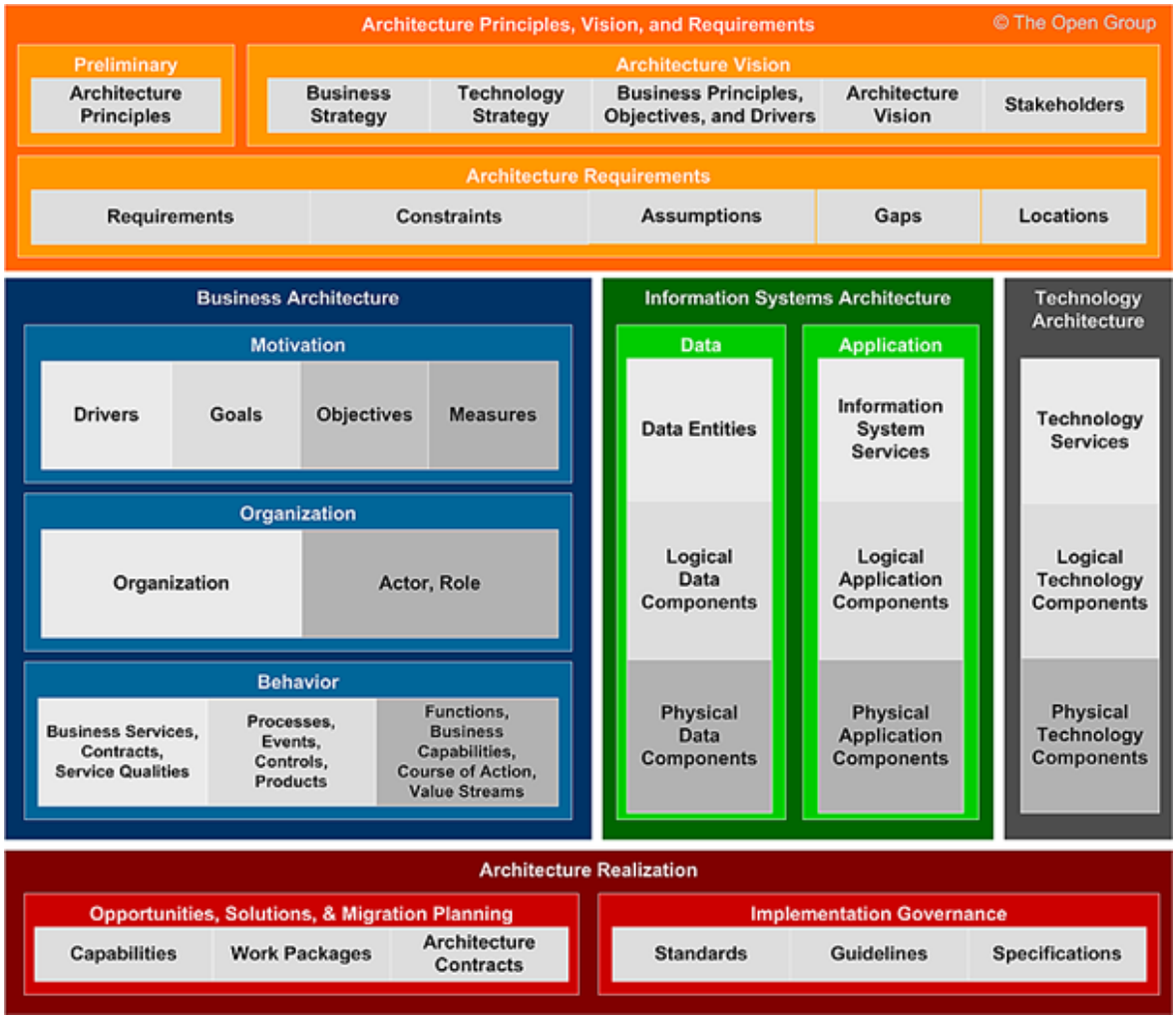


Abbildung 3: Architekturdomänen am Beispiel des TOGAF Content-Framework Metamodell

[8] Siehe https://www.opengroup.org/togaf

3.3 Abgrenzung

Das vorliegende Dokument umfasst eine Beschreibung der Architekturrichtlinien. Deren konkrete Verwendung wird separat im Rahmen des noch zu erstellenden Dokumentes “Dokumentation von Prozessen zur Gestaltung der Architektur” beschrieben.

4 Struktur der Architekturrichtlinien

Die Strukturierung der Architekturrichtlinien orientiert sich an den Architekturrichtlinien Bund und ist in Abbildung 4 aufgeführt.

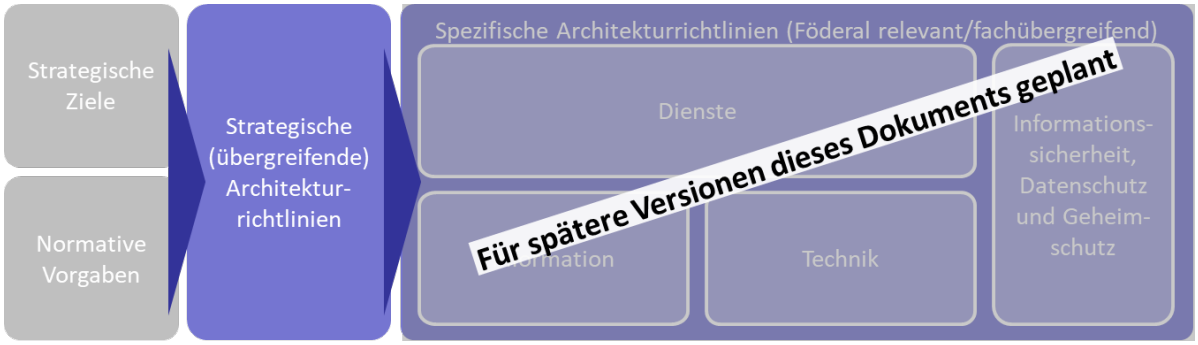


Abbildung 4: Struktur der Architekturrichtlinien

Abgeleitet aus den strategischen Zielen und normativen Vorgaben werden übergreifende strategische Architekturrichtlinien festgehalten. Diese dienen wiederum als Ausgangspunkt für eine Ableitung von spezifischen Architekturrichtlinien, rechts in der Abbildung 4. Diese spezifischen Architekturrichtlinien beziehen sich auf föderal relevante und fachübergreifende Aspekte und umfassen folgende Domänen:

(1) Dienste: Hier werden Architekturrichtlinien festgehalten, die sich auf einzelne Dienste beziehen. Ein Dienst ist eine logische Einheit, die einen definierten Umfang an funktionalen Anforderungen erfüllt. Betrachtet werden Infrastrukturdienste, Basisdienste und Querschnittsdienste und nicht Fachdienste, siehe auch Kapitel 3 .

(2) Information: Hier werden Architekturrichtlinien aufgeführt, die sich auf die Semantik der Informationsobjekte, z. B. im Umfeld Nachrichtenaustausch zwischen Systemen beziehen.

(3) Technik: Architekturrichtlinien umfassen technische Vorgaben, z. B. hinsichtlich der Nutzung spezifischer technischer Standards wie z. B. technische Protokolle.

(4) Informationssicherheit, Datenschutz und Geheimschutz: Wegen der hohen Relevanz für die öffentlichen Verwaltungen werden diese Architekturrichtlinien als eigene Domäne festgehalten.

In der vorliegenden Version werden die **strategischen Architekturrichtlinien** behandelt. Diese sind bei der Konkretisierung der weiteren Domänen zu beachten und einzuhalten. Sie stellen den strategischen Rahmen der Architekturentwicklung dar. Die Einhaltung dieser Vorgaben dient unmittelbar der Erreichung der vereinbarten Ziele zur Digitalisierung der Verwaltung. Die

strategischen Architekturvorgaben können sich aufgrund neuer Zielsetzungen ändern, sind also nicht als unveränderbar anzusehen.

Die spezifischen Architekturrichtlinien werden in der vorliegenden Version dieses Dokuments nicht weiter spezifiziert, sondern sind für weitere Ausbaustufen der Architekturrichtlinie vorgesehen.

Vorlage zur Beschreibung der Architekturrichtlinien

Um die praktische Arbeit mit den Architekturrichtlinien zu erleichtern, wird jede Architektur im Folgenden durch einen eindeutigen Bezeichner, einen aussagekräftigen Titel sowie den Verbindlichkeitsgrad gekennzeichnet. Für eine einheitliche Darstellung und Lesbarkeit der in diesem Dokument beschriebenen Architekturrichtlinien wurde die folgende, aus dem TOGAF Framework adaptierte, Formatvorlage genutzt.

Bezeichner: Titel der Architekturrichtlinie	**Verbindlichkeitsgrad**
Beschreibung	Kurze Beschreibung der Architekturrichtlinie.
Begründung	Darstellung der geschäftlichen und technologischen Vorteile der Architekturrichtlinie.
Abhängigkeiten	Beschreibung der Beziehungen zu anderen Architekturrichtlinien und der Erläuterung, unter welchen Umständen einer konkurrierenden Architekturrichtlinie Priorität eingeräumt wird.
Implikationen	Beschreibung der geschäftlichen und technologischen Auswirkungen der Architekturrichtlinie auf die Behörden und Dienstleister (z. B. in Bezug auf IT-Systeme, Ressourcen, Kosten und Aktivitäten/ Aufgaben).
Beispiele für die Anwendung	Beispiele für die Anwendung der Architekturrichtlinie
Bezug zu Zielen und Gesetzen	Verlinkung zu Zielen und Gesetzen aus der sich die Architekturrichtlinie ableitet.

Zur Verringerung des Interpretationsspielraums und somit besseren Verständlichkeit für die Anwenderin und den Anwender des vorliegenden Dokuments wird zur Beschreibung der Architekturrichtlinie eine einheitliche Beschreibungssemantik verwendet. Diese orientiert sich an

RFC 2119[9] und sieht zur Beschreibung des Verbindlichkeitsgrads einer Architekturvorgabe grundsätzlich vier Abstufungen vor, die in der nachfolgenden Tabelle verdeutlicht werden. Allerdings wird auf die Option „SOLL“ verzichtet, da auch für „MUSS“-Anforderungen begründete Abweichungen und Ausnahmegenehmigungen zulässig sind.

Begriff	**Begriffsdefinition**	**Anmerkungen**
MUSS	„MUSS“ kennzeichnet eine Aussage mit dem Charakter einer verbindlichen Festlegung.	Evtl. Abweichungen von der Vorgabe müssen schriftlich begründet und durch das Architekturboard geprüft und genehmigt werden. Auch die Einhaltung muss dokumentiert und begründet werden.
KANN	„KANN“ kennzeichnet eine Aussage mit dem Charakter einer gestatteten Option.	Diese Architekturrichtlinien werden vom Architekturboard stark empfohlen
DARF NICHT	„DARF NICHT“ kennzeichnet eine Aussage mit dem Charakter eines absoluten Verbots, z. B. veraltete Technologien oder STandards	Die Einhaltung muss dokumentiert und begründet werden.

Die Prüfung der Einhaltung der „MUSS“ und „DARF NICHT“-Kriterien erfolgt durch das Architekturboard auf Grundlage der Dokumentenlage.

[9] Weiterführende Informationen finden Sie unter https://tools.ietf.org/html/rfc2119;

5 Strategische Architekturrichtlinien

Nachstehend werden die strategischen Architekturrichtlinien beschrieben.

SR1: Verwendung von Standards	**MUSS**
Beschreibung	Eine der Hauptaufgaben des IT-Planungsrates ist die Bereitstellung fachübergreifender Standards (vgl. Staatsvertrag). Der IT-Planungsrat hat bereits einige Standards verbindlich verabschiedet. Sie sind daher konsequent anzuwenden. Bedarfe für neue Standards sind über die bei der FITKO geführte Standardisierungsagenda anzumelden. Standards werden auf alle architekturrelevante Ebenen gemäß European Interoperability Framwork (EIF) verwendet. Betrachtet werden die Ebenen Prozesse, Semantik und Technik sofern föderal relevant. Standards dienen u. a. dazu, Daten effizient zwischen und innerhalb der föderalen Ebenen digital auszutauschen. Ergänzend dazu müssen Standards betrachtet werden, die für eine einheitliche Qualität der IT-Architektur sorgen, z. B. zum Thema IT-Sicherheit und Nutzerorientierung. Unter Standards werden auch einheitliche Methoden betrachtet, sofern diese für die Gestaltung der föderalen IT-Architektur relevant sind.
Begründung	Für ein effizientes Zusammenspiel der IT-Lösungen in Deutschland bedarf es einer Standardisierung auf der föderalen Ebene (horizontal Land - Land und vertikal – Bund, Land, Kommune). Diese orientieren sich in erster Linie an Aspekten, die eine föderale Interoperabilität gewährleisten. Standardisierte Methoden vereinfachen den Austausch zwischen Projektbeteiligten und sorgen für eine effiziente Projektdurchführung.
Abhängigkeiten	Eine Verwendung von Standards unterstützt die Architekturrichtlinie (SR9): Gewährleistung der Interoperabilität von IT-Lösungen. Auch kann das Ziel Wiederverwendung (SR2) unterstützt werden, wenn einzelne Anwendungen oder Komponenten als Standards erklärt werden. Bestehende Marktstandards sind zu verwenden (SR3) sofern Herstellerunabhängigkeit gewährleistet ist (SR7). Bestimmte Standards im Umfeld Nutzereinbindung (SR6), IT-

	Sicherheit (SR4) und Open Data (SR14) sind ebenfalls zu berücksichtigen.
Implikationen	Die konsequente Anwendung einheitlicher Standards und Methoden beschleunigt die Digitalisierung signifikant. Dies unterstützt zudem den föderalen Staatsaufbau, wobei alle Länder und der Bund eigene Architekturen betreiben können. Anpassungen sind nur dort vorzunehmen, wo ein föderaler Datenaustausch erforderlich wird. Einheitliche Standards und Methoden führen zu minimalen Aufwänden. Anforderungen föderaler Infrastrukturprojekte können zur Erweiterung bestehender Standards oder der Entwicklung und Einführung neuer Standards führen. Das föderale Architekturboard wird eine Liste der relevanten Standards veröffentlichen und regelmäßig aktualisieren[10].
Beispiele für die Anwendung	Sicherstellung föderal einheitliche Architekturnotation z. B. durch den Einsatz von Archimate
Bezug zu Zielen und Gesetzen	S1: Digitale Souveränität, S3: Digitale Verwaltung, S4 Verwaltung als Plattform, S5: Open Data

SR2: Sicherstellung von Wiederverwendung	**MUSS**
Beschreibung	Bei der Neu- und Weiterentwicklung von IT-Lösungen und -Diensten soll die Wiederverwendung von Komponenten/Modulen anderer IT-Lösungen und Dienste geprüft werden. Geeignete Komponenten/Module sollen als Bestandteil der zu entwickelnden Lösung integriert werden. Bei der Abgrenzung des Funktionsumfangs und der qualitativen Eigenschaften von Komponenten/Modulen soll speziell deren Wiederverwendbarkeit im Kontext mehrerer Lösungen berücksichtigt und gewährleistet werden.

[10] Sobald diese Standards veröffentlicht sind, werden auf diese Standards in diesem Dokument verlinkt.

Begründung	Die systematische Wiederverwendung von (Teil-)Lösungen in einer IT- Landschaft vermeidet unnötige Redundanzen und konzeptionell unterschiedliche Lösungen derselben Problemstellung und trägt damit wesentlich zur Reduzierung des Aufwands und der Kosten für die Entwicklung, die Wartung und den Betrieb von Lösungen bei. Durch spezifische Maßgaben hinsichtlich des Designs von (Teil-)Lösungen kann die Wiederverwendbarkeit optimiert werden (Design for Reuse)
Abhängigkeiten	Die Architekturrichtlinien SR9 (Interoperabilität), SR10 (Lose Kopplung/Modularität) bilden die Grundlage für die Schaffung von wiederverwendbaren IT-Lösungen. Allerdings darf die Schaffung einer wiederverwendbaren IT-Lösung nicht dazu führen, dass die IT-Lösung übermäßig komplex wird, siehe SR12 oder die Herstellerunabhängigkeit gefährdet (S7). Bei der Auswahl einer IT-Lösung, die wiederverwendet werden kann, ist ebenfalls diese IT-Lösung auf Eignung zu prüfen, siehe z. B. SR3 (Bestehende Marktstandards verwenden)
Implikationen	Die Wiederverwendung und Wiederverwendbarkeit von Komponenten/Modulen wird bei Neu- und Weiterentwicklungen durch das föderale Architekturboard geprüft.
Beispiel für die Anwendung	Einsatz „Einer für Alle“, d. h. Schaffung eines Vorgehens und einer Infrastruktur, die eine deutschlandweite Wiederverwendung von Online-Diensten ermöglicht.
Bezug zu Zielen und Gesetzen	S3: Digitale Verwaltung (Grundprinzip: „Einer für Alle/Wirtschaftlichkeit“)

SR3: Bestehende Marktstandards verwenden	**MUSS**
Beschreibung	Bestehende Marktstandards sind zu verwenden.
Begründung	Bestehende Marktstandards haben eine breite Nutzungsbasis, die über die öffentliche Verwaltung in Deutschland hinaus geht. Sie öffnen Möglichkeiten einer schnelleren Umsetzung, bewährter sowie von Nutzern bekannten und somit akzeptierten IT-Lösungen sowie die Umsetzung neuer bisher ohne den Marktstandards nicht umsetzbaren fachlichen Anforderungen.

Abhängigkeiten	Die Marktstandards dürfen das Ziel einer digitalen Souveränität in Deutschland nicht gefährden. Auch ist eine Abwägung mit der Architekturrichtlinie SR2 (Sicherstellung von Wiederverwendung) notwendig.
Implikationen	Bei Einführung neuer IT-Lösungen sollen diese auf bestehende Marktstandards setzen, vgl. Gartner Quadranten. Bestehende IT-Lösungen und Standards sind regelmäßig auf eine Ertüchtigung zu bestehenden Marktstandards auszurichten.
Beispiel für die Anwendung	Maschine zu Maschine Kommunikation auf der Grundlage von RESTful WebServices. Einsatz von IPv6
Bezug zu Zielen und Gesetzen	S3: Digitale Verwaltung (Grundprinzip: „Nutzerfreundlichkeit“ und „Innovation und nachhaltige technische Qualität“)

SR4: Sichere Systemgrundkonfiguration („Security-by-Default“ und “Privacy-by-Default”)	**MUSS**
Beschreibung	Alle relevanten Sicherheitseinstellungen müssen bereits in der Grundkonfiguration des Dienstes aktiviert sein (Security-by-Default und „Privacy-by-Default“)
Begründung	Nur wenn bereits in der Grundkonfiguration eines Dienstes relevante Sicherheitsfestlegungen getroffen werden (z. B. DENY ALL Regeln), kann sichergestellt werden, dass unautorisierte Zugriffe (z. B. bei Nicht-Verfügbarkeit von Sicherheitsdiensten) verhindert werden.
Abhängigkeiten	Abhängigkeiten bestehen grundsätzlich zu allen Architekturrichtlinien.
Implikationen	Die Architekturrichtlinie ist bei Entwurf, Entwicklung, Bereitstellung und Einsatz von Diensten zu berücksichtigen.
Beispiel für die Anwendung	Frühzeitige Einbindung von IT-Sicherheitsexperten, frühzeitige Festlegung der Anforderungen an IT-Sicherheit z. B. auf der Grundlage von IT-Grundschutzvorgaben (BSI). Firewallkonfiguration entsprechend der Vorgabe „Deny all by default“.
Bezug zu Zielen und Gesetzen	R4: E-Government-Gesetze, R5: Verwaltungsverfahrensgesetze

SR5: API-First Ansatz	**MUSS**
Beschreibung	Bei der Entwicklung von neuen IT-Lösungen und Interoperabilitätskonzepten sind diese nach dem API-First Ansatz zu konzipieren. Konkret bedeutet dies, dass zuerst die Schnittstellen spezifiziert, mit allen Beteiligten getestet und abgestimmt werden. Erst danach erfolgt die Umsetzung der konkreten IT-Lösungen.
Begründung	Dies führt zu einer Vermeidung von Missverständnissen bzgl. des Funktionsumfangs und zur frühzeitigen Klärung von offenen fachlichen Fragen. Außerdem kann mit diesem Ansatz die Integration neuer Lösungen in bestehende Architekturen frühzeitig verprobt werden.
Abhängigkeiten	Mit dem API-First Ansatz werden die Wiederverwendbarkeit von IT-Lösungen (SR2) und die Interoperabilität (SR9) gefördert. Ebenfalls ermöglicht es eine lose Kopplung/Modularität (SR10) und reduziert durch wohldefinierte Schnittstellen die Komplexität der Gesamtlösung (SR12). Schnittstellen eignen sich in besonderem Maße zur Standardisierung (SR1).
Implikationen	Die Architekturrichtlinie fordert eine frühzeitige Festlegung der notwendigen Schnittstellen sowie deren Abstimmung mit allen Beteiligten. Die Schnittstellen müssen im fachlichen Kontext entlang eines Prozesses oder ggf. Sequenzdiagramms genau verortet werden können. Die im Kontext der OZG-Umsetzung erarbeitete Landkarte für Kommunikationsbeziehungen (Landkarte Standards und Schnittstellen) ist zu prüfen und zu ergänzen. Während der Umsetzung der Lösungen sollen frühzeitig auf Grundlage der Schnittstellen anzubindende Lösungen für eine Anbindung ertüchtigt werden. Es soll möglich sein, während der Umsetzung Änderungswünsche an die Schnittstellenspezifikation zu formulieren. Geplante und umgesetzte Schnittstellen werden an zentraler Stelle veröffentlicht und im Rahmen eines definierten Releasemanagements versioniert. Alte Versionen werden in einer Übergangszeit unterstützt und dann abgeschaltet. Schnittstellen sind sicher zu gestalten und sollen - sofern sinnvoll - auch für externe Akteure (Wirtschaft etc.) verfügbar gemacht werden. Im OZG-Kontext können z. B. Online-Dienste ergänzend zu Formularen als API-Schnittstellen bereitgestellt werden. Externe Akteure können diese Schnittstellen bei der

	Entwicklung von integrierten Lösungen nutzen, um somit die Verbreitung der Verwaltungsleistungen und Nutzerakzeptanz zu erhöhen.
Beispiel für die Anwendung	Definition von standardisierten Schnittstellen, um länderübergreifende Interoperabilität zu ermöglichen, z. B. im Kontext OZG-Einführung und Registermodernisierung. Einsatz z.B. von OpenAPI für eine konkrete und leicht verständliche Schnittstellenbeschreibung. Frühzeitige Festlegung der Schnittstellen („Schnittstellenverträge“)
Bezug zu Zielen und Gesetzen	S3: Digitale Verwaltung (Grundprinzipen „Geschwindigkeit“, „Nutzerfreundlichkeit“, „Innovation und nachhaltige technische Qualität“), S4: Verwaltung als Plattform

SR6: Sicherstellung der Nutzereinbindung („Usability by Design“)	**MUSS**
Beschreibung	Die Gestaltung und Bedienung von IT-Lösungen muss für jeden Benutzenden einfach, einheitlich und intuitiv sein. Die zugrundeliegenden Bedienungskonzepte müssen den Anwendenden bekannt und transparent sein. Insbesondere müssen muss hierbei der Industriestandard DIN EN ISO 9241 beachtet werden.
Begründung	Wenn die zugrundeliegenden Bedienkonzepte einer IT-Lösung den Benutzerinnen und Benutzern unbekannt sind, wird deren Produktivität negativ beeinträchtigt. Benutzerfreundliche IT-Lösungen erreichen eine höhere Akzeptanz bei den Anwendenden und fördern ein produktiveres Arbeiten, eine höhere Qualität und verringern Fehlbedienungen durch die Anwendenden. Aufwände und Kosten werden gespart, da die Bedienung ähnlich zu anderen, gängigen IT-Lösungen erfolgt, der Schulungsaufwand begrenzt und das Risiko einer unsachgemäßen Bedienung der IT-Lösung gering ist.
Abhängigkeiten	Ausgehend von dieser Architektur-Richtlinie können föderal verbindliche Standards abgeleitet werden (SR1). Die Architekturrichtlinie kann zu einem Konflikt mit der Erfüllung von IT-Sicherheitsanforderungen führen (SR4). Es ist fallbezogen eine gute Abwägung zwischen den Zielen der Nutzerorientierung und IT-Sicherheit zu finden, so dass z. B.

	die konzipierte Lösung sowohl sicher ist als auch von den Nutzern akzeptiert wird.
Implikationen	Eine frühzeitige und laufende Einbindung der zukünftigen Nutzer ist sicherzustellen. Es werden Aspekte wie Sprache, Lokation, Barrierefreiheit, körperliche Einschränkungen der Anwendenden (z. B. Sehschwäche, beschränkte Möglichkeit Tastatur und Maus zu nutzen) und Schulungen beim Design der IT-Lösung berücksichtigt. Standardisierte Design-Aspekte für die grafische Benutzeroberfläche der IT-Lösungen werden angewandt (einheitliches Look-and-Feel) und moderne Technologien berücksichtigt (z. B. Touchscreen). Die Architekturrichtlinie ist nur für IT-Lösungen relevant, die direkt oder indirekt einen Einfluss auf die Interaktion durch den Nutzer hat.
Beispiel für die Anwendung	Der Projektplan umfasst Aktivitäten zur laufenden Einbindung der Nutzer.
Bezug zu Zielen und Gesetzen	S3: Digitale Verwaltung (Grundprinzip: Nutzerfreundlichkeit)

SR7: Sicherstellung der Herstellerunabhängigkeit	**MUSS**
Beschreibung	IT-Lösungen sollen derart gestaltet werden, dass eine realisierte IT-Unterstützung nicht nur durch einen einzigen Hersteller erbracht werden kann bzw. nur ein einziges IT-Produkt in Frage kommt (Verfolgung einer Dual- bzw. Multi-Vendor-Strategie). Um dies zu gewährleisten, sollen IT-Lösungen gem. Europäischem Interoperabilitätsrahmen (COM/2017/0134), soweit sinnvoll und wirtschaftlich, herstellerunabhängige/(quell-)offene Standards und Technologien nutzen. Dies betrifft sowohl die Beschaffung von Standardlösungen als auch die Entwicklung von Individuallösungen und die Implementierung von Schnittstellen zwischen den IT-Lösungen. Insbesondere für Austauschformate gelten folgende Mindestanforderungen an die Offenheit als Leitlinie: - Die Spezifikation wurde vollständig publiziert und die Publikation ist kostenfrei erhältlich. - Die Verwendung der Spezifikation ist für Hersteller und Nutzerinnen und Nutzer der Software-Systeme uneingeschränkt und kostenfrei möglich.

	- Zum Zeitpunkt der Bewertung ist nicht erkennbar, dass die Spezifikation in Zukunft die vorherstehenden Anforderungen nicht mehr erfüllen wird.
Begründung	Herstellerunabhängigkeit ist gerade für die öffentliche Verwaltung ein wesentliches IT-architektonisches Leitprinzip zur Sicherstellung architektonischer Flexibilität, Gestaltungs- und Handlungshoheit und Vermeidung von Abhängigkeitsverhältnissen zu einzelnen Herstellern („Herstellermonopole“). Solche Abhängigkeitsbeziehungen zu einzelnen Anbietern führen z. B. zu - eingeschränkten Mitspracherechten seitens öffentlicher Verwaltung hinsichtlich geschäftlicher Konditionen und technischer Umsetzungen (z. B. der Zwang, Nutzungsdaten an den Hersteller zu übermitteln), - potenziell höheren Kosten bei der Beschaffung von IT-Produkten und der Beeinträchtigung des Prinzips der Wirtschaftlichkeit (z. B. durch das Risiko ungünstiger Lizenzbedingungen für die öffentliche Verwaltung), - Risiken für den IT-Betrieb (z. B. durch das Kündigen des Supports durch den Hersteller), - einer Erhöhung der Systemkomplexität durch Vorhalten funktionsähnlicher IT-Produkte unterschiedlicher Hersteller zur Erbringung einer konkreten Leistung, - einer schlechteren Verhandlungsbasis und Verringerung der Innovationsfähigkeit durch das Entstehen von „Lock-in-Effekten“. IT-Lösungen sollen daher nicht an bestimmte herstellerspezifische Funktionen, Austauschformate oder an spezielle Hardware-Technologien/-Plattformen individueller Hersteller gebunden sein, solange diese nicht explizit notwendig sind. Insbesondere für Fachanwendungen können definierte Ausnahmen hiervon begründet sein. Falls die öffentliche Verwaltung nicht in der Lage wäre, kurz- bzw. mittelfristig auf ein anderes IT-Produkt (ggf. auch das eines anderen Herstellers) auszuweichen, könnte dies in letzter Konsequenz die effiziente Erbringung hoheitlicher Aufgaben beeinträchtigen. Um

	auch in Zukunft selbstbestimmt und selbständig sowie flexibel auf Herausforderungen des digitalen Wandels reagieren zu können, ist es auch im Sinne der digitalen Souveränität der deutschen Verwaltung eine langfristige Abhängigkeit von einzelnen Herstellern zu vermeiden.
Abhängigkeiten	Diese Vorgabe steht in direktem Zusammenhang mit der Architekturrichtlinien SR1 (Standards), SR8 (Open Source) und SR9 (Interoperabilität). Die vorgenannten Vorgaben begünstigen die Anbindung und Interoperabilität verschiedener IT-Lösungen und fördern somit eine Herstellerunabhängigkeit i. S. der Vermeidung von Abhängigkeiten zu einzelnen Herstellern sowie Sicherstellung der Flexibilität i. d. S., dass Hersteller und deren IT-Produkte bedarfsbezogen getauscht werden können.
Implikationen	Die Sicherstellung der Herstellerunabhängigkeit erfordert eine Verankerung in strategische, prozessuale und technische Strukturen der öffentlichen Verwaltung. Auf strategischer Ebene sind klare Leitlinien zu entwickeln, was unter Herstellerunabhängigkeit zu verstehen ist. Hier ist insbesondere auch festzulegen, wie mit einzelnen Ausnahmen (i. S. einer „bewussten Herstellerabhängigkeit“) umzugehen ist. Auf technischer Ebene erfordert die Herstellerunabhängigkeit klare Leitlinien hinsichtlich zu nutzender Standards für die Entwicklung und den Einsatz von IT-Lösungen. Diese Standards sind übergreifend festzulegen und in den Produktkatalogen der IT-Dienstleister zu detaillieren. Die Gewährleistung der Herstellerunabhängigkeit kann einen hohen Implementierungsaufwand – und damit die Entstehung von Mehrkosten – durch den Verzicht von einzelnen herstellerabhängigen Funktionen nach sich ziehen. Darüber hinaus können weitere Risiken durch die Nutzung von Schnittstellen zwischen verschiedenen Komponenten entstehen. Zudem ist nicht auszuschließen, dass durch eine bewusste Fokussierung auf einzelne Hersteller, i. S. von spezifischen Anwendungsfällen (z. B. hinsichtlich der strategischen Mitgestaltungsmöglichkeit technischer Weiterentwicklungen von IT-Lösungen), eine positive Wirkung erzielt werden kann.
Beispiel für die Anwendung	Eine IT-Lösung eines Herstellers hat durch den Einsatz von offenen Standards und Open Source-Werkzeugen eine breite

	Entwicklerbasis die über den Hersteller hinausgehen. Die Lösung ist grundsätzlich auf alternative Produkte portierbar. Vermeidung von Hersteller-Lösungen mit monolithischen Software-Architekturen zur einfachen Austauschbarkeit einzelner Komponenten (Frontend, Persistenz, aber auch horizontal Module der Anwendung.
Bezug zu Zielen und Gesetzen	S1: Digitale Souveränität, S3: Digitale Verwaltung – Grundprinzip

SR8: Einsatz von Open Source	**MUSS**
Beschreibung	Der Quellcode aus der Realisierung digitaler Angebote der Verwaltung (Eigenentwicklung) ist als Open Source, d. h. in nachnutzbarer Form zur Verfügung zu stellen. Open Source Lösungen sind Nicht-Open Source Lösungen vorzuziehen, sofern geeignet und wirtschaftlich.
Begründung	Der Einsatz von Open Source unterstützt die Wiederverwendbarkeit und Herstellerunabhängigkeit. Etablierte Open Source Lösungen werden gemeinsam (durch eine breite Nutzerbasis) weiterentwickelt. Es ist möglich Einfluss auf Open Source Lösungen zu nehmen. Durch die Bereitstellung der eigenen Lösungen als Open Source wird die Wiederverwendung gefördert.
Abhängigkeiten	Der Einsatz von Open Source fördert eine Wiederverwendung (SR2) und stärkt die Herstellerunabhängigkeit sowie die digitale Souveränität (SR7), siehe auch oben.
Implikationen	Bei der Auswahl der Architektur neuer IT-Lösungen sind Open Source Produkte einzusetzen. Darüber hinaus muss die Eigenentwicklung als Open Source bereitgestellt werden.
Beispiel für die Anwendung	Eigenentwicklungen und deren Abhängige Komponenten verwenden Open Source-Infrastrukturen statt proprietären Infrastrukturen (z. B. Applikationsserver und Datenbanken) Bereitstellung des Quellcodes und der Betriebs- und Installationshandbüchern in öffentlichen Repositories
Bezug zu Zielen und Gesetzen	S1: Digitale Souveränität, S3: Digitale Verwaltung – Grundprinzip „Open Source“

SR9: Gewährleistung der Interoperabilität von IT-Lösungen	**MUSS**
Beschreibung	Bei der Neu- und Weiterentwicklung von IT-Lösungen sollen Interoperabilitätsstandards angewendet werden. Dies umfasst neben Anwendungen insbesondere auch Schnittstellen, Daten, Protokolle und Netze. Hierfür sollen u. a. geeignete Austauschformate (z. B. XML, XÖV-Standards) und relevante semantische Standards angewendet werden. Für IT-Lösungen, die europaweit eingesetzt werden können, muss weiterhin das European Interoperability Framework (EIF) berücksichtigt werden.
Begründung	Ein maßgeblicher Faktor bei der Neu- und Weiterentwicklung sowie der Beschaffung von IT-Lösungen ist die Interoperabilität. Interoperabilität erleichtert den Datenaustausch zwischen den IT-Lösungen, ermöglicht eine einfache Integration unterschiedlicher Anwendungen und Technologien über Daten und Schnittstellen. Interoperabilität hilft dabei, die grenz- und sektorübergreifende Interaktion zwischen europäischen Verwaltungen zu erleichtern und zu fördern. Ähnliches gilt für die Zusammenarbeit mit anderen Bundesländern. Neben den bekannten Vorteilen der Nutzung von Standards (u. a. Austauschbarkeit, Flexibilität, erhöhte Kompatibilität) ermöglicht die Nutzung von Interoperabilitätsstandards auch die Zusicherung mehrerer Hersteller hinsichtlich Produktunterstützung und fördert das Zusammenspiel und die Integration zu anderen Anwendungen und Technologien. Weitere Vorteile, die durch Einhaltung dieser Vorgabe entstehen, sind die Vermeidung von Medienbrüchen und die Ermöglichung von „Best-of-Breed“-Architekturen im Gegensatz zu den Lock-in-Effekt begünstigenden, monolithischen Architekturen.
Abhängigkeiten	Die Architekturvorgabe ergänzt und erweitert die Architekturrichtlinie SR4 (Standards).
Implikationen	Die Bereitstellung von Anwendungen durch unterschiedliche IT-Dienstleister und in unterschiedlichen Sicherheitsdomänen erfordert zur Sicherstellung der Interoperabilität erweiterte Regelungen zur Harmonisierung und Standardisierung der IT-Lösungsbereitstellung. Diese Regelungen sind auf rechtlicher, organisatorischer, semantischer und technischer Ebene zwischen den Ländern abzustimmen und umzusetzen, sodass

	ein einheitlicher und nahtloser Zugang zu den Diensten in unterschiedlichen Sicherheitsdomänen der Länder gewährleistet ist und Dienste in unterschiedlichen Sicherheitsdomänen interoperabel erbracht werden können. Die Regelungen sollen insbesondere auch einen Wechsel des Dienstleisters durch die Länder technisch ermöglichen.
Beispiel für die Anwendung	Erarbeitung einer föderalen Interoperabilitätsschicht für die Umsetzung des Onlinezugangsgesetzes, die einen Datenaustausch zwischen den Digitalisierungsplattformen der Länder ermöglicht. Die Interoperabilitätsplattform sorgt z. B. dafür, dass Nutzerkonten der Länder interoperabel gestaltet werden können und dass unterschiedliche Bezahldienste der Länder mit Hilfe von standardisierten Schnittstellen durch zentral betriebene Einer für Alle Online-Dienste standardisiert angesprochen werden können. Sie enthält weiterhin zentrale Verzeichnisse z. B. für die Verwaltung von Verwaltungsleistungen und Links zu Online-Dienste aller Länder unter Beibehaltung der regionalen Redaktionssysteme und Zuständigkeitsfinder (Online-Gateway)
Bezug zu Zielen und Gesetzen	S1: Digitale Souveränität, S3: Digitale Verwaltung – Grundprinzip „Einer für Alle/Wirtschaftlichkeit“, S4: Verwaltung als Plattform

SR10: Sicherstellung von loser Kopplung/Modularität	**MUSS**
Beschreibung	Die föderale IT-Architektur muss nach dem Baukastenprinzip modular aufgebaut werden. Jeder Baustein soll eigenständig nutzbar sein und entsprechend unabhängig weiterentwickelt, aktualisiert und betrieben werden können. Der funktionale Umfang eines Bausteins soll sich hierbei an etablierten Referenzmodellen und -architekturen sowie sinnvollen Kriterien für den jeweiligen Zuschnitt (z. B. der Abdeckung fachlich abgegrenzter Funktionen, Wirtschaftlichkeit, Wiederverwendbarkeit) orientieren.
Begründung	Das Ergebnis nicht-modular aufgebauter Anwendungen und Dienste sind schwer anpassbare und inflexible Lösungen, mit denen hohe Kosten und Aufwände einhergehen. Eine lose Kopplung ermöglicht es, Änderungen an einzelnen Komponenten eines Systems einfacher durchzuführen und vereinfacht auch die Wartbarkeit der Komponenten, da diese

	unabhängig von anderen Komponenten durchgeführt werden kann (ausgenommen Schnittstellen). Weiterhin ist die Modularisierung eine wesentliche Voraussetzung für die Wiederverwendbarkeit/Nachnutzung und ermöglicht ein strukturiertes Testvorgehen bei der Weiterentwicklung/Wartung. Außerdem sind modularisierte Anwendungen und Dienste aufgrund der klaren Abgrenzungen der Teilkomponenten einfacher zu verwalten. Funktional sinnvoll und schlank geschnittene Module, die eine eindeutige Verantwortlichkeit wahrnehmen, beugen unnötiger Komplexität und mangelnder Flexibilität vor. Die lose Kopplung kann des Weiteren auch die Stabilität des Gesamtsystems begünstigen, da der Ausfall von losen gekoppelten Modulen ggf. nur einzelne Funktionalitäten der IT-Lösung beeinflussen. Auch die Herstellerunabhängigkeit (SR7) wird durch die Anwendung begünstigt.
Abhängigkeiten	Diese Vorgabe steht in engem Zusammenhang mit den Architekturrichtlinien Wiederverwendung (SR2) und Reduzierung der Komplexität auf ein notwendiges Maß (SR12). Des Weiteren bildet sie eine Grundlage für Interoperabilität (SR9), da sie aktiv die Wiederverwendung von IT-Lösungen bzw. ausgewählten Teilbereichen adressiert.
Implikationen	Die Vorgabe impliziert eine Abkehr von rein monolithischen IT-Lösungen zugunsten flexibler, modularer IT-Lösungen. Die Richtlinie ist für den Funktionsumfang der föderalen IT-Lösungen relevant (unabhängig von der internen IT-Architektur). Dabei geht es darum IT-Lösungen mit einem zu umfassenden Funktionsumfang zu vermeiden. Sie ist auch für die Gestaltung der internen IT-Architektur einzelner IT-Lösungen relevant. Dieses Kriterium verfolgt den Ansatz, Anforderungen an die Architektur in Form von Architekturbausteinen zu beschreiben und in Form von Lösungsbausteinen umzusetzen. Auf Basis dieser Bausteine und ihrer Beziehungen untereinander lassen sich Referenzmodelle und –architekturen entwickeln. Die Bausteine sind geeignet, in ein Architektur-Repository aufgenommen zu werden und können hieraus zur Darstellung von IST-Architekturen und SOLL-Architekturen herangezogen werden. Aufgrund der Bedeutung für die Wartbarkeit, Flexibilität und Wirtschaftlichkeit der IT-Landschaft wird eine

	Prüfung von loser Kopplung/Modularität bei Neu- und Weiterentwicklungen von föderalen IT-Lösungen durch das Architekturboard vorgenommen.
Beispiel für die Anwendung	Erarbeitung einer föderalen IT-Landkarte als Orientierung für den Schnitt von föderalen IT-Lösungen.. Auch die interne IT-Architektur einer IT-Lösung ist modular aufzubauen.
Bezug zu Zielen und Gesetzen	S3: Digitale Verwaltung – Grundprinzipen „Wirtschaftlichkeit“ und „nachhaltige technische Qualität“

SR11: Gewährleistung einer umweltfreundlichen und nachhaltigen Nutzung von Informationstechnik	**MUSS**
Beschreibung	Es muss über den gesamten Lebenszyklus der Informationstechnik auf einen umweltfreundlichen und nachhaltigen Einsatz geachtet werden. Rechenzentren und deren Infrastruktur sollen so ausgewählt und gestaltet werden, dass eine hohe Energieeffizienz und hohe Auslastung der Hardware-Ressourcen (z. B. Serverkapazitäten) erreicht wird. Darüber hinaus sind die Anforderungen des “Blauen Engels” für einen energieeffizienten Rechenzentrumsbetrieb in den Rechenzentren der öffentlichen Verwaltung einzuhalten. Ein flexibles Up-/Downsizing an kapazitative Anforderungen soll dabei Berücksichtigung finden. Um natürliche Ressourcen zu schonen, soll funktionstüchtige IKT nach dem Nutzungsende in den Behörden für eine Wiederverwendung Verfügung gestellt oder fachgerecht verwertet werden. Zusätzlich sollen jegliche IT-Lösungen so konzipiert werden, dass der Ressourcenverbrauch über den gesamten Lebenszyklus minimiert wird und gleichzeitig möglichst optimale Auslastungszeiten realisiert werden.
Begründung	Umsetzung der Green-IT-Strategie des IT-Planungsrates
Abhängigkeiten	Keine Abhängigkeiten vorhanden
Implikationen	Die Anschaffungskosten für Hardware können im Zusammenhang mit dieser Richtlinie steigen, da umweltfreundliche Geräte häufig preisintensiver sind.
Beispiel für die Anwendung	Bewertung von Architekturalternativen auch auf der Grundlage vom geschätzten Energieverbrauch.

Bezug zu Zielen und Gesetzen	S2: Green-IT

SR12: Umsetzung des „Once Only“ Prinzips	**SOLL**
Beschreibung	Bürgerinnen und Bürger sollten ihre Daten und Dokumente nur einmal mitteilen müssen. Nachweisdokumente werden schrittweise durch Registerabfragen und zwischenbehördliche Datenaustausche ersetzt.
Begründung	Das Once-Only-Prinzip ist nicht nur eine Entlastung der Bürgerinnen und Bürger, sondern auch der Verwaltung selbst. Durch den Austausch, das Abrufen und gemeinsame Speichern bereits gesammelter Informationen verringern sich der Aufwand und die Kosten für die Verwaltung.
Abhängigkeiten	Keine
Implikationen	Das Once-Only-Prinzip kann direkt über Registerabfragen und Once-Only-Projekte umgesetzt werden, wenn diese Ressourcen bestehen und keine rechtlichen Hürden im Weg stehen. Sollte es Hürden technischer oder rechtlicher Art geben, ist es wichtig, den Onlinedienst standardisiert so umzusetzen, dass dieser in Zukunft in neue Systeme integriert werden kann.
Beispiel für die Anwendung	Online-Dienstanträge werden mit Informationen aus Registern vorbefüllt. Der Nutzer muss nur die Korrektheit der Informationen bestätigen.
Bezug zu Zielen und Gesetzen	R2: Single Digital Gateway Verordnung, R3: Registermodernisierungsgesetz

SR13: Open Data by Design	**MUSS**
Beschreibung	IT-Lösungen sind bereits während des Designs so zu gestalten, damit Daten über öffentliche Netze verfügbar gemacht werden können. Dies gilt für alle Daten, die nicht geschützt werden müssen.
Begründung	Daten der öffentlichen Verwaltung öffnen Möglichkeiten für externe Akteure (Wirtschaft und Privatpersonen) Mehrwert-Dienstleistungen zu schaffen.

Abhängigkeiten	Keine
Implikationen	Föderale Infrastrukturprojekte müssen unentgeltliche Bereitstellungen von Daten ermöglichen. Die föderale Infrastruktur ist auf Open Data Fähigkeit zu prüfen, sofern relevant. Das Architekturboard wird bei der Prüfung von Infrastrukturprojekten die geplante IT-Architektur und deren Umsetzung prüfen. Die Daten müssen mit Metadaten versehen werden und auf dem nationalen Portal GovData eingestellt werden.
Beispiel für die Anwendung	# Statistische Erhebungen z. B. Anzahl der Zugriffe auf Verwaltungsleistungen und Online-Dienste Recyclingkarte mit Altkleider-, Altpapier- und Altglas-Container.
Bezug zu Zielen und Gesetzen	S5: Open Data fördern, S4: Verwaltung als Plattform

6 Anwendung der Architekturrichtlinien

Die Anwendung der Architekturrichtlinien richten sich nach der Verbindlichkeit der Architekturrichtlinien (MUSS, KANN, DARF NICHT). Abweichungen von Architekturrichtlinien der Kategorie MUSS und DARF NICHT müssen dem Architekturboard dargelegt und begründet werden. Für Anträge auf diesbezügliche Ausnahmegenehmigungen wird das föderale Architekturboard entsprechende Vorlagen bereitstellen. Neue Projekte müssen begründen, wie sie beabsichtigen, MUSS-Architekturrichtlinien umzusetzen, wenn diese nicht unmittelbar eindeutig messbar sind. Dies ist insbesondere für strategische Architekturrichtlinien der Fall.

Der Ablauf zur Nutzung der Architekturrichtlinien ist Teil des Architekturmanagementprozesses und wird separat dokumentiert. Grundsätzlich gilt, dass entlang des Lebenszyklus von föderalen IT-Lösungen Quality-Gates vorgesehen sind. Zu ausgewählten Zeitpunkten, z. B. vor Projektinitialisierung oder vor einer Ausschreibung muss der Projektleiter bzw. verantwortliche IT-Architekt die Konformität zu den Architekturrichtlinien begründen. Ergänzend dazu dienen die Architekturrichtlinien als Grundlage für Architekturreviews, die durch das Architekturboard initiiert werden können.

7 Anpassung und Weiterentwicklung der Architekturrichtlinien

Die vorliegende Version der Architekturrichtlinie soll für ausgewählte Projekte/ Infrastrukturanträge erprobt werden. Basierend auf den Erfahrungen sollen sie bedarfsorientiert angepasst werden. Im weiteren Verlauf sollen die Architekturrichtlinien ergänzt werden, so dass zusätzlich zu den übergreifenden strategischen Architekturrichtlinien domänenspezifische

Architekturrichtlinien hinzukommen. Darüber hinaus werden die Architekturrichtlinien wie folgt angepasst:

- Turnusmäßige (z. B. jährliche) Überprüfung der Architekturrichtlinien. Dabei erfolgt eine Überprüfung der neuen Versionen vorhandener aktualisierter Architekturrichtlinien Bund und Länder. Sofern für föderale Belange relevant und sinnvoll, werden angepasste oder neue Architekturrichtlinien übernommen.
- Anpassung auf Antrag: Beteiligte Bund und Länder können Vorschläge zur Ergänzung der Architekturrichtlinien unterbreiten und dem Architekturboard senden. Das Architekturboard wird für die Anträge entsprechende Vorlagen erarbeiten und veröffentlichen. Die Entscheidung, inwieweit die Vorschläge unverändert oder mit Anpassung übernommen werden, wird im Architekturboard getroffen.
- Anpassungen können sich auch aufgrund geänderter strategischer Vorgaben des IT-Planungsrates ergeben. Die Richtlinien sind in diesen Fällen zeitnah den geänderten Rahmenbedingungen anzupassen.
- Die Architekturrichtlinien werden nach Vorlage und Vorstellung durch das Architekturboard von der AL-Runde verabschiedet.

Die Architekturrichtlinien in der vorliegenden Fassung sollen als Grundlagendokument initial seitens des IT-Planungsrates beschlossen werden. Entsprechend dem Dokument „Zusammenwirken im föderalen Architekturboard (Organisation)“[11] werden alle weiteren Anpassungen der strategischen Architekturrichtlinien nach Vorlage und Vorstellung durch das Architekturboard von der AL-Runde verabschiedet.

[11] https://www.fitko.de/mm/Organisation_Architekturboard_1.0.pdf

Empfehlungen zur Weiterentwicklung der Digitaltauglichkeit der Verwaltung

Die Umsetzung des Onlinezugangsgesetzes und die Registermodernisierung haben das Bewusstsein gestärkt, dass die Verwaltungsdigitalisierung einen grundlegenden Transformationsprozess ausgelöst hat, der ganzheitliches Denken und Handeln auf allen staatlichen Ebenen erfordert. Die Erwartungen der Nutzerinnen und Nutzer, die Wirtschaftlichkeit von digitalisierten Verfahren und die finanzielle Förderung von Digitalisierungsprojekten beschleunigen diesen Veränderungsprozess erheblich. Der Übergang zu einem vorrangig digitalen Verwaltungshandeln stellt jedoch eine erhebliche Herausforderung dar, die nicht ohne eine Weiterentwicklung des Rechts bewältigt werden

Um grundsätzliche Digitalisierungshemmnisse abzubauen, sind daher rechtliche Rahmenbedingungen zu schaffen, die die erforderliche Standardisierung in Recht und Technik konsequent vorantreiben und eine flexible, sachgerechte Aufgabenverteilung innerhalb der föderalen Strukturen ermöglichen:

1. Die Digitaltauglichkeit muss auf allen staatlichen Ebenen weiter vorangetrieben werden. Das Zielbild bleibt, den Bürgerinnen und Bürgern und der Wirtschaft durchgehend möglichst viele Verwaltungsleistungen digital zur Verfügung zu stellen.

Es gilt, die Potentiale der Digitalisierung umfassend nutzbar zu machen und eine moderne, effiziente und bürgerfreundliche Verwaltung zu gewährleisten. Weitere wichtige Bausteine hierfür sind u.a. die technische und rechtliche Gleichstellung von digitalen und schriftlichen Nachweisen und die Verbesserung der Nutzerfreundlichkeit des elektronischen Schriftformersatzes im Rahmen der Schaffung der OZG-Nutzerkonten. Ziel sollte sein, dass die Ergebnisse von Verwaltungsleistungen (Genehmigungen, Nachweise, o.ä.) nicht nur digital beantragt, sondern auch in digitaler Form weiterverwendet werden können.

Die von der Digitalisierung eröffneten Möglichkeiten und Chancen sind dabei noch konsequenter zu nutzen. Zu prüfen ist etwa, ob Bürgerinnen und Bürger sowie der Wirtschaft auf der Grundlage bereits erhobener Daten proaktiv auf mögliche relevante Verwaltungsleistungen hingewiesen werden können. Von allen staatlichen Ebenen geprüft werden sollte auch, inwieweit eine Pflicht zur Nutzung elektronischer Kommunikation mit der Verwaltung und eine ausschließlich elektronische Ausgestaltung von Verwaltungsverfahren im wirtschaftlichen Kontext (Unternehmen, Selbstständige) mit der Verwaltung ausgeweitet werden kann.

2. Das Verwaltungsverfahren muss sich auf den Standardfall der digitalen Dienstleistung gegenüber Bürgerinnen, Bürgern und der Wirtschaft hin ausrichten. Alle Potentiale der Digitalisierung müssen nutzbar gemacht werden.

Grundlage hierfür ist insbesondere die Herausarbeitung einer gemeinsamen „DNA“ der Verfahrensordnungen und die Schaffung eines einheitlichen Ordnungsrahmens, um eine einheitliche digitale Abwicklung aller Verwaltungskontakte zu ermöglichen. Die bestehenden Regelungen für den digitalen Kontakt des Bürgers zur Verwaltung sind dabei konsistent und verständlich fortzuentwickeln. Besonderes Augenmerk liegt auf den verschiedenen Regelungen zu Authentifizierungsniveaus, Zustellungs- und Bekanntgabe von Verwaltungsakten und Widerspruchsverfahren.

3. Der laufenden Standardisierung im Bereich der IT muss auch eine Harmonisierung von Rechtsbegriffen folgen.

Die Vielfalt der bestehenden inhaltlichen Divergenzen bestehender Grundbegriffe im Recht (Einkommen, Vermögen, Kind, u.a.) und die daraus erwachsenden Hemmnisse bei der digitalen Umsetzung sind hinlänglich bekannt. Insbesondere auch für die Umsetzung des „Once-Only“-Prinzips im Kontext der Registermodernisierung ist die Harmonisierung von Rechtsbegriffen unumgänglich. Daher sind Schwerpunkte für solche Harmonisierungsbedarfe aktiv zu setzen und in ressortübergreifenden Projekten zu adressieren. Als Ausgangspunkt eignen sich die Überlegungen des Nationalen Normenkontrollrates zum Einkommensbegriff, deren praktische Umsetzung zu prüfen ist.

4. Schon im Entstehungsprozess von Regelungsvorhaben muss ein Fokus auf einfachen, digital- und praxistauglichen Verwaltungsprozessen liegen

Es gilt, die Logik digitaler Verwaltungsprozesse in Einklang mit rechtlicher Regulierung zu bringen. Erst nach dem Design eines guten Prozesses sollte daher die Phase der Gesetzeserarbeitung starten. Ziel ist es, die Prozesse auf allen staatlichen Ebenen so einfach und konsistent wie möglich, also digitaltauglich, zu machen. Dabei sollte auch geprüft werden, welche informationstechnischen Strukturen, Kapazitäten und Standards für den Gesetzesvollzug jeweils notwendig sind.

Verschiedene Akteure haben hierzu bereits zielführende Vorschläge erarbeitet

(vgl. NKR, „Erst der Inhalt, dann die Paragrafen. Gesetze wirksam und praxistauglich gestalten“, www.gute-gesetze.de ; ÖFIT, Recht digital, https://www.oeffentliche-it.de/publikationen?doc=104099&title=Recht+Digital+-+Maschinenverst%C3%A4ndlich+und+automatisierbar).

Einige Vorschläge werden bereits auf Bundesebene an ausgewählten Regulierungsvorhaben erprobt. Es gilt, dortige Erfahrungen zeitnah auszuwerten und darauf aufsetzend diese Verfahrensweisen breiter in die Praxis umzusetzen. Als Basis für die Überlegungen bietet sich die FIM-Methodik an.

5. Die Verpflichtung zur Digitalisierung der Verwaltung muss auch über das Ende der Umsetzungsfrist des OZG in 2022 hinaus fortgeschrieben werden. Der Digitalisierung der Antragsprozesse muss die Digitalisierung der internen Prozesse folgen, um die notwendigen Effizienz- und Serviceversprechen auch einlösen zu können.

Das OZG mit seiner rechtlichen Pflicht zur Digitalisierung hat den notwendigen Impuls für die Ebenen übergreifende Digitalisierung ausgelöst. Auch wenn dieser Prozess noch nicht abgeschlossen ist, bedarf es einer weiteren, auch rechtlichen Zielvorgabe, wie die Digitalisierung in Bund, Ländern und Kommunen insgesamt weitergehen soll. Notwendig ist ein Impuls ("OZG 2.0"), der insbesondere auch den Blick auf die Fachverfahren der Verwaltung richten und auch dort eine Digitalisierung nach denselben Prinzipien vorsehen sollte. Bei der Weiterentwicklung sollte auch geklärt werden, in welcher Weise Bund und Länder bei diesen und weiteren Digitalisierungsvorhaben künftig zusammenarbeiten wollen.

6. Die für die Digitalisierung notwendige Zusammenarbeit im Föderalstaat muss eine flexible, sachgerechte Aufgabenverteilung auch rechtlich zulassen. Ziel muss es sein, die interföderalen Vollzugsstrukturen so auszugestalten, dass diese nicht länger als Hindernis für die Standardisierung und als Hemmnis für die Digitalisierung insgesamt wirken.

Die bei der Verwaltungsdigitalisierung bestehenden Möglichkeiten und Notwendigkeiten einer Zusammenarbeit von Bund, Ländern und Kommunen dürfen nicht an überwindbaren rechtlichen Hindernissen scheitern. Rechtliche Strukturen sind im Rahmen des Föderalismus so weiterzuentwickeln, dass sie den Austausch von Arbeitsergebnissen sowie die Verankerung von technischen Standards und die Nutzung von digitalisierten Leistungen zwischen staatlichen Stellen aller Ebenen fördern und voraussetzen. Die aus der Umsetzung des "Einer für Alle"-Prinzips gewonnenen Erkenntnisse sind so zu operationalisieren, dass ein arbeitsteiliges Vorgehen und die Möglichkeit der Mitnutzung von standardisierten Leistungen bei der Verwaltungsdigitalisierung zukünftig den Normalfall der Zusammenarbeit darstellen.

35. Sitzung des IT-Planungsrates (23.06.2021 | Videokonferenz)

Steckbrief

Berichterstatter: Freie Hansestadt Bremen
Organisationseinheit: Der Senator für Finanzen, Referat 40
Ansprechpartner: Dirk Caliebe, 0421 361-4975, dirk.caliebe@finanzen.bremen.de
Stand: 10.05.2021

TOP 10 Digitale Datenaustauschverfahren und Einkommensbegriff modularisieren

Kategorie B | Schwerpunktthemen

Quellbeschluss (nur bei Folgeauftrag) 2021/ 34. IT-PLR, TOP 00

Geschätzte Dauer der Behandlung: ca. 10 Minuten

Gegenstand der Behandlung:
Bund und Länder sind nach dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG) verpflichtet, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten (§ 1 Abs. 1 OZG).

Die deutsche Register- und Fachverfahrenslandschaft umfasst mehrere Hundert einzelne Register und Fachverfahren, die alle zweckgebunden und bislang weitestgehend unabhängig voneinander agieren. Für den Austausch von Informationen zwischen den Registern und Fachverfahren der unterschiedlichen Stellen der öffentlichen Verwaltung bedarf es aktueller, konsistenter und eineindeutiger Daten. Das Registermodernisierungsgesetz und das Unternehmensbasisdatenregistergesetz haben die Basis für den Aufbau einer modernen Registerlandschaft geschaffen, die – jenseits von Stammdaten – den Austausch der zu einer natürlichen Person oder zu einem Unternehmen gespeicherten Daten ermöglichen soll. Dies ist die Voraussetzung für die Umsetzung des „once only"-Prinzips. Nun gilt es, die in den Registern und Fachverfahren vorhandenen Daten verfahrensübergreifend zu nutzen (Level 4 des Reifegradmodells bei der OZG-Umsetzung) und die Datenqualität so zu verbessern, dass das „once only"-Prinzip verwirklicht wird und Daten, die bereits bei öffentlichen Stellen vorhanden sind, nicht erneut durch die Betroffenen beigebracht werden müssen. Dies ist ein wesentlicher Schritt zur Harmonisierung der Zielbilder in einer verfahrensübergreifenden, dezentralen Datenarchitektur.

Zum Zwecke der Digitalisierung von Verwaltungsleistungen müssen Rechtsvorschriften in Datenstrukturen und Algorithmen abgebildet werden können. Je eineindeutiger Rechtsbegriffe sind, desto einfacher gelingt ihre digitale Übersetzung. Sind die Rechtsbegriffe

aber nicht eindeutig oder sogar unterschiedlich definiert oder werden sie unterschiedlich ausgelegt und angewendet, stößt die digitale Übersetzung schnell an ihre Grenzen und es wird eine verfahrensübergreifende Nutzung von Daten unter dem Gesichtspunkt von „once only“ erheblich erschwert, wenn nicht gar unmöglich.

Ein dem Wortlaut nach identischer Begriff (z.B. Einkommen) kann in unterschiedlichen Rechtsgebieten – teilweise sogar innerhalb desselben Rechtsgebiets – ganz unterschiedliche Bedeutungen und damit auch ganz unterschiedliche Inhalte haben, etwa im Hinblick auf sachliche Bezugspunkte und Abgrenzungen, Zeit- und Personenbezüge. Daten, die von einer Stelle erhoben und verarbeitet werden, können in diesem Fall von anderen Stellen nicht im Sinne von „once only“ genutzt werden, da die verschiedenen Stellen unter dem vermeintlich gleichen Begriff Unterschiedliches verstehen. Dies gilt insbesondere für den Begriff des Einkommens, der für die Gewährung von Sozialleistungen (z.B. Elterngeld, Wohngeld, SGB II-Leistungen) und bei der Steuererhebung im höchsten Maße relevant ist.

Der Nationale Normenkontrollrat (NKR) hat diese Thematik anhand des Einkommensbegriffs untersucht, der für die Digitalisierung diverser Verwaltungsleistungen ein Kernelement darstellt. Ausgangspunkt ist dabei die Erkenntnis, dass die Digitalisierung von Verwaltungsleistungen im Sinne des „once only“-Prinzips verfahrens- und rechtsgebietsübergreifende eineindeutige (d.h. wechselseitig eindeutige), referenzierbare, Datenfelddefinitionen erforderlich sind. Diese wiederum setzen jedoch ihrerseits verfahrens- und rechtsgebietsübergreifend eineindeutige Rechtsbegriffe voraus.

Hiervon ausgehend hat der NKR in seinem Gutachten folgende – hier nur auszugsweise und verkürzt dargestellte - Handlungsempfehlungen ausgesprochen:

1. Es soll geprüft werden, inwieweit eine Angleichung von Rechtsbegriffen ohne inhaltliche Änderungen möglich ist, um zu einer verfahrens- und rechtsgebietsübergreifenden eineindeutigen Nomenklatur bei der Verwendung von Rechtsbegriffen zu kommen.
2. Ist dies nicht möglich, wird empfohlen, bestehende Rechtsbegriffe weitestmöglich zu modularisieren, so dass aus wechselseitig eineindeutig referenzierbaren und digital nachnutzbaren Rechtsbegriffsmodulen oder -submodulen, je nach Rechtskontext und Rechtsgebiet, übergeordnete Rechtsbegriffe zusammengestellt werden können.
3. Rechtsbegriffe sollten durch Rechtsverweise auf einzelne Rechtsbegriffsmodule oder -submodule oder durch Typisierungen und Pauschalisierungen harmonisiert werden.
4. Um einen Überblick zu schaffen und dauerhaft zu behalten, welche Begriffsmodule existieren, bedarf es eines Data Dictionary. Darin werden Begriffsmodule (Datenmodelle), Zuständigkeiten und mithilfe der Verwaltungsdaten-Informationsplattform (gem. § 5a Bundesstatistikgesetz - BStatG) oder der Registerlandkarte (gem. § 3 I Nr. 1 Identifikationsnummerngesetz - IDNrG) zugehörige Datenquellen eindeutig beschrieben. Je automatisierter und einfacher der Datenaustausch erfolgen soll, desto wichtiger ist die semantische, aber auch die technische Standardisierung. Hier hilft ein auf das Data Dictionary aufbauendes Data Repository, indem die technische Datenstruktur definiert wird. Hierbei kann auf bestehende Projekte wie z. B. OMS, rvBEA, XÖV-Standards, die Prozess- und

Datenfeld-Repositorien des Föderalen Informationsmanagements (FIM) aufgebaut werden.

5. Damit bei der Umsetzung des Onlinezugangsgesetzes die 575 wichtigsten Verwaltungsleistungen vollständig digital und mit Rückgriff auf elektronische Datenbestände abgebildet werden können, müssen die Umsetzungsverantwortlichen u. a. prüfen, wie die gesetzlich vorgegebenen Rechtsbegriffe zu den verfügbaren Datenquellen passen. Hierzu bedarf es der gemeinsamen systematischen und schrittweisen Inventur des Rechts- und Datenbestandes.
6. Schließlich wird die Etablierung eines Digitaltauglichkeits-Checks bei der Gesetzesvorbereitung (z.B. Rechtsbegriffswahl, grafische Darstellung der Datenströme) empfohlen, der es bereits bei der Formulierung neuer rechtlicher Regeln erlaubt, deren Digitaltauglichkeit sicherzustellen.

Fachliche Betroffenheit der Fachministerkonferenzen[1]:

☒ Ja Allgemeine Betroffenheit durch potentielle fehlende Digitaltauglichkeit von Recht bei der Digitalisierung der OZG-Leistungen

☐ Nein

Art der Behandlung:
☐ Information
☒ Beschluss

Die folgenden Felder sind nur bei der Behandlungsart *Beschluss* auszufüllen.

Geplante Sitzungsunterlagen
Anlage1: Gutachten des Nationalen Normenkontrollrates „Einkommen einfacher nachweisen – Harmonisierung von Rechtsbegriffen und Digitalisierung der Nachweisführung“

Beschlussvorschlag

1. Der IT-Planungsrat nimmt das Gutachten des Nationalen Normenkontrollrates „Einkommen einfacher nachweisen – Harmonisierung von Rechtsbegriffen und Digitalisierung der Nachweisführung“ zur Kenntnis.
2. Der IT-Planungsrat bittet Bund, Bremen und Hamburg bis zur nächsten Sitzung des IT-Planungsrates eine Bewertung der Handlungsempfehlungen vorzulegen.
3. Der IT-Planungsrat bittet das Land Bremen, anhand von konkreten Leistungen aufzuzeigen, welche Hinderungsgründe einem digitalen Datenaustausch zu Einkommensmodulen entgegenstehen, weitere Handlungsvorschläge zu unterbreiten und über seine Ergebnisse auf der 37. IT-Planungsratssitzung zu berichten.

1 Gemäß § 1 Abs. 6 des IT-Staatsvertrags werden die Fachministerkonferenzen vom IT-Planungsrat beteiligt, sofern deren Fachplanungen von seinen Entscheidungen betroffen sind.

Nur bei Standards: Halten die Berichterstatter eine Beschlussfassung nach § 3 Abs. 2 des IT-Staatsvertrages zur Ausführung von § 91c GG[2] für angezeigt (Interoperabilitätsstandard)?

☐ Ja ☐ Nein

Ist das Recht auf informationelle Selbstbestimmung betroffen[3]?
☐ Ja ☒ Nein

Wie wirkt sich der Entscheidungsvorschlag auf das Recht der informationellen Selbstbestimmung aus?
[Auswirkung]

Veröffentlichung[4] der im Entscheidungsvorschlag in Bezug genommenen Sitzungsunterlagen:

☐ Ja

☒ Nein. Das angehängte Gutachten des Normenkontrollrats ist mit einem Sperrvermerk bis zum 29.06.202, 11.00 Uhr, als vertraulich „Nur für den Dienstgebrauch" eingestuft und darf nur ausschließlich Vorbereitung der AL-Runde und der Sitzung des IT-Planungsrates verwendet werden.

Die folgenden Felder sind nur bei der geplanten Beanspruchung von durch die *FITKO verwalteten Ressourcen* auszufüllen.

Schätzung des Ressourcenbedarfs[5] (*Bitte Erklärung in den Fußnoten beachten)*:

	2021	2022	2023	2024	2025
Sachmittel[6] (in TEUR)					

[2] Beschlüsse über Standards werden vom IT-Planungsrat mit der Zustimmung des Bundes und einer Mehrheit von 11 Ländern, welche mindestens zwei Drittel ihrer Finanzierungsanteile nach dem Königsteiner Schlüssel abbildet, gefasst, soweit dies zum bund-länderübergreifenden Datenaustausch oder zur Vereinheitlichung des Datenaustauschs der öffentlichen Verwaltung mit Bürgern und Wirtschaft notwendig ist (§ 2 Abs. 2 IT-Staatsvertrag).
[3] Nach § 5 Abs. 2 Nr. 1 der Geschäftsordnung des IT-Planungsrats ist bei Entscheidungsvorschlägen insbesondere darzulegen, ob und inwieweit durch die Entscheidung das Recht auf informationelle Selbstbestimmung betroffen sein könnte.
[4] Der IT-Planungsrat hat eine grundsätzlich transparente Veröffentlichungspraxis beschlossen. Sollte im Einzelfall keine oder eine nur teilweise Veröffentlichung geboten erscheinen, ist dies kurz zu begründen.
[5] Zeithorizont: laufendes Jahr +3 Jahre (bei kürzeren Projekten bitte den gesamten Projektzeitraum betrachten)
[6] Sachmittel sind alle bei der FITKO in Rechnung zu stellenden Kosten des Vorhabens (inkl. Investitions-, Betriebs- und Übergabekosten sowie Personalkosten)

FITKO-Personal[7] (in VZÄ)					

☐ Ressourcen sind im laufenden Wirtschaftsplan **vorhanden**
☐ Ressourcen sind im Wirtschaftsplan der FITKO für das kommende Jahr **eingeplant**
☐ Ressourcen sind aktuell **nicht** eingeplant

[7] FITKO-Personal sind FITKO-Mitarbeiter:innen, die für die Koordinierung und Steuerung oder anderweitige Unterstützung des Vorhabens benötigt werden.

IT-Planungsrat

Digitale Zukunft gestalten

Bericht zum IT-Planungsrat

215. Sitzung der Innenministerkonferenz (IMK)
vom 1. bis 3. Dezember 2021 in Stuttgart

Inhalt

Der IT-Planungsrat hat seit der letzten Berichterstattung an die IMK zwei Sitzungen am 23.06.2021 (35. Sitzung) und am 29.10.2021 (36. Sitzung) abgehalten. In diesem Jahr hat die Freie und Hansestadt Hamburg den Vorsitz im IT-Planungsrat, der durch Herrn Staatsrat Jan Pörksen, Chef der Senatskanzlei, ausgeübt wird.

Schwerpunktthemen der Sitzung waren u. a. die OZG-Umsetzung, die Registermodernisierung sowie die Beschleunigung der Digitalisierung mittels einer digitalisierungsfreundlichen Weiterentwicklung des Rechts und einer konsequenten Ausrichtung an den Bedürfnissen von Bürgerinnen, Bürgern und Unternehmen.

1 Schwerpunktthemen

1.1. OZG-Umsetzung

1.1.1 Konjunkturpaket und OZG-Umsetzung

Das Konjunkturpaket hat der Umsetzung des Onlinezugangsgesetzes (OZG) weiteren Schub verliehen. Dem Digitalisierungsprogramm Föderal, in dem sich die Länder aktiv einbringen, sind im Rahmen des Konjunkturpakets ein Anteil von 1,5 Mrd. Euro von insgesamt 3 Mrd. Euro für die Leistungsdigitalisierung zur Verfügung gestellt worden. Für eine Reihe von Umsetzungsprojekten sind bereits Mittel bereitgestellt, bei zahlreichen weiteren steht dies unmittelbar bevor.

Neben dem bereits vom Bund und allen Ländern geschlossenen Dachabkommen gehört der Abschluss von Einzelvereinbarungen zwischen den federführenden Bundesressorts und Ländern sowie das Einreichen von Projektanträgen zu den Voraussetzungen für die Nutzung von Konjunkturpaketmitteln. Von insgesamt 41 Einzelvereinbarungen sind 28 bereits geschlossen, weitere 13 befinden sich in der Finalisierung (Stand: 29.10.2021). Von den derzeit 119 geplanten Projektanträgen sind zudem bereits 95 von den Ländern erstellt. Für insgesamt 62 Projektanträge aus zehn der 14 Themenfelder stehen bereits Mittel bereit.

In der 35. Sitzung wurde zudem ein grundlegendes Kostenmodell sowie mögliche Verteilschlüssel für die Finanzierung von EfA-Leistungen beschlossen (Anlage 1)[1].

Mit dem nahenden Abschluss der Operationalisierung rückt nun die Leistungsdigitalisierung nach dem „Einer-für-Alle“-Prinzip (EfA) verstärkt in den Vordergrund, d. h. die Umsetzung in einem Land mit anschließender Nachnutzung in den übrigen Ländern. Die Vorteile des EfA-Prinzips werden in der Praxis bereits durch einige Pilotvorhaben erfolgreich demonstriert. Ein Beispiel ist die Leistung BAföG. An die EfA-Leistung sind in den vergangenen Monaten sukzessive weitere Länder angeschlossen worden, sodass der Online-Service ab Herbst 2021 von allen Bundesländern genutzt wird.

Seit August ist eine weitere Ausbaustufe des OZG-Dashboards[2] online. Sie beinhaltet eine interaktive Kartendarstellung verfügbarer Online-Dienste auf Bundes-, Länder und Kommunalebene. Als Datengrundlage dient das Online-Gateway des Portalverbunds. Dies ermöglicht eine regelmäßige Datenaktualisierung und damit einen aktuellen, öffentlich einsehbaren Stand über die Online-Verfügbarkeiten. Eine weitere Ausbaustufe zur Darstellung der Nutzerzufriedenheit soll zeitnah umgesetzt werden.

1.1.2 Kommunale Nachnutzung von EfA-Leistungen

Ein wichtiges Signal bzgl. der OZG-Umsetzung in Richtung Kommunen ist der Beschluss des IT-Planungsrats in seiner 36. Sitzung, einen virtuellen Marktplatz aufzubauen, der eine Nachnutzung von Online-Diensten nach dem EfA-Prinzip auch für die Kommunen ermöglicht. Mit der Umsetzung solch eines ganzheitlichen EfA-Nachnutzugsmodells wurde die govdigital eG beauftragt, die aktuell über ihre 20 Genossenschaftsmitglieder bundesweit rund 65 Prozent aller Kommunen erreicht. Ziel ist es, einen anbieteroffenen Marktplatz zu gestalten, in dem auch Leistungsangebote anderer Nachnutzungsmodelle, wie zum Beispiel der von der FITKO (Föderale IT-Kooperation) betreute FIT-Store, angeboten werden können. Über den FIT-Store werden zentral durch die FITKO betriebsbereite Online-Leistungen zu standardisierten Vertragsbedingungen eingekauft, im FIT-Store angeboten und an nachnutzungsinteressierte Länder

[1] Beschluss 2021/24
[2] https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/ozg-dashboard/ozg-dashboard-node.html

weiterverkauft. Die govdigital und die FITKO werden eng zusammenarbeiten, um den FIT-Store als Bestandteil des neuen Marktplatzes fortzuführen und weiterzuentwickeln.

1.2 Registermodernisierung

Der IT-Planungsrat hat am 17. März 2021 das vom Koordinierungsprojekt Registermodernisierung erarbeitete Zielbild der Registermodernisierung beschlossen. Um eine konzertierte Umsetzung der Registermodernisierung zu ermöglichen, wurde im IT-Planungsrat mit Beschluss vom 23. Juni 2021 die Einrichtung des Projektes „Gesamtsteuerung Registermodernisierung“ beschlossen. Unter Federführung des Bundes (Bundesministerium des Innern, für Bau und Heimat (BMI)) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen soll im Rahmen eines übergreifenden Programmmanagements die Umsetzung aller Teilprojekte der Registermodernisierung vorangetrieben werden.

Das Projekt hat zur 36. Sitzung einen Bericht zum Umsetzungsstand vorgelegt. Fokus hierbei liegt auf den durch die Federführenden definierten Zielen 2021 zur Aufnahme der inhaltlichen Arbeit, dem Stand des Aufbaus der Steuerungsstrukturen, dem Vorgehen zur Integration der Teilprojekte, aktuellen Pilotierungsvorhaben sowie dem Stand zur Umsetzung zum Art. 14 der SDG-Verordnung.

Daneben wurde eine vorläufige Schätzung des Ressourcenbedarfes zum Aufbau und Betrieb einer Gesamtsteuerung Registermodernisierung vorgelegt, welcher perspektivisch als Bund-Länder-Vorhaben durch ein Budget zur Programmsteuerung des IT-Planungsrats zu decken ist. Darüber hinaus fallen zur Umsetzung des Gesamtvorhabens Registermodernisierung auf Ebene Bund, Länder und Kommunen in den nächsten Jahren weiterführende Aufwände zur Realisierung des Zielbildes der Registermodernisierung an. Im Rahmen der Abstimmungen zu diesem Zielbild und zum Konzept Gesamtsteuerung Registermodernisierung wurde von Länderseite eine Bezifferung der zu erwartenden Aufwände zum Zwecke der Haushaltsvorsorge erbeten. Zur Abschätzung dieser Aufwände wurde daher ein Entwurf für ein Aufwandsschätzmodell (ASM) entwickelt. Die über das ASM geschätzten Gesamtaufwände sollen im nächsten Schritt mit Bund und Ländern unter Einbeziehung kommunaler Expertise validiert werden.

Da die zur Verfügung gestellten Mittel aus dem Konjunkturpaket des Bundes für die Umsetzung des Registermodernisierungsgesetzes für die im ASM abgedeckten Aufwände zur Reali-

sierung des Gesamtvorhabens nicht ausreichen werden, soll der weiterführende Finanzierungsbedarf auf Basis des ASM im Weiteren validiert und für die weitere Haushaltsvorsorge herangezogen werden.

Insgesamt sollte berücksichtigt werden, dass die Registermodernisierung in ihrer Komplexität ein ähnlich großes Vorhaben wie die Umsetzung des OZG darstellen dürfte.

Die Fachministerkonferenzen sind in die Umsetzung der Registermodernisierung einzubeziehen und sollten diese aktiv begleiten, da Register unterschiedlicher Fachbereiche betroffen sind. Die bereits von einigen Fachministerkonferenzen beschlossenen Digitalisierungsstrategien müssen im Zuge der Gesamtsteuerung Registermodernisierung an die neu zu errichtende, fachübergreifende Once-Only-Architektur angebunden werden. Von den Fachbereichen zu berücksichtigen sind hierbei auch die in der 36. Sitzung unter TOP 07 beschlossenen „Föderalen IT-Architekturrichtlinien“ (Anlage 2)[3]. Durch die Benennung von Ansprechpartnern seitens der Fachministerkonferenzen soll eine kontinuierliche Begleitung des Gesamtvorhabens gewährleistet werden.

1.3 Beschleunigung der Digitalisierung und Digitaltauglichkeit von Gesetzen

In der 36. Sitzung wurden Empfehlungen zur Beschleunigung der Digitalisierung der Verwaltung beschlossen, die der neuen Bundesregierung und den Regierungen der Länder übermittelt werden sollen. Diese Empfehlungen beziehen sich insbesondere auf die Weiterentwicklung der Digitaltauglichkeit der Verwaltung. Sie liegen diesem Bericht als Anlage 3[4] bei.

Die Umsetzung des Onlinezugangsgesetzes und die Registermodernisierung haben das Bewusstsein gestärkt, dass die Verwaltungsdigitalisierung einen grundlegenden Transformationsprozess ausgelöst hat, der ganzheitliches Denken und Handeln auf allen staatlichen Ebenen erfordert. Die Erwartungen der Nutzerinnen und Nutzer, die Wirtschaftlichkeit von digitalisierten Verfahren und die finanzielle Förderung von Digitalisierungsprojekten beschleunigen diesen Veränderungsprozess erheblich. Der Übergang zu einem vorrangig digitalen Verwaltungshandeln stellt jedoch eine erhebliche Herausforderung dar, die nicht ohne eine Weiterentwicklung des Rechts bewältigt werden können.

[3] Beschluss 2021/37
[4] Beschluss 2021/34

Um grundsätzliche Digitalisierungshemmnisse abzubauen, sind daher schnelle einfache, digital- und praxistaugliche Verwaltungsprozesse zu entwickeln. Die Optimierung interner Abläufe durch zeitgemäße digitale Lösungen kommt den Bürgerinnen, Bürgern und Unternehmen zugute. So soll zum Beispiel die technische und rechtliche Gleichstellung von digitalen und schriftlichen Nachweisen geprüft werden. Außerdem geht es um die praktische Umsetzung bei der Vereinheitlichung von Rechtsbegriffen. Beispielhaft kann hier der in der 35. Sitzung getroffene Beschluss zum Thema „Digitale Datenaustauschverfahren und Einkommensbegriff“ genannt werden (Anlage 4)[5].

1.4 Deutsche Verwaltungscloud-Strategie und Zentrum für Digitale Souveränität (ZenDiS)

Die im Oktober 2020 durch den IT-PLR beschlossene Deutsche Verwaltungscloud-Strategie (DVS) soll gemeinsame Standards und offene Schnittstellen für Cloud-Lösungen der Öffentlichen Verwaltung schaffen, um übergreifend eine interoperable sowie modulare föderale Cloud-Infrastruktur zu etablieren. Die Arbeitsgruppe „Cloud-Computing und Digitale Souveränität“ hat ein Rahmenwerk der Zielarchitektur für die DVS erarbeitet, welche in der 36. Sitzung beschlossen worden ist.

Auch wurde in der 36. Sitzung die Weiterentwicklung des Organisationskonzepts „Zentrums für Digitale Souveränität“ beschlossenen. Hiermit bestätigt der IT-Planungsrat die grundsätzliche Notwendigkeit zur Etablierung einer zentralen, koordinierenden Stelle zur Förderung von Open Source Software (OSS) in der Öffentlichen Verwaltung.

Beide Entscheidungen stellen einen wichtigen Beitrag im Bereich der Digitalen Souveränität dar und sind wesentliche Maßnahmen innerhalb der beschlossenen Strategie zur Stärkung der Digitalen Souveränität der IT der Öffentlichen Verwaltung (vgl. Entscheidung 2021/09).

[5] Beschluss 2021/27, für das in der Anlage genannte Gutachten des Normenkontrollrats siehe auch https://www.it-planungsrat.de/beschluss/beschluss-2021-27

2 Informationssicherheit

2.1 Umsetzung des Verbindlichen Meldeverfahrens zum Informationsaustausch über IT-Sicherheitsvorfälle

Der IT-Planungsrat hat turnusmäßig in der 35. Sitzung den Bericht der AG Informationssicherheit zur Umsetzung des Verbindlichen Meldeverfahrens zum Informationsaustausch über IT-Sicherheitsvorfälle im Verwaltungs-CERT-Verbund (VCV) zur Kenntnis genommen. Er bittet die Mitglieder des IT-Planungsrats, für den Meldestandard in Bund und Ländern zu werben und für eine Einhaltung der Meldepflicht Sorge zu tragen.

2.2 Anforderungskatalog zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen

Im Rahmen hybrider Bedrohungen können mögliche Versuche der Einflussnahme fremder Staaten auf die Bundestagswahl und damit einhergehend (Cyber-)Angriffe auf die Wahl nicht ausgeschlossen werden. Die zeitgerechte und korrekte Ermittlung des vorläufigen Wahlergebnisses hat herausragende Bedeutung für das Vertrauen der Öffentlichkeit in die Ordnungsmäßigkeit der Wahl insgesamt. Eine Manipulation oder Verzögerung der Ergebnisermittlung würde dieses Vertrauen nachhaltig erschüttern.

Eine Bund-Länder-Arbeitsgruppe des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Landeswahlleitungen und des Bundeswahlleiters unter Beteiligung der kommunalen Spitzenverbände hat daher einen „Anforderungskatalog zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen“ erstellt. Den beteiligten Wahlorganen und –behörden wurde mit Beschluss in der 35. Sitzung empfohlen, diesen Anforderungskatalog umzusetzen.

3 Änderung des E-Government-Gesetzes und Einführung des Gesetzes für die Nutzung von Daten des öffentlichen Sektors

Die Geschäfts- und Koordinierungsstelle GovData hat Vorschläge unterbreitet, wie das Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz (DNG)) in Deutschland sinnvoll umgesetzt werden kann. Noch nicht alle Länder sind der Verwaltungsvereinbarung GovData beigetreten und haben in der Folge aktuell keinen Zugang zu GovData. Des Weiteren ist auf der Grundlage des DNG mit einer Veröffentlichung von Daten in größerem Maße zu rechnen, zu denen die jeweiligen Metadaten auf GovData zu veröffentlichen sind. Dies ist organisatorisch und finanziell durch GovData in der derzeitigen Struktur nicht leistbar.

Vor diesem Hintergrund wurde in der 36. Sitzung beschlossen, dass - soweit noch nicht vorhanden - vom Bund und den Ländern Schnittstellen bzw. Übergabepunkte bereitgestellt werden, mit denen die Metadaten, die in Umsetzung des DNG bei GovData veröffentlicht werden sollen, gebündelt und strukturiert bereitgestellt werden. Für die Länder, denen der Aufbau einer Schnittstelle bzw. eines Übergabepunktes nicht möglich ist, wird die Geschäfts- und Koordinierungsstelle GovData in Abstimmung mit der FITKO ein verursachungsgerechtes Kostenmodell für die Länder ohne zentralen Datenübergabepunkt auf der Basis der Daten des kommenden Jahres zur Verfügung stellen. Zudem werde alle Länder gebeten, soweit noch nicht erfolgt, bis spätestens 31.12.2021 der Verwaltungsvereinbarung GovData beizutreten.

4 Anlagen

1. Kostenmodell und Verteilschlüssel für Finanzierung von EfA-Leistungen
2. Föderale IT-Architekturrichtlinien
3. Empfehlungen zur Beschleunigung der Digitalisierung
4. Steckbrief „Digitale Datenaustauschverfahren und Einkommensbegriff“

Der Beauftragte des Bundesrates in Ratstagungen der Europäischen Union für den Rat Justiz und Inneres (JI-Rat), Bereich Inneres, Staatsminister Peter Beuth MdL

JI-Rat-Bericht
an die Ständige Konferenz der Innenminister und -senatoren der Länder
(Mai 2020 bis Oktober 2021)

215. Sitzung vom 1. bis 3. Dezember 2021 in Stuttgart
(Stand 29.10.2021)

I.

In den Berichtszeitraum fallen folgende Sitzungen:

- Sitzung der EU-Innenminister vom 8. Juni 2021 (im 1+1-Format),
- informelle Sitzung der EU-Innenminister vom 15. Juli 2021,
- außerordentliche Videokonferenz der EU- Innenminister vom 18. August 2021 im Rahmen des IPCR-Formats (Integrierte Regelung für die politische Reaktion auf Krisen),
- Sitzung der EU-Innenminister vom 31. August 2021 zu Afghanistan,
- Sitzung der EU-Innenminister vom 8. Oktober 2021 (im 1+1-Format).

Nachdem seit Ausbruch der Corona-Pandemie ausschließlich in digitalem Format getagt worden war, wurden ab Juni 2021 wieder Präsenzsitzungen aufgenommen; regelmäßig jedoch in reduziertem Teilnahmeformat (grundsätzlich zwei Vertreter pro Mitgliedstaat/sog. 1+1 Regelung). Aus diesen Gründen erging an den Bundesratsbeauftragten zu keiner der Tagungen eine Einladung, so dass sich die Berichterstattung wiederum maßgeblich aus Berichten der Bundesregierung speisen muss.

II.

Schwerpunkt der Diskussionen des JI-Rats waren im betrachteten Zeitraum die Entwicklungen an der Außengrenze der EU zu Belarus sowie die migrationspolitische Lage nach der Machtübernahme der Taliban in Afghanistan. Hinsichtlich der Beratungen der Vorschläge zum Gemeinsamen Europäischen Asylsystem wurden teilweise Fortschritte erzielt – jedoch nicht in den zentralen Fragen der Solidarität und Umverteilung von Schutzsuchenden. Dahingegen gelang es, den Verordnungsvorschlag über eine Umwandlung von EASO in eine EU-Asylagentur (EUAA) zu verabschieden. Auch konnten Einigungen über der Blaue Karte-Richtlinie sowie die Fonds im Innenbereich erzielt werden. Im Bereich der Inneren Sicherheit standen Auswirkungen der Corona-Pandemie sowie der technologischen Entwicklungen (Künstliche Intelligenz sowie Nutzung digitaler Instrumente zur Strafverfolgung, insb. zur Bekämpfung von Kindesmissbrauch) im Vordergrund.

Die Berichterstattung bezieht sich auf die folgenden Politikbereiche:

Inhalt

I. Asyl und Migration

Die Themen Asyl und Migration standen im Berichtszeitraum wiederum im Mittelpunkt der Diskussionen.

1. Reform des Gemeinsamen Europäischen Asylsystems (GEAS)

Am 08.06.2021 gab der portugiesische Vorsitz einen Sachstandsbericht zum „neuen Migrations- und Asylpaket“ vom 23.09.2020[1], wobei der Fokus unter portugiesischem Ratsvorsitz auf der externen Dimension gelegen habe.

[1] Mitteilung der Kommission „Ein neues Migrations- und Asylpaket“ (COM(2020) 609 vom 23. September 2020).
Vorschlag für eine Verordnung zur Einführung eines Screenings von Drittstaatsangehörigen an den Außengrenzen (COM(2020) 612 vom 23. September 2020).
Geänderter Vorschlag für eine Verordnung zur Einführung eines gemeinsamen Verfahrens zur Gewährung internationalen Schutzes in der Union und zur Aufhebung der Richtlinie 2013/32/EU (COM(2020) 611 vom 23. September 2020).
Vorschlag für eine Verordnung über Asyl- und Migrationsmanagement, COM(2020) 610 vom 23. September 2020.
Geänderter Vorschlag für eine Verordnung über die Einrichtung von „Eurodac“, COM(2020) 614 vom 23. September 2020.
Vorschlag für eine Verordnung zur Bewältigung von Krisensituationen und Fällen höherer Gewalt im Bereich Migration und Asyl (COM(2020) 613 vom 23. September 2020).
Empfehlung der Kommission über einen Vorsorge- und Krisenmanagementmechanismus der EU für Migration (Vorsorge- und Krisenplan für Migration) (C(2020) 6469 vom 23. September 2020).
Empfehlung der Kommission zur Zusammenarbeit zwischen den Mitgliedstaaten bei Such- und Rettungsaktionen, für die im Eigentum privater Einrichtungen befindliche oder von solchen betriebene Schiffe eingesetzt werden (C(2020) 6468 vom 23. September 2020).
Leitlinien der Kommission zur Anwendung der EU-Vorschriften betreffend die Definition und Bekämpfung der Beihilfe zur unerlaubten Ein- und Durchreise und zum unerlaubten Aufenthalt (C(2020) 6470 vom 23. September 2020).
Empfehlung der Kommission zu legalen Schutzwegen in die EU: Förderung der Neuansiedlung, der Aufnahme aus humanitären Gründen und anderer komplementärer Zugangswege, C(2020) 6467 vom 23. September 2020.

Daneben seien die Arbeiten an den Verordnungs-Vorschlägen über Asyl- und Migrationsmanagement, zur Einführung eines gemeinsamen Verfahrens für den internationalen Schutz und zur Einführung eines Screenings von Drittstaatsangehörigen an den Außengrenzen auf technischer Ebene fortgeführt worden. Die KOM unterstrich die konstruktive Atmosphäre, in der an den Migrations-Dossiers gearbeitet worden sei.

Eine Kompromissfindung zur EU-Asylagentur-VO (EUAA)[2] erscheine in greifbarer Nähe. Diese Einigung (mit dem EP) wurde in der Folge auch erzielt, so dass das bisherige Europäische Unterstützungsbüro für Asylfragen (EASO) in eine Asylagentur der Europäischen Union noch bis Jahresende umgewandelt werden könnte. Die neue Agentur soll dazu beitragen, die Qualität der Asylverfahren in den Mitgliedstaaten zu verbessern sowie die Verfahren einheitlicher zu gestalten und zu beschleunigen. Eine neue Reserve von 500 Experten soll es der Agentur ferner ermöglichen, die nationalen Asylsysteme, die mit einer großen Zahl von Fällen konfrontiert sind, wirksamer zu unterstützen.

Am 15.07.2021 wurden die Diskussionen fortgeführt. Der ab Juli amtierende slowenische Ratsvorsitz hob hervor, dass trotz Festhalten an der sog. Paket-Lösung eine vorzeitige Verabschiedung einzelner Dossiers, insbesondere der Eurodac-Verordnung, möglich sein müsse, um schrittweise Fortschritte zu erzielen. Die Minister betonten u.a. die Notwendigkeit, die Diskussionen über Verantwortung und Solidarität fortzusetzen.

Am 08.10.2021 führte der JI-Rat eine Orientierungsaussprache zu Screening und Inhaftnahme an der Grenze durch. Die Frage eines separaten und zeitnahen Abschlusses der Screening-Verordnung wurde kontrovers diskutiert. Kommissarin Johansson verwies angesichts verstärkten Drucks an den Außengrenzen durch hybride Bedrohungen und zunehmender Sekundärmigration auf die Notwendigkeit zügiger Fortschritte bei Screening, Eurodac und Resettlement. Trotz Unterstützung der Mehrheit der Mitgliedstaaten (darunter DEU) für dieses Ansinnen blieben insbesondere die Mittelmeeranrainer-, die Visegrád-Staaten und BUL bei ihrer ablehnenden Haltung. V.a. HUN, SVK und CZE hoben zwar die essentielle Bedeutung des Screenings für den Außengrenzschutz hervor, beharrten jedoch weiter auf einer gemeinsamen Verabschiedung aller Dossiers des Asyl- und Migrationspaktes (sog. „Paketansatz).

Abschließend bekräftigte der JI-Rat seine Entschlossenheit, mit Unterstützung von Frontex die EU-Außengrenzen wirksam zu schützen, unerlaubte Einreisen zu verhindern und die am stärksten betroffenen Mitgliedstaaten zu unterstützen.

2. Externe Dimension – Zusammenarbeit mit Drittländern in Migrationsfragen

Anlässlich des o.g. Berichts des portugiesischen Ratsvorsitzes vom 08.06.2021 wurde aus dem Kreis der Mitgliedstaaten die Bitte geäußert, die KOM möge über den Stand und die Ergebnisse ihrer Verhandlungen im Namen der EU und ihrer Mitgliedstaaten mit Drittstaaten regelmäßig und strukturiert berichten. POR erinnerte daran, dass die verstärkte Zusammenarbeit mit Nordafrika eine Priorität seines Vorsitzes gewesen sei, mit besonderem Fokus auf MAR, LBY, TUN, EGY und MRT. Der Europäische Auswärtige Dienst habe begonnen, eine Strategie für privilegierte Partnerschaften zu erarbeiten.

[2] Vorschlag für eine Verodnung des Europäischen Parlaments und des Rates über die Asylagentur der Europäischen Union und zur Aufhebung der Verordnung (EU) Nr. 439/2010, COM(2016)271.

Am 15.07.2021 unterstrichen die Minister erneut die Bedeutung einer engeren Zusammenarbeit mit den Herkunfts- und Transitländern sowie einer effizienten Rückführung. Die Minister brachten ihre gemeinsame Besorgnis über die Situation in LIT zum Ausdruck und sicherten ihre volle Unterstützung bei der Bewältigung des Migrationsdrucks zu.

Am 18.08.2021 tagten die EU-Innenministerinnen und Innenminister kurzfristig aufgrund der Migrationssituation an der litauisch-belarussischen Grenze im Rahmen des IPCR-Formats („Integrierte Regelung für die politische Reaktion auf Krisen“ – diese ist pandemiebedingt seit Januar 2020 aktiviert). Einhellig wurde der Missbrauch von Migranten zu politischen Zwecken verurteilt. Viele der Mitgliedstaaten verwiesen auf die Bedeutung eines starken Außengrenzschutzes, aber auch der Instrumente der externen Dimension sowie auf die Notwendigkeit der zügigen Verabschiedung eines reformierten GEAS. Daneben berieten die Innenministerinnen und Innenminister über (weitere) materielle, personelle oder finanzielle Unterstützungsmöglichkeiten.
Ferner brieften der Hohe Vertreter der Europäischen Union für Außen- und Sicherheitspolitik Borrell sowie Kommissarin Johansson zur Lage in Afghanistan. Mit Blick auf die Migrationssituation sei es erforderlich, den Menschen vor Ort Unterstützung zukommen zu lassen; humanitäre Hilfe in Afghanistan und den Nachbarstaaten sei jetzt die wichtigste Aufgabe. Dies wurde von allen wortnehmenden Mitgliedstaaten unterstützt. FRA und DEU betonten zudem erneut die Dringlichkeit, bei der GEAS-Reform voranzukommen, um gerade auch in einer Krisensituation human und geordnet reagieren zu können und forderten eine zeitnahe erneute Befassung der Innenministerinnen und Innenminister mit der Lage in Afghanistan.

Diese erfolgte am 31.08.2021 im Rahmen einer Sondersitzung zu den Entwicklungen in Afghanistan. Der Rat nahm eine Erklärung an, in der die Minister betonten, dass die Evakuierung von EU-Bürgern und, soweit möglich, von afghanischen Staatsangehörigen, die mit der EU und ihren Mitgliedstaaten zusammengearbeitet haben, sowie deren Familienangehörigen vorrangig durchgeführt worden sei und fortgesetzt werde. Als unmittelbare Priorität werde sich die EU weiterhin mit internationalen Partnern, insbesondere den Vereinten Nationen und ihren Organisationen, bei der Stabilisierung der Region abstimmen und sicherstellen, dass die humanitäre Hilfe die gefährdeten Bevölkerungsgruppen erreicht. Die EU werde auch ihre Unterstützung für Drittländer, insbesondere für die Nachbar- und Transitländer, die eine große Zahl von Migranten und Flüchtlingen aufnehmen, verstärken. Die EU werde auch mit diesen Ländern zusammenarbeiten, um die illegale Migration aus der Region zu verhindern. Ferner versicherten die EU und ihre Mitgliedstaaten, ihr Möglichstes zu tun, um sicherzustellen, dass die Situation in Afghanistan nicht zu neuen Sicherheitsbedrohungen für EU-Bürger führe.

Am 08.10.2021 informierten KOM, der Europäische Auswärtige Dienst (EAD) sowie der neue EU-Koordinator für die Terrorismusbekämpfung Ilkka Salmi über die aktuelle Lage in Afghanistan. Tags zuvor hatte die KOM zu einem „Hochrangigen Forum zum Schutz gefährdeter afghanischer Staatsbürger“ geladen, bei dem die Mitgliedstaaten ihre bisher erfolgten bzw. die geplanten Hilfen für schutzbedürftige Afghanen darlegen konnten. Im Rahmen der Ratssitzung dankte die KOM den Mitgliedstaaten für ihre Hilfsbeiträge und zeigte sich erfreut darüber, dass im Rahmen der Evakuierungsaktionen bereits 22.000 afghanische Staatsbürger in der EU Aufnahme gefunden hätten (es befinden sich allerdings noch allein 25.000-30.000 Personen im Land, die nach DEU ausreiseberechtigt sind). Kommissarin Johansson berichtete, dass die humanitäre Lage in Afghanistan besorgniserregend sei. Da fast die Hälfte der Menschen in Afghanistan auf

humanitäre Hilfe angewiesen wäre, habe die EU ihren Beitrag kurzfristig von 50 Mio. EUR auf 300 Mio. EUR erhöht. Allerdings reiche auch dieser Betrag nicht aus, es gehe darum einen vollständigen Zusammenbruch Afghanistans zu verhindern. KOM berichtete, dass sich zwar 2 Mio. afghanische Staatsbürger in Pakistan und im Iran aufhielten, darüber hinaus jedoch nennenswerte Migrationsbewegungen ausgeblieben seien. Vielmehr seien bereits 150.000 Binnenvertriebene an ihre Wohnorte zurückgekehrt, an denen sich mit Ende des Krieges die Sicherheitslage teilweise stabilisiert habe. Anti-Terror-Koordinator Salmi stellte einen Aktionsplan zur Terrorismusbekämpfung in Afghanistan vor, der 23 Empfehlungen enthält. Kernpunkte seien die Durchführung von Sicherheitschecks, die Bereitstellung von EU-Grenzschutzkapazitätshilfen für Drittstaaten entlang von Migrationsrouten, die Implementierung einer Interoperabilitäts-Architektur, das Zusammenführen von Informationen, die strategische Kommunikation und das Aufstellen von Gegennarrativen zur Bekämpfung islamistischer Ideologien sowie der Kampf gegen Terrorismus-Finanzierung.

Ferner stellten KOM, Frontex, EASO und Europol am 08.10.2021 die aktuelle Lage auf den Migrationsrouten dar. Frontex verwies auf eine Zunahme der irregulären Grenzübertritte (+49%), insbesondere auf der zentralen Mittelmeer- und der Westbalkanroute. Im anschließenden Austausch erklärte MTA, die zentrale Mittelmeerroute sei aktuell am stärksten belastet, GRC meldete dagegen für die östliche Mittelmeerroute einen Rückgang der Ankünfte um 90% gegenüber dem Jahr 2020. Allerdings sei die Krise noch nicht vorbei, zumal das EU-Türkei-Abkommen faktisch nicht mehr angewendet werde. Für die Westbalkanroute forderten HUN und AUT eine stärkere Überwachung und wirksamere Bekämpfung von Schleusern. Eine Reihe von Mitgliedstaaten verurteilte den Einsatz von Migration als Waffe und politisches Druckmittel in einem hybriden Angriff wie aktuell an der EU-Außengrenze zu Belarus. Die KOM forderte dazu auf, ihren Vorschlag vom 29.09.2021 zur partiellen Aussetzung des Visaerleichterungsabkommens zwischen der EU und Belarus als europäische Reaktion zügig umzusetzen. SWE ergänzte, dass mittlerweile auch gezielte Migrationslenkungen durch Russland zu beobachten seien, die man aufmerksam verfolgen müsse. Im Hinblick auf die sich entspannende Pandemielage appellierten einige Mitgliedstaaten an die KOM, Verbesserungen beim Thema Rückführungen wieder prioritär in den Blick zu nehmen. SVN sagte, ein Ziel der Präsidentschaft sei, neun Migrationsaktionspläne zu finalisieren. Als konkrete Maßnahme wurde der sog. Visahebel gegenüber Gambia erwähnt.

3. Schengen-Raum

Nachdem die KOM ihre „Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum“[3] am 02.06.2021 vorgestellt hatte, erfolgte am 08.06.2021 eine erste Diskussion im JI-Rat. Ziel der Strategie ist es, den Schengen-Raum als zentrale Voraussetzung für den freien Verkehr von Personen, Waren und Dienstleistungen in der EU mit Blick auf die Erfahrungen der letzten Jahre, auch auf die COVID-19-Pandemie, zu stärken und widerstandsfähiger zu machen. Dazu sieht die Strategie eine Erhöhung der Wirksamkeit des EU-Außengrenzmanagements, eine Stärkung der Maßnahmen zum Ausgleich der fehlenden Binnengrenzkontrollen, insbesondere in den Bereichen Polizeizusammenarbeit, Sicherheit und Migrationsmanagement, sowie eine solide Krisenvorsorge und Governance einschließlich der Vollendung des Schengen-Raums vor. Die Mitgliedstaaten begrüßten die neue Strategie grundsätzlich, jedoch hoben zahlreiche

[3] Mitteilung der Kommission an das Europäische Parlament und den Rat „Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum“, COM(2021)277.

Mitgliedstaaten, darunter DEU, hervor, dass die Mitgliedstaaten weiterhin in Eigenverantwortung über die Einführung von Binnengrenzkontrollen entscheiden können müssten, wenn dies aus Sicherheitsgründen (insbesondere zur Terrorismusbekämpfung), im Falle unzureichenden Außengrenzschutzes oder in einer weiteren Gesundheitskrise wie der COVID-19-Pandemie geboten sei. BUL, GRC, LTV, POR, EST, LIT und ROM erklärten, dass der Erhalt der Freizügigkeit vordringlich sei. Neben einem effizienten Außengrenzschutz sei daher eine Verbesserung der „Kompensationsmaßnahmen" für Grenzkontrollen notwendig, d.h. verstärkte Polizeizusammenarbeit, Daten- und Informationsaustausch und Einsatz neuer Technologien. Damit werde es möglich, Kontrollen nicht nur an den Grenzen durchzuführen. CZE betonte außerdem, dass das Funktionieren des Binnenmarktes dauerhaft gewährleistet werden müsse.

4. Verschiedenes

a) Frontex

Am 08.06.2021 unterrichtete Kommissarin Johansson den Rat zum Umsetzungsstand der Verordnung über die Europäische Grenz- und Küstenwache (Frontex). Die Kommissarin hob insbesondere das ausgeweitete Mandat der Agentur hervor, das zugleich mit mehr Verantwortung, Personal und Finanzausstattung einhergehe. Bedauerlich sei, dass es zu einigen Verzögerungen (z.B. Einstellungen und Verwaltungsstruktur) gekommen sei. Wichtig sei in diesem Zusammenhang daher, dass die Mitgliedstaaten vermehrt ihrer Kontrollfunktion im Frontex-Verwaltungsrat nachkämen. Auch die Leitung der Agentur müsse sich den gestiegenen Anforderungen anpassen. Von Seiten der KOM unterstütze man ferner die Aufklärungsarbeiten in Bezug auf verschiedene Vorwürfe gegen die Agentur.

b) Interoperabilität der EU-Informationssysteme

Zur Umsetzung der Interoperabilität der EU-Informationssysteme, insbesondere des Entry-Exit-Systems (EES) und das Europäische Reiseinformations- und -genehmigungssystems (ETIAS), berichtete Kommissarin Johansson ebenfalls am 08.06.2021 und mahnte erneut eine Umsetzung aller erforderlichen Projekte innerhalb des geplanten Zeitrahmens an.

Am 08.10.2021 berichtete SVN, dass die Inbetriebnahme von EES und ETIAS jedoch nicht zuletzt aufgrund der COVID-19-Pandemie in Verzug sei. euLISA wurde daher beauftragt, bis zum Jahresende eine neue Zeitplanung für die Inbetriebnahme von EES und ETIAS vorzulegen, wobei an dem Ziel, die volle Interoperabilität bis Ende 2023 zu erreichen, festgehalten werden solle.

c) Blaue Karte-Richtlinie

Am 07.10.2021 hat der Rat die Richtlinie über die Bedingungen für die Einreise und den Aufenthalt von hochqualifizierten Drittstaatsangehörigen, die zum Leben und Arbeiten in die EU ziehen (sog. Richtlinie über die Blaue Karte), verabschiedet. Sie zielt darauf ab, einen Beitrag zur Harmonisierung der Einreise- und Aufenthaltsbedingungen und zur Stärkung der Attraktivität der Blauen Karte zu leisten. Konkret sollen durch die neuen Vorschriften die Mobilität innerhalb der EU erleichtert, Familienzusammenführungen ermöglicht und Verfahren für bereits anerkannte Arbeitgeberinnen und Arbeitgeber vereinfacht werden. Zudem wird der Geltungsbereich der Richtlinie nunmehr auf Drittstaatenangehörige, die Familienmitglieder in der EU haben, sowie auf Personen mit internationalem Schutzstatus ausgedehnt.

II. Innere Sicherheit

1. Europol-Verordnung

Am 08.06.2021 stellte der portugiesische Vorsitz seinen Fortschrittsbericht zu den Beratungen des Änderungsvorschlag zur Europol-Verordnung[4] vor. Das Dossier sei seitens des portugiesischen Ratsvorsitzes prioritär behandelt und in den meisten Themenbereichen seien erhebliche Fortschritte erzielt worden, u.a. zur Zusammenarbeit mit Privaten und Drittstaaten sowie der Europäischen Staatsanwaltschaft und den Regelungen zum Europol-Verwaltungsrat.
Am 30.06.2021 wurde schließlich ein Mandat für Verhandlungen mit dem Europäischen Parlament seitens des Ausschusses der Ständigen Vertreter (AStV) angenommen. Sowohl der portugiesische Vorsitz als auch Kommissarin Johansson hoben hervor, dass Europol die Verarbeitung und Analyse von Big Data ermöglicht werden müsse, wobei es gelte, den Datenschutz zu gewährleisten.

2. Richtlinie über die Resilienz kritischer Infrastrukturen

Am 08.06.2021 berichtete der portugiesische Vorsitz, dass der Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen[5] eine Priorität des Vorsitzes gewesen sei, nicht zuletzt vor dem Hintergrund terroristischer Bedrohungen und der COVID-19-Pandemie. Einigkeit bestehe darüber, dass die Richtlinie eng mit der NIS 2-Richtlinie zur Resilienz im Cyberbereich abgestimmt werden müsse. KOM betonte die Bedeutung der Aktualisierung des EU-Resilienzrechtsrahmens und der Kohärenz der Richtlinie mit der NIS 2-Richtlinie. Mit Blick auf fortbestehende Bedenken einiger Mitgliedstaaten aufgrund der Rechtsgrundlage, auf die die Richtlinie gestützt worden sei (Art. 114 AEUV – Binnenmarkt-Kompetenz), führte die KOM erneut aus, dass Aspekte der nationalen Sicherheit nicht betroffen seien und ein funktionierender Binnenmarkt angestrebt werde, sodass die Rechtsgrundlage zutreffend gewählt worden sei. Angesichts der intensiven Arbeit an dem Dossier im EP könne der Trilog bereits Anfang 2022 beginnen.

3. Künstliche Intelligenz

Am 08.06.2021 wurden die innenpolitischen Aspekte des KOM-Vorschlags zur Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-VO)[6] diskutiert. Der portugiesische Vorsitz betonte, dass die Verordnung eigentlich im Wettbewerbsrat durch die für Telekommunikation zuständigen Ministerinnen und Minister behandelt werde, jedoch bedeutende Auswirkungen auf den Bereich der inneren Sicherheit zu erwarten seien. Dies gelte insbesondere für ein grundsätzliches Verbot biometrischer Echtzeit-Identifizierungssysteme mit wenigen Ausnahmen und die Einordnung fast aller im Bereich der Strafverfolgung denkbaren KI-Anwendungen als Hochrisiko-Anwendungen. Kommissarin Johansson erläuterte das Ziel, einen

[4] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2016/794 in Bezug auf die Zusammenarbeit von Europol mit privaten Parteien, die Verarbeitung personenbezogener Daten durch Europol zur Unterstützung strafrechtlicher Ermittlungen und die Rolle von Europol in Forschung und Innovation, COM(2020) 796 final.
[5] Vorschlag für eine Richtlinie des Europäische Parlaments und des Rates über die Resilienz kritischer Einrichtungen, KOM(2020) 829.
[6] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtakte der Union, COM(2021) 206, vom 21.04.2021.

Rechtsrahmen für menschenzentrierte, vertrauenswürdige und ethische KI-Anwendungen zu schaffen, wobei KI-Anwendungen in den Bereichen Strafverfolgung, Migration und Asyl essentiell seien. Je höher jedoch die mit einer KI-Nutzung verbundenen Risiken seien, desto strenger müssten die Regeln sein. Daher seien viele Anwendungen im Bereich der Strafverfolgung in den Hochrisiko-Bereich mit erweiterten Prüf-, Aufsichts-, Transparenz- und Rechenschaftspflichten eingeordnet worden. Dies habe auch zu dem Verbot mit Erlaubnisvorbehalt für biometrische Echtzeit-Identifizierungen geführt, für Massenüberwachungen sei dagegen kein Raum. In der anschließenden Diskussion wurde die KI-VO grundsätzlich begrüßt, allerdings wurde auch das Bedürfnis nach erweiterten Möglichkeiten zur biometrischen Identifizierung in Echtzeit hervorgehoben. Lediglich IRL stimmte dem KOM-Vorschlag in seiner gegenwärtigen Form zu. Alle Teilnehmer begrüßten die Behandlung des Themas beim Innen-Rat. Konsens bestand darüber, dass die von KOM vorgeschlagene Regelungstechnik bedeutende Auswirkungen auf Entwicklung und Nutzung von KI-Anwendungen im Bereich der Inneren Sicherheit haben werde. Ein Vorschlag des portugiesischen Vorsitzes, aufgrund der Auswirkungen auf die innere Sicherheit zunächst eine auf diesen Bereich fokussierte Folgenabschätzung anzustreben, fand breite Zustimmung. POR schlussfolgerte, dass die Belange des Innenministerrates in geeigneter Weise an den Telekom-Rat kommuniziert werden müssten und stellte dafür einen Workshop in Aussicht, an dem Experten aus den Telekom- und Innenbereichen teilnehmen sollten. Insbesondere sollten praktische Beispiele dafür präsentiert werden, wie KI schon heute bei der Polizeiarbeit genutzt werde.

4. Digitale Dimension von Ermittlungen in Fällen von sexuellem Missbrauch von Kindern

Am 08.10.2021 fand eine Aussprache zum Schutz von Kindern vor sexuellem Missbrauch statt. Der slowenische Vorsitz betonte dabei, dass die Bekämpfung des sexuellen Missbrauchs von Kindern eine Priorität der Präsidentschaft sei, die im November im Rahmen eines informellen Ministertreffens weiter erörtert werden solle. Die KOM erneuerte ihre Ankündigung, im Dezember 2021 einen Legislativvorschlag vorzulegen. Alle wortnehmenden Mitgliedstaaten begrüßten die Ankündigung, da es verbindlicher und klarer Regeln, insbesondere für Diensteanbieter, bedürfe. Zahlreiche Mitgliedstaaten sprachen sich zudem für die Einrichtung eines EU-Zentrums zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern aus. SVN betonte abschließend, dass Strafverfolgungsbehörden für eine wirksamere Bekämpfung Zugang zu allen relevanten Daten haben müssten. Auch solle die Nutzung von KI zur Aufdeckung und Verfolgung erwogen werden. Man dürfe sich nicht auf freiwillige Maßnahmen von Diensteanbietern verlassen.

III. Umgang mit COVID-19 und der Kampf gegen Kriminalität

Am 08.06.2021 diskutierte der JI-Rat über das Thema „COVID-19 und der Kampf gegen die Kriminalität: ein Jahr danach“. Im Rahmen der Politikdebatte führten der portugiesische Vorsitz und Kommissarin Johansson zunächst aus, dass sich Verbrecher, insbesondere die Organisierte Kriminalität, schnell an die Gegebenheiten der COVID-19-Pandemie angepasst hätten. Besonderer Handlungsbedarf bestehe bei der Bekämpfung von Cyberkriminalität, Kindesmissbrauch und Produktpiraterie sowie bei der sicheren Kommunikation der Sicherheitsbehörden untereinander, vor allem zum Daten- und Informationsaustausch. Vor diesem Hintergrund kündigte Kommissarin Johansson an, dass unter Bezugnahme auf die im April 2021 vorgelegte Strategie zur Bekämpfung der organisierten Kriminalität 2021-2025 das

bekanntermaßen heikle Thema Vorratsdatenspeicherung wiederaufgegriffen werden solle, zunächst durch ein Ausloten unterschiedlicher Möglichkeiten und juristische Überprüfungen. Die wortnehmenden Mitgliedstaaten (ITA, ESP, FRA, CYP und IRL) berichteten, dass sich die Begehung vieler Straftaten ins Netz verlagert hätten, neben Radikalisierung und Produktpiraterie aber insbesondere häusliche Gewalt und Korruption zugenommen hätten. Vor diesem Hintergrund sei ein entschlossener und gemeinsamer Kampf gegen organisierte Kriminalität von großer Bedeutung, hierzu werde der neue und erweiterte Politikzyklus zur Bekämpfung der organisierten und schweren Kriminalität (EMPACT) 2022-2025 beitragen.

IV. Sonstiges

1. Reform des EU-Katastrophenschutzverfahrens

Am 08.06.2021 informierte der portugiesische Vorsitz über den erfolgreichen Abschluss der Reform des EU-Katastrophenschutzverfahrens[7]. Anders als der ursprüngliche Entwurf sieht die verabschiedete Fassung lediglich eine Festlegung unverbindlicher Krisenresilienzziele durch die KOM in Zusammenarbeit mit den Mitgliedstaaten vor. Zudem wurde die Zuständigkeit der KOM für die Beschaffung von rescEU-Kapazitäten beschränkt auf den Bereich Transport und Logistik sowie in hinreichend begründeten dringenden Fällen materielle Mittel und erforderliche Dienstleistungen.

2. Fonds im Innen-Bereich

Ferner berichtete POR am 08.06.2021 darüber, dass die Verhandlungen zum Fonds für integriertes Grenzmanagement, zum Asyl-, Migrations- und Integrationsfonds (AMIF) sowie zum Fonds für die innere Sicherheit unter dem mehrjährigen Finanzrahmen 2021-2027 erfolgreich abgeschlossen worden seien. Der Fonds für integriertes Grenzmanagement soll danach 6,24 Mrd. EUR umfassen, mit ihm sollen Maßnahmen zum Schutz der Außengrenzen unter Wahrung der Grundrechte, der Aufbau einer gemeinsamen Visapolitik und Maßnahmen zu Gunsten schutzbedürftiger Personen, insbesondere unbegleiteter Minderjähriger, gefördert werden. Der AMIF soll 9,88 Mrd. EUR umfassen und soll zur Stärkung der gemeinsamen Asylpolitik, der Weiterentwicklung von Wegen der legalen Migration, der Integration von Drittstaatsangehörigen, der Bekämpfung irregulärer Migration und zur Erhöhung der Bereitschaft aller Mitgliedstaaten, Verantwortung für die Aufnahme von Migranten zu übernehmen, beitragen. Mithilfe des Fonds für die innere Sicherheit sollen die Verhütung und Bekämpfung von Terrorismus und Radikalisierung, schwerer und organisierter Kriminalität sowie Cyberkriminalität, die Unterstützung und der Schutz der Opfer von Straftaten sowie der Umgang mit sicherheitsrelevanten Vorfällen, Risiken und Krisen gefördert werden. Der Fonds soll mit 1,9 Mrd. EUR ausgestattet sein.

[7] Verordnung (EU) 2021/836 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Änderung des Beschlusses Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union.

LKA BW

Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten

ERSTER SACHSTANDSBERICHT DER BUND-LÄNDER-ARBEITSGRUPPE „BEKÄMPFUNG VON GESCHLECHTSSPEZIFISCH GEGEN FRAUEN GERICHTETEN STRAFTATEN“

STAND 22.10.2021

2021

Baden-Württemberg
LANDESKRIMINALAMT

BEREIT FÜR SICHERHEIT

IMPRESSUM

ERSTER SACHSTANDSBERICHT DER BUND-LÄNDER-ARBEITSGRUPPE „BEKÄMPFUNG VON GESCHLECHTSSPEZIFISCH GEGEN FRAUEN GERICHTETEN STRAFTATEN“

020-1262.1

HERAUSGEBER

Landeskriminalamt Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart

Telefon 0711 5401-0
Fax 0711 5401-3355
E-Mail stuttgart.lka@polizei.bwl.de
Internet www.lka-bw.de

INHALT

1 WESENTLICHE ERGEBNISSE UND GESAMTAUSBLICK

DEFINITION

Wichtiger Ausgangspunkt der Überlegungen für eine bundeseinheitliche Definition von „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ ist das „Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt“ vom 07. April 2011, die sog. Istanbul-Konvention:

„Der Begriff "geschlechtsspezifische Gewalt gegen Frauen" […] bezeichnet eine Form von Gewalt, die gegen eine Frau gerichtet ist, weil sie eine Frau ist, oder die Frauen unverhältnismäßig stark betrifft. Sie unterscheidet sich dadurch von anderen Formen von Gewalt, dass das Geschlecht des Opfers das Hauptmotiv für die […] Gewalttaten ist […] und stellt sowohl die Ursache als auch die Folge ungleicher Machtverhältnisse dar, die auf zwischen Männern und Frauen wahrgenommenen Unterschieden beruhen und zur Unterordnung der Frau in öffentlichen und privaten Bereichen führen.“[1]

Im Einzelnen könnte eine künftige bundeseinheitliche Definition „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ aus zwei Blickwinkeln heraus betrachtet werden und folgende zwei Erscheinungsformen umfassen.

Eine Erscheinungsform wären Taten, bei denen die Motivation des Täters (zumindest auch) im weiblichen Geschlecht des Opfers begründet liegt. Dies sind alle strafbaren Handlungen, die sich gegen Frauen aufgrund von Vorurteilen gegen deren weiblichen Geschlechts richten und daher der sog. „Hasskriminalität“ des Definitionssystems Politisch motivierte Kriminalität[2] zuzurechnen sind. Die Vorurteile äußern sich dabei in einer ablehnenden Einstellung zur Gleichwertigkeit und Gleichberechtigung der Geschlechter im Sinne des Art. 3 Absatz 2 des Grundgesetzes, bezogen auf die gesamte gesellschaftliche Gruppe der Frauen. In der BLAG besteht Übereinstimmung, dass dieses Element der „Hasskriminalität“ in jedem Fall Teil einer zukünftigen bundeseinheitlichen Definition „geschlechtsspezifisch gegen Frauen gerichteter Straftaten“ sein soll.

In der zweiten Erscheinungsform sollten Delikte und Fallgruppen einbezogen werden, die überwiegend zum Nachteil von Frauen begangen werden bzw. in ihrer Ausprägung primär Frauen betreffen, jedoch eine andere Motivation vorliegt oder das Motiv nicht zu ermitteln ist. Diese können grundsätzlich über die Polizeiliche Kriminalstatistik (PKS) abgebildet werden. Es bedarf hier der weiteren Ausgestaltung, unter welchen Voraussetzungen oder Kriterien solche Delikte ohne ein vorurteilsgeleitetes Motiv den „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ zugeordnet werden können.

Die Festlegung auf eine bundeseinheitliche Definition ist Grundlage für die weiteren, vom Auftrag der IMK erfassten Bereiche Statistik, Prävention, Bekämpfungsmaßnahmen und Forschungsbedarfe.

---

[1] *s. Anlage 5, Istanbul-Konvention, Erläuternder Bericht, Art. 3, Ziff. 44, S. 47*

[2] *s. Anlage 6, Definitionssystem Politisch motivierte Kriminalität, Stand: 09.09.20, Gültig: ab 01.01.21, Ziff. 2.4.1, S. 18*

WESENTLICHE ERGEBNISSE UND GESAMTAUSBLICK

STATISTIK

Die PKS wie auch der KPMD-PMK bieten grundsätzlich eine gute Grundlage, um Straftaten, die gegen Frauen gerichtet sind, auszuwerten. Dies umfasst auch vorurteilsgeleitete, gegen das weibliche Geschlecht gerichtete Straftaten der Hasskriminalität. Allerdings werden schon jetzt, auch abhängig von der konkreten Ausgestaltung der o.g. Definition, Optimierungsmöglichkeiten gesehen. In der PKS könnte eine Anpassung des Katalogs der Opferdelikte sinnvoll sein, um z.B. bei Beleidigungs- und Verleumdungsstraftaten eine Erfassung des Opfergeschlechts und damit eine Zuordnung zum Phänomenbereich der geschlechtsspezifischen Straftaten zu ermöglichen. Innerhalb des KPMD-PMK ist eine Ausdifferenzierung des bisherigen Unterthemenfeldes (UTF) „Geschlecht/Sexuelle Identität“ im Sinne von „männlich“, „weiblich“ bzw. „divers“ zu gewährleisten.

PRÄVENTIONS- UND BEKÄMPFUNGSMAßNAHMEN

In Bund und Ländern existiert eine Vielzahl von polizeilichen und nicht-polizeilichen Präventions- und Bekämpfungsmaßnahmen, die bislang nur Einzelaspekte der „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ in den Blick nehmen (z.B. „Häusliche Gewalt“, Sexualdelikte, Hasskriminalität etc.).

FORSCHUNG

Die Facetten der gegen Frauen gerichteten Straftaten werden in der Forschung sehr unterschiedlich intensiv bearbeitet. Einen Forschungsschwerpunkt in diesem Themenbereich bildet die Gewalt gegen Frauen, während sich die Forschung zu Ursachen, Umfang und Auswirkungen frauenfeindlich motivierter Straftaten bislang noch in einem Frühstadium befindet.

GESAMTAUSBLICK

Hinsichtlich der differenzierten Auswertbarkeit der gegen ein bestimmtes Geschlecht gerichteten Hasskriminalität erarbeitet die AG „Qualitätskontrolle PMK“ aktuell einen Vorschlag zur Ausdifferenzierung des UTF „Geschlecht/Sexuelle Identität“ im Sinne von „männlich“, „weiblich“, „divers“.[3] Der Vorschlag befindet sich bereits in der Gremienbefassung und soll im Umlaufbeschlussverfahren auf der 92. Tagung der Kommission Staatsschutz unter TOP 2.3 beschlossen werden. Eine Einführung ist zum 01. Januar 2022 vorgesehen. Damit wäre der erste Teil einer bundeseinheitlichen Definition umgesetzt.

Der zweite Teil einer solchen Definition betrifft Delikte, die überwiegend zum Nachteil von Frauen verübt werden, wenn andere als vorurteilsgeleitete Motive vorliegen oder die Motivation nicht festgestellt werden können und die über die PKS abgebildet werden kann. Hier sind Kriterien bzw. Konstellationen zu erarbeiten, die eine Zuordnung von Delikten und Fallgruppen zu den „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ ermöglichen. Dafür ist in einem ersten

[3] *s. Anlage 7, Sachstandsbericht UAG Statistik, Ziff. 2.1.5.1, S. 8*

Schritt eine Erörterung in der Gesamt-BLAG beabsichtigt und im Weiteren die Einbindung von Expertenwissen aus Wissenschaft und Zivilgesellschaft, der DHPOL und polizeilichen kriminalistisch-kriminologischen Forschungsstellen vorgesehen. Dabei soll auch geprüft werden, ob eine Ausweisung des Geschlechts des Tatopfers bei Beleidigungs- und ähnlichen Delikten die kriminalistische Aussagekraft bei der Darstellung von „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ erhöht und daher angezeigt ist. Es ist geplant, die bundeseinheitliche Begriffsdefinition sowie die Erarbeitung von Fallgruppen, zur aussagekräftigeren Zu- und Einordnung von Delikten als geschlechtsspezifische Taten gegen Frauen zur Herbstsitzung der IMK 2022 zu finalisieren.

Eine Anpassung der PKS erfolgt – analog zum KPMD-PMK – über ein Gremienverfahren unter Beteiligung der Kommission Polizeiliche Kriminalstatistik (KPKS). Änderungen könnten erstmals auf der Frühjahressitzung 2022 beschlossen werden.

Perspektivisch wird empfohlen, ein regelmäßig zu aktualisierendes Lagebild zu „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ zu erstellen, welches sich aus dem KPMD-PMK sowie der PKS speist und die jeweiligen Entwicklungen bewertet. Ein solches Lagebild soll auf Basis der Fallzahlen 2022 im Sommer 2023 erstmals umgesetzt werden.

Die bisher im KPMD-PMK im Themenfeld „Geschlecht/sexuelle Identität“ erfassten Fallzahlen sind außergewöhnlich niedrig. Vor diesem Hintergrund sind entsprechende Informations- und Sensibilisierungsmaßnahmen (Handreichungen, Fallbeispiele) erforderlich, die insbesondere Dienststellen außerhalb des Polizeilichen Staatsschutzes eine wichtige Hilfestellung bei der Ermittlung der Motive und der Zuordnung der Straftaten in der Statistik leisten können.

Die vielschichtige Komplexität des Phänomenbereichs „geschlechtsspezifisch gegen Frauen gerichteter Straftaten“ wird sich im Hinblick auf die zukünftige Erarbeitung von möglichen Präventions- und Bekämpfungsmaßnahmen widerspiegeln und dürfte eine Vielzahl an möglichen Ansätzen bieten. Erst mit der Festlegung auf eine bundeseinheitliche Begriffsdefinition ist eine vollumfassende Ist-Stand Erhebung der derzeit in den Bundesländern und im Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) vorhandenen Präventions- und Bekämpfungskonzepte sinnvoll. Erst dann können enstprechende Ergänzungsbedarfe für mögliche bundesweite Handlungsempfehlungen im Kontext des BLAG-Auftrages formuliert werden.

Mögliche Forschungsbedarfe sollen aufgrund einer systematischen Literaturrecherche und einer ergänzenden Bund-Länder-Abfrage zu themenrelevanten Forschungsprojekten erhoben werden. Auch diese lassen sich erst in Abhängigkeit der Definition im weiteren Verlauf konkret darlegen.

Die im Beschluss der IMK, Ziff. 6,[4] genannte vorgesehene Durchführung einer geschlechtervergleichenden Opferbefragung zu Gewalterfahrungen in Kooperation zwischen dem Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ), dem Bundesministerium des

[4] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 6*

Innern, für Bau und Heimat (BMI) und dem BKA befindet sich derzeit in der Konzeptionierungsphase. Die Datenerhebung bzw. Befragung wird voraussichtlich 2023 beginnen. Der Abschlussbericht soll Anfang 2025 vorliegen.

2 AUFTRAG

AUFTRAG DER IMK

Die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) hat sich auf ihrer 214. Sitzung vom 16. bis 18.06.2021 in Rust unter TOP 24 mit der „Bekämpfung von gezielt gegen Frauen gerichteten Straftaten“ auseinandergesetzt.[5]

Sie zeigte sich besorgt über die feststellbare Gewalt durch männliche Täter gegenüber Frauen und eine sich ausprägende Form der Hasskriminalität, die sich beispielsweise durch schwerste Straftaten in Form von Gewaltanwendungen, aber ebenso durch Drohungen, Beleidigungen oder Nötigungen im digitalen Raum zeigen.[6]

Die IMK misst der nachhaltigen Bekämpfung gezielt gegen Frauen gerichteter Straftaten, wie zum Beispiel Hasskriminalität gegen Frauen, eine besondere Bedeutung zu und beauftragte daher den AK II zur Bearbeitung der folgenden Aufträge mit der Einrichtung der BLAG "Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten"[7]:

- Überprüfung der vorhandenen Strafvorschriften, ob diese besser auf eine schuldangemessene Bestrafung ausgerichtet werden können.[8]
- Entwicklung einer bundeseinheitlichen Begriffsdefinition sowie von Fallgruppen, zur aussagekräftigeren Zu- und Einordnung von Delikten als geschlechtsspezifische Straftaten gegen Frauen.[9]
- Ausdifferenzierung des Kriminalpolizeilichen Meldedienstes Politisch motivierte Kriminalität (KPMD-PMK) im Unterthemenfeld „Geschlecht/sexuelle Identität“ sowie Prüfung einer differenzierteren Erfassung gegen Frauen gerichteter Straftaten durch eine Erweiterung der Polizeilichen Kriminalstatistik (PKS).[10]
- Prüfung von Konzepten und Handlungsempfehlungen zur nachdrücklichen Begegnung solcher Straftaten durch Darstellung bereits bestehender Prävention- und Bekämpfungsmaßnahmen sowie der Formulierung von kurz- und mittelfristig umsetzbaren Präventions- und Bekämpfungsmaßnahmen inklusive eines etwaigen Forschungsbedarfs.[11]

Der AK II wurde darüber hinaus mit der Erstellung eines ersten Sachstandsberichts zur IMK-Herbstsitzung 2021 beauftragt, welcher auch die Ergebnisse der BLAG "Gewalt im familiären Umfeld"

[5] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24*
[6] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 1*
[7] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 2*
[8] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 3*
[9] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 4*
[10] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 5*
[11] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 7*

des AK II[12] sowie gegebenenfalls vorhandene Erkenntnisse bundesweiter und landesweiter Dunkelfeld-Opferbefragungen themenspezifisch mit einbeziehen soll.[13]

AUFTRAG DES IM-LPP BW[14]

Mit Schreiben vom 29.06.2021 wurde das Landeskriminalamt Baden-Württemberg (LKA BW) durch das Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Abteilung 3 – Landespolizeipräsidium (IM-LPP) im Vorgriff auf den Auftrag des AK II mit der Einrichtung der BLAG „Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ beauftragt.[15]

Der Auftrag des IM-LPP umfasste **nicht** die Überprüfung der vorhandenen Strafvorschriften, ob diese besser auf eine schuldangemessene Bestrafung ausgerichtet werden können.[16] Hierzu sagte das IM-LPP zu, die Konferenz der Justizministerinnen und Justizminister um eine Bewertung und die Erarbeitung möglicher Anpassungen zu bitten. Auf dieser Basis sollen dann ggf. weitere, resultierende Maßnahmen geprüft werden.[17]

AUFTRAG DES AK II[18]

Mit Schreiben vom 15.07.2021 beauftragte der Vorsitzende des AK II, der bayrische Landespolizeipräsident Herr Prof. Dr. jur. Wilhelm Schmidbauer, die baden-württembergische Landespolizeipräsidentin Frau Dr. Stefanie Hinz mit der Einrichtung der BLAG „Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten“.[19]

[12] *vgl. Anlage 8, Ergebnisbericht der BLAG „Gewalt im familiären Umfeld“ vom 27.07.2021*

[13] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 8*

[14] *vgl. Anlage 3, Auftrag IM-LPP BW*

[15] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 3*

[16] *ebenda*

[17] *ebenda*

[18] *vgl. Anlage 4, Auftrag AK II*

[19] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 2*

3 AUSGANGSLAGE

In den letzten Jahren rücken Straftaten gegen Frauen immer mehr in den Mittelpunkt gesellschaftlicher Diskussionen, medialer Berichterstattung und politischer Befassung. So verfolgt die Bewegung rund um den Hashtag „#MeToo“ seit 2017 das Ziel, auf das Ausmaß von sexueller Belästigung und sexueller Übergriffe hinzuweisen. Das Thema der „häuslichen Gewalt“ erlebte in Zeiten der häuslichen Isolation aufgrund der Maßnahmen der Bekämpfung der Corona-Pandemie besondere Aufmerksamkeit. Gleichzeitig ist festzustellen, dass die zunehmende Polarisierung der Gesellschaft in Verbindung mit der Digitalisierung zu neuen Formen der (digitalen) Gewalt gegen Frauen führt. Hass und Hetze, auch im Internet, haben in unserer Gesellschaft ein erhebliches Ausmaß angenommen, wobei Frauen von dieser digitalen Gewalt besonders betroffen sind, auch im Kontext neuer ideologischer Phänomene wie etwa der frauenfeindlichen „Incel“-Bewegung („Involuntary celibates“, „Unfreiwillig im Zölibat Lebende“). Diese gesamtgesellschaftlich diskutierten Entwicklungen wurden ausgehend von der Mitunterzeichnung des „Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt“ vom 07. April 2011 durch Deutschland in Istanbul von einem politischen Prozess begleitet. Diese so genannte Istanbul-Konvention gilt nach ihrer Ratifizierung im Jahr 2017 seit dem 01. Februar 2018 im Rang eines Bundesgesetzes. Sie zielt darauf ab, Frauen vor allen Formen von Gewalt zu schützen.[20] Neben dem oben bereits genannten Phänomen der „häuslichen Gewalt“ richtet sich die Istanbul-Konvention insgesamt gegen sog. „geschlechtsspezifisch gegen Frauen gerichtete Gewalt“. Aktuell durchläuft Deutschland den Prozess zur Überprüfung der Einhaltung der Vorgaben der Konvention durch das Expert/innen-Gremium zur Überwachung der Umsetzung der Istanbul-Konvention durch die Vertragsstaaten (GREVIO).

Nachdem bereits vor Inkrafttreten der Istanbul-Konvention verschiedene gesetzgeberische Initiativen umgesetzt wurden (wie das Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen (Gewaltschutzgesetz - GewSchG) im Jahr 2001 oder das 50. Gesetz zur Änderung des Strafgesetzbuches – Verbesserung des Schutzes der sexuellen Selbstbestimmung („Nein heißt nein“) im Jahr 2016) wurden im Zuge der Ratifizierung eine Reihe weiterer Maßnahmen und Gesetzen auf Ebene von Bund, Ländern und Kommunen erlassen, wie das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) (2017), das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (2021) oder das Gesetz zur effektiveren Bekämpfung von Nachstellungen und besseren Erfassung des Cyberstalkings (2021).

Die umfassende Erfassung und tiefergehende Analyse von Gewalttaten gegen Frauen und deren Motivation ist ein aktuell (kriminal)politisch wichtiges Anliegen: Nach der intensiven Auseinandersetzung mit dem Phänomen der „häuslichen Gewalt“, unter anderem im Rahmen der BLAG „Gewalt im familiären Umfeld“ der AG Kripo[21], wird mit dem Beschluss der IMK und der Einrichtung

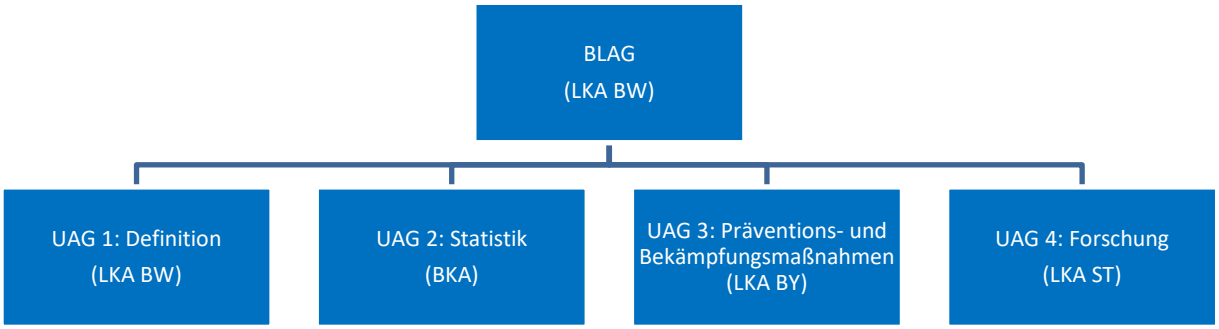
[20] *vgl. Anlage 5, Istanbul-Konvention, Art. 1 Nr. 1 a*

[21] *vgl. Anlage 8, Ergebnisbericht der BLAG „Gewalt im familiären Umfeld“ vom 27. Juli 2021*

dieser BLAG nun der Fokus auf die Bekämpfung „geschlechtsspezifisch gegen Frauen gerichteter Straftaten“ gelegt.

4 AUFBAU DER BLAG

Gem. dem Auftrag des IM-LPP vom 29.06.2021 wurde durch das LKA BW zur Einrichtung der BLAG „Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ am 05.08.2021 die konstituierende Sitzung der BLAG per Videokonferenz einberufen, an welcher die Leitungen der Unterarbeitsgruppen teilnahmen. Im Rahmen dieser Sitzung wurde die folgende Organisationsstruktur der BLAG sowie die Leitung der Unterarbeitsgruppen festgelegt:



5 KORRESPONDIERENDE BEFASSUNGEN ANDERER FACHMINISTERKONFERENZEN UND ARBEITSGRUPPEN

Aktuell befassen sich weitere Fachministerkonferenzen mit verwandten Themen oder Teilaspekten der „Bekämpfung geschlechtsspezifisch gegen Frauen gerichteter Straftaten“. Dies ist zunächst die Konferenz der Gleichstellungs- und Frauenministerinnen und -minister, -senatorinnen und -senatoren der Länder (GFMK), welche die AG „Gewaltschutz“ u. a. mit einer Definition des Begriffs „Femizid“ beauftragt hat.[22] Darüber hinaus befasst sich eine Arbeitsgruppe der Konferenz der Justizministerinnen und Justizminister der Länder (JuMiKo) mit der Verbesserung der justiziellen statistischen Erfassung von Gewalt gegen Mädchen und Frauen.[23] Die Integrationsministerkonferenz (IntMK) befasste sich mit dem Schutz von Frauen gegen Gewalt. Sie plant, gemeinsam mit der Jugend- und Familienministerkonferenz der Länder (JFMK) und der GFMK, ein geeignetes Gremium, wie beispielsweise die BLAG Häusliche Gewalt, mit der Prüfung von melderechtlichen Alternativen zur Vermeidung der Eintragung der „Klaradresse“ im Personalausweis für betroffene Personen zu beauftragen.[24]

Eine strukturierte Form der Zusammenarbeit mit diesen Arbeitsgruppen erfolgt über das Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg (IM BW).

Die Ergebnisse der BLAG „Gewalt im familiären Umfeld“ fanden und finden Eingang in die Arbeit dieser BLAG. Zum jetzigen Zeitpunkt wurde insbesondere deren Herangehensweise an eine Definition einbezogen. Aufgrund der breiten und umfassenden phänomenologischen und deliktischen Ausrichtung des Auftrages der IMK hat die BLAG hinsichtlich der Definition allerdings einen anderen Ansatz verfolgt. Die Einbeziehung der Ergebnisse der BLAG „Gewalt im familiären Umfeld“ erfolgt kontinuierlich im Verlauf der weiteren Projektarbeit.

[22] *vgl. 31. GFMK, 23./24.06.2021, Beschlussniederschrift zu TOP 10.8, Ziff. 2*

[23] *vgl. 91. JuMiKo, 26./27.11.2020, Beschlussniederschrift zu TOP II 10, Ziff. 3*

[24] *vgl. 16. IntMK, 29.04.2021, Beschlussniederschrift zu TOP 3.8, Ziff. 3*

6 DEFINITION

AUSGANGSLAGE

Die Unterarbeitsgruppe Definition befasst sich mit dem in Beschlussziffer 4 des IMK-Beschlusses formulierten Auftrag:

„Die IMK erachtet es als erforderlich, gegebenenfalls unter Berücksichtigung von Expertenwissen aus der Wissenschaft und Zivilgesellschaft, zunächst eine bundeseinheitliche Begriffsdefinition sowie entsprechende Fallgruppen zu entwickeln, die eine noch aussagekräftigere Zu- und Einordnung von Delikten als geschlechtsspezifische Straftaten gegen Frauen in der polizeilichen Erfassung ermöglichen. Diese soll auch Fälle über die Definitionen im KPMD-PMK hinaus, im Rahmen auch gegebenenfalls weiterer Erfassungsmöglichkeiten in der PKS, besonders in den Blick nehmen und damit eine verbesserte Zu- und Einordnung von entsprechenden Delikten ermöglichen. Ziel ist die Sicherstellung einer differenzierteren polizeilichen Erfassung, da aussagekräftige Daten die Grundlage für gezielte Präventions- und Bekämpfungsmaßnahmen bilden.“[25]

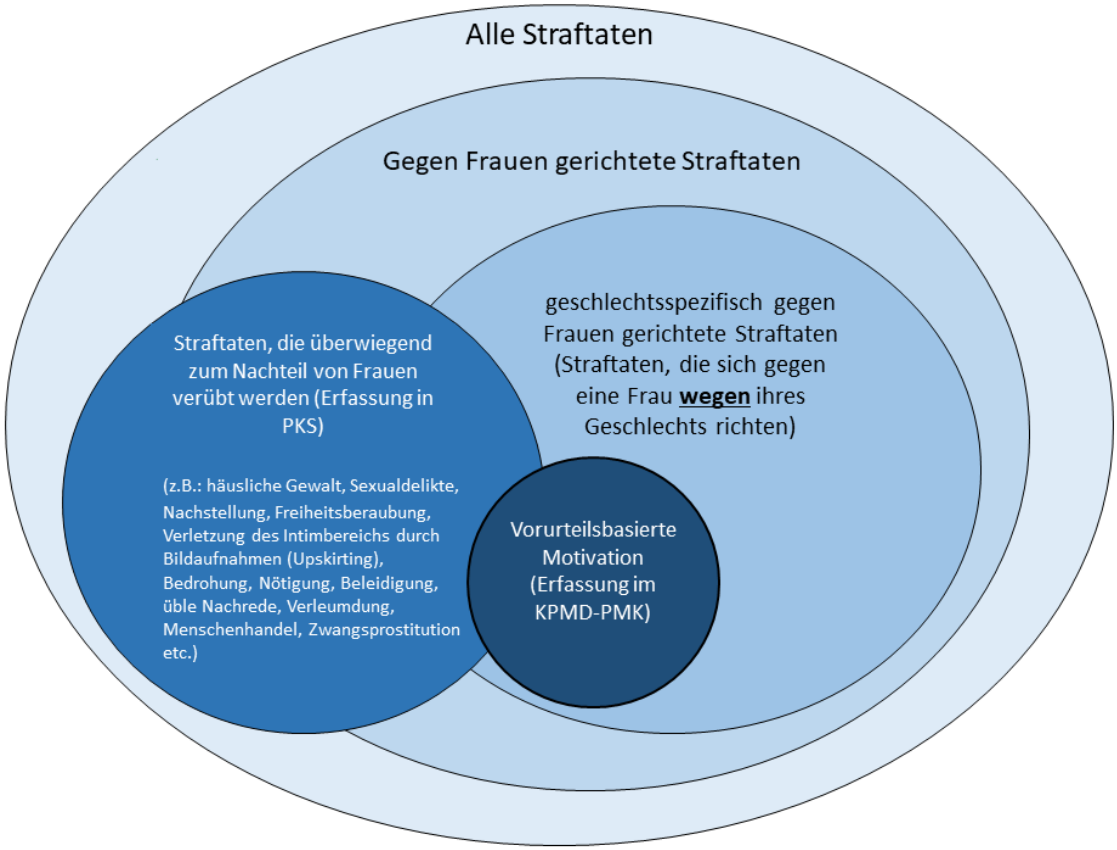
Gegenwärtig existiert keine bundeseinheitliche polizeiliche Definition der „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“. Eine solche Definition soll präzise das Phänomen beschreiben und gleichzeitig eine Abgrenzung von anderen strafbaren Handlungen gegen Frauen ermöglichen. Darüber hinaus sind Anforderungen hinsichtlich Verständlichkeit und Handhabbarkeit für die polizeiliche Praxis zu berücksichtigen. Schließlich soll die Definition eine ausreichende Bestimmtheit für eine statistische Erfassung in den polizeilichen Systemen bieten.

Die UAG Definition tagte zweimal im Videokonferenzformat. Aufgrund des knappen Zeitfensters zwischen der Auftragserteilung und der Abgabe des ersten Sachstandsberichts, welches zudem von der Sommerferienzeit geprägt war, wurde bislang auf die Einbeziehung von Expertenwissen aus Wissenschaft und Zivilgesellschaft verzichtet. Eine entsprechende Einbindung soll perspektivisch im weiteren Verlauf erfolgen.

AKTUELLER SACHSTAND

Die dargestellten komplexen Rahmenbedingungen führten in der UAG Definition zu einem mehrstufigen Prozess, sich einer bundeseinheitlichen Definition der „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ zu nähern. In einem ersten Schritt wurden breit Phänomene, Delikte und mögliche Fallgruppen betrachtet, die generell im Zusammenhang mit der Thematik „Straftaten gegen Frauen“ in der Öffentlichkeit diskutiert werden. In einem zweiten Schritt wurden diese in einer Gesamtschau der polizeilichen Erfassungs- und Statistiksysteme KPMD-PMK und PKS im Sinne von Teilmengen kategorisiert. Das nachfolgende Schaubild verdeutlicht diesen Prozess:

[25] *s. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24*



„Geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ bilden eine Teilmenge der „gegen Frauen gerichteten Straftaten“. Dies korrespondiert mit dem „Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt“ vom 07. April 2011, der sog. Istanbul-Konvention:

„Der Begriff "geschlechtsspezifische Gewalt gegen Frauen" […] bezeichnet eine Form von Gewalt, die gegen eine Frau gerichtet ist, weil sie eine Frau ist, oder die Frauen unverhältnismäßig stark betrifft. Sie unterscheidet sich dadurch von anderen Formen von Gewalt, dass das Geschlecht des Opfers das Hauptmotiv für die […] Gewalttaten ist […] und stellt sowohl die Ursache als auch die Folge ungleicher Machtverhältnisse dar, die auf zwischen Männern und Frauen wahrgenommenen Unterschieden beruhen und zur Unterordnung der Frau in öffentlichen und privaten Bereichen führen.“[26]

Im Einzelnen könnte eine künftige bundeseinheitliche Definition „geschlechtsspezifisch gegen Frauen gerichteter Straftaten“ aus zwei Blickwinkeln heraus betrachtet werden und folgende zwei Erscheinungsformen umfassen:

[26] *s. Anlage 5, Istanbul-Konvention, Erläuternder Bericht, Art. 3, Ziff. 44, S. 47*

1. Beim ersten Bereich wird die Motivation für die Tat in den Mittelpunkt gestellt. Kennzeichnend ist, dass Frauen nicht nur zufällig, sondern wegen ihres Geschlechts[27] aus einer vorurteilsgeleiteten Motivation des Täters heraus Opfer einer Straftat werden.

   In der UAG Definition besteht Einigkeit darüber, dass zu den „geschlechtsspezifisch gegen Frauen gerichteten Straftaten" in jedem Fall solche zu zählen sind, die sich gegen Frauen aufgrund von Vorurteilen gegen deren weibliches Geschlecht oder deren weibliche geschlechtliche Identität richten. Diese Straftaten fallen damit unter die sog. „Hasskriminalität" des Definitionssystems Politisch motivierte Kriminalität, welche wie folgt definiert ist:

   „Hasskriminalität bezeichnet politisch motivierte Straftaten, wenn in Würdigung der Umstände der Tat und/oder der Einstellung des Täters Anhaltspunkte dafür vorliegen, dass sie aufgrund von Vorurteilen des Täters bezogen auf […] Geschlecht/sexuelle Identität […] begangen werden."[28]

   Die „Vorurteile des Täters" äußern sich dabei in einer ablehnenden Einstellung zur Gleichwertigkeit und Gleichberechtigung der Geschlechter. Dies beinhaltet auch ein Über-/ Unterordnungsverhältnis zwischen Mann und Frau im Sinne eines patriarchalischen Verständnisses. Diese Einstellung ist bezogen auf die gesamte gesellschaftliche Gruppe der Frauen.

   Damit sind auch die aktuell diskutierten Phänomene wie misogyner, also frauenfeindlicher „Hass und Hetze" im Internet und in der analogen Welt, antifeministische Straftaten, Straftaten aus kulturell frauenfeindlicher Motivation (z.B. im Namen der „Ehre") oder Taten im Zusammenhang mit sexueller Diskriminierung (z.B. „Body Shaming" oder „Dick Pics") im KPMD-PMK erfassbar, wenn die Motivation des Täters vorurteilsgeleitet gegen das weibliche Geschlecht gerichtet ist.

   Eine Einschränkung, welche konkreten Straftatbestände durch die Motivation des Täters zu „geschlechtsspezifisch gegen Frauen gerichteten Straftaten" qualifiziert werden können, kann nicht vorgenommen werden, da alle mit einer entsprechenden Motivation begangen werden können und demnach als „geschlechtsspezifisch gegen Frauen gerichtete Straftat" zu klassifizieren wären.

   In verschiedenen Konstellationen dürfte zu Beginn der Ermittlungen noch kein eindeutiger Schluss auf die Motivation des Täters möglich sein. Das gilt insbesondere für Fälle mit unbekannten oder noch nicht ermittelten Tatverdächtigen (so genannte ungeklärte Fälle). Es sollte daher im Zuge der Definitionsentwicklung geprüft werden, ob zu der Definition ein Hinweis/eine Erläuterung implementiert werden kann, der/die in solchen Fällen auf die besondere Bedeutung der Opferperspektive bei der Motivermittlung hinweist.

[27] *Dies schließt die vom Täter unterstellte Zugehörigkeit zur Gruppe der Frauen mit ein.*

[28] *s. Anlage 6, Definitionssystem Politisch motivierte Kriminalität, Stand: 09.09.20, Gültig: ab 01.01.21, Ziff. 2.4.1, S. 18*

2. Der zweite Bereich betrachtet Delikte und Fallgruppen unter dem Blickwinkel, dass diese überwiegend zum Nachteil von Frauen begangen werden bzw. die Taten in ihrer Ausprägung primär Frauen betreffen.[29] Es geht dabei um die Frage, ob bzw. unter welchen Voraussetzungen solche Delikte, auch ohne dass ein vorurteilsgeleitetes Motiv vorliegt, ebenfalls den „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ zugeordnet werden können. In der Praxis kann in einem durchaus beträchtlichen Teil dieser Fälle der überwiegend gegen Frauen gerichteten Delikte der Allgemeinkriminalität eine andere Motivlage, als die der zuvor genannten Hasskriminalität des Definitionssystems PMK, vorliegen. In vielen Konstellationen dürfte die Motivation des Täters unklar bleiben, die Umstände der Tat keinen eindeutigen Schluss zulassen und ein Motiv letztendlich nicht zu ermitteln sein. Letzteres liegt regelmäßig bei unbekannten oder noch nicht ermittelten Tätern vor. Hier Kriterien zur Zuordnung dieser Delikte zur Gruppe der „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ zu entwickeln, wird ein weiteres Arbeitspaket der UAG Definition im Fortgang der UAG-Arbeit sein. Die hierfür benötigten Daten dürften in der Polizeiliche Kriminalstatistik (PKS) bereits überwiegend vorliegen, was die Bildung konkreter Fallgruppen erleichtern wird. Diese Fallgruppen sollen als Basis für die weiteren Diskussionen im Rahmen der UAG-Arbeit, unter Hinzuziehung weiterer Akteure aus Wissenschaft und Zivilgesellschaft, ggf. auch der DHPOL und der kriminalistisch-kriminologischen Forschungsstellen des BKA sowie der Länder dienen.

AUSBLICK

Folgende Maßnahmen sind im weiteren Verlauf der Projektarbeit vorgesehen:

Hinsichtlich der differenzierten Auswertbarkeit der gegen ein bestimmtes Geschlecht gerichteten Hasskriminalität erarbeitet die AG „Qualitätskontrolle PMK“ aktuell einen Vorschlag zur Ausdifferenzierung des UTF „Geschlecht/Sexuelle Identität“ im Sinne von „männlich“, „weiblich“, „divers“.[30] Der Vorschlag befindet sich bereits in der Gremienbefassung und soll im Umlaufbeschlussverfahren auf der 92. Tagung der Kommission Staatsschutz unter TOP 2.3 beschlossen werden. Eine Einführung ist zum 01. Januar 2022 vorgesehen. Damit wäre der erste Teil einer bundeseinheitlichen Definition umgesetzt.

Die bisher im KPMD-PMK im Themenfeld „Geschlecht/sexuelle Identität“ erfassten Fallzahlen sind außergewöhnlich niedrig. Vor diesem Hintergrund hält die UAG entsprechende Informations- und Sensibilisierungsmaßnahmen (Handreichungen, Fallbeispiele) für erforderlich, die insbesondere Dienststellen außerhalb des Polizeilichen Staatsschutzes eine wichtige Hilfestellung bei der Ermittlung der Motive und der Zuordnung der Straftaten in der Statistik leisten können.

Bei Delikten, die überwiegend zum Nachteil von Frauen verübt werden, sind Kriterien bzw. Konstellationen zu erarbeiten, die eine Zuordnung von Delikten und Fallgruppen zu den

[29] *vgl. Anlage 5, Istanbul-Konvention, Art. 3 d, S. 5*

[30] *s. Anlage 7, Sachstandsbericht UAG Statistik, Ziff. 2.1.5.1, S. 8*

„geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ ermöglichen, wenn andere als vorurteilsgeleitete Motive vorliegen oder die Motivation nicht festgestellt werden kann. Hierzu beabsichtigt die UAG Definition in einem ersten Schritt eine Erörterung in der Gesamt-BLAG. In einem weiteren Schritt soll die Einbindung von Expertenwissen aus Wissenschaft und Zivilgesellschaft, der DHPOL und polizeilichen kriminalistisch-kriminologischen Forschungsstellen erfolgen. Dabei sollte auch geprüft werden, ob eine Ausweisung des Geschlechts des Tatopfers bei Beleidigungsdelikten die kriminalistische Aussagekraft bei der Darstellung von „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ erhöht und daher angezeigt ist. Es ist geplant die bundeseinheitliche Begriffsdefinition sowie die Erarbeitung von Fallgruppen, zur aussagekräftigeren Zu- und Einordnung von Delikten als geschlechtsspezifische Straftaten gegen Frauen zur Herbstsitzung der IMK 2022 zu finalisieren.

Perspektivisch empfiehlt die UAG Definition, ein regelmäßig zu aktualisierendes Lagebild zu „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ zu erstellen, welches sich aus dem KPMD-PMK sowie der PKS speist und die jeweiligen Entwicklungen bewertet. Ein solches Lagebild soll auf Basis der Fallzahlen 2022 im Sommer 2023 erstmals umgesetzt werden.

7 STATISTIK[31]

AUSGANGSLAGE

In der 214. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) zu TOP 24 wurde unter Beschlussziffer 5 Folgendes beschlossen:

„[Die IMK] sieht zudem das Erfordernis, in einem ersten Schritt im ***Kriminalpolizeilichen Meldedienst*** *[in Fällen] Politisch motivierte Kriminalität (KPMD-PMK), basierend auf der dortigen im Kontext stehenden Definition, Tathandlungen* ***nach den Merkmalen "Geschlecht/sexuelle Identität" weiter auszudifferenzieren****, um damit die* ***bundesweit einheitliche automatisierte Auswertung*** *über die Gewaltkriminalität hinaus, einschließlich beispielsweise Hasspostings, zu optimieren und die Transparenz zu dieser Kriminalität* ***zu verbessern****.*

Sie sieht darüber hinaus die Notwendigkeit zu prüfen, ob und wie eine differenziertere Erfassung gegen Frauen gerichteter Straftaten beispielsweise im Rahmen einer ***möglichen Erweiterung der Polizeilichen Kriminalstatistik*** *sachgerecht erfolgen kann.“*[32]

Am 30.08.2021 fand die erste Sitzung der UAG Statistik statt. Auf Basis von im Vorfeld übersandten Positionspapieren wurden in der Sitzung Inhalte und Vorgehen bzgl. der Zulieferung zum ersten Sachstandsbericht der BLAG besprochen. Festgelegt wurde, dass wegen der parallel laufenden Arbeiten in allen UAGen im ersten Sachstandsbericht zunächst der Ist-Stand der Erfassungen im KPMD-PMK und der PKS dargestellt wird, um einen Überblick zu aktuellen Möglichkeiten und Grenzen zu geben.

AKTUELLER SACHSTAND

Die PKS wie auch der KPMD-PMK bieten gegenwärtig eine gute Grundlage, um zahlreiche Straftaten, die gegen Frauen gerichtet sind, mit „Opfer weiblich“ auszuwerten. Sämtliche Straftaten, die gegen Frauen gerichtet sind (inklusive vorurteilsgeleiteter, gegen das weibliche Geschlecht gerichteter Straftaten der Hasskriminalität[33]), sind bereits in der PKS enthalten.

AUSBLICK

Eine bessere Sichtbarmachung dieser Straftaten in Auswertungen kann über noch festzulegende Fallgruppen erfolgen, die Delikte umfassen, die überwiegend als „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ eingestuft werden können, wie bspw. Sexualdelikte. Des Weiteren kann auch eine Eingrenzung (Fallgruppe) nach weiteren bereits verfügbaren Kriterien in der PKS vorgenommen werden, wie bspw. die Straftatenbegehung im „häuslichen Kontext“[34].

---

[31] *vgl. Anlage 7, Sachstandsbericht UAG Statistik*

[32] *s. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 5*

[33] *Außer den „echten Staatschutzdelikten“.*

[34] *„Häusliche Gewalt beinhaltet alle Formen körperlicher, sexueller oder psychischer Gewalt und umfasst familiäre sowie partnerschaftliche Gewalt. Häusliche Gewalt liegt vor, wenn die Gewalt zwischen Personen stattfindet, die in einer*

Angepasst an den Definitionsvorschlag wären konkrete Inhalte und Auswertungen festzulegen sowie zu prüfen, welche Ergänzungen ggf. erforderlich sind (bspw. erneute Befassung der Kommission Polizeiliche Kriminalstatistik (KPKS) mit dem Thema „Opfererfassung bei Beleidigungs- und Verleumdungsstraftaten“, die sich bereits aufgrund der konkreten Benennung der Hasspostings im Beschluss der IMK abzeichnet).

Vorurteilsgeleitete, gegen das weibliche Geschlecht gerichtete Straftaten der Hasskriminalität können als solche im KPMD-PMK erfasst bzw. über diesen ausgewiesen werden. Die Fälle sind, soweit sie der Allgemeinkriminalität zuzuordnen sind, auch in der PKS registriert. Vor diesem Hintergrund bildet der KPMD-PMK eine gute Grundlage für eine verbesserte Erfassung frauenfeindlich motivierter Straftaten. Ein erster Schritt hierfür ist, entsprechend dem Auftrag der IMK,[35] die weitere Ausdifferenzierung des bisherigen UTF „Geschlecht/Sexuelle Identität“ im Sinne von „männlich“, „weiblich“ bzw. „divers“.

Die bisher erfassten Fallzahlen zeigen die Erforderlichkeit der Erstellung von Fallgruppen/-beispielen und Handreichungen, um eine flächendeckende Erfassung vorurteilsgeleitet gegen Frauen gerichteter Straften auch in der Praxis zu gewährleisten.

Ergänzende Anforderungen in Bezug auf weitere Differenzierungen, die über die „Fallgruppen“

- Vorurteilsgeleitete geschlechtsspezifisch gegen Frauen gerichtete Hasskriminalität
- Häusliche Gewalt (Auswertung „weibliche Opfer“)

sowie

- Straftaten, die in ihrer Ausprägung primär Frauen betreffen (insbes. Sexualstraftaten, Verstümmelung weiblicher Genitalien (Auswertung „weibliche Opfer“))
- Tötungsdelikte (Femizide[36]) und Straftaten gegen die persönliche Freiheit (Zwangsheirat; Menschenhandel zum Zwecke der sex. Ausbeutung (Auswertung „weibliche Opfer“))
- sowie sonstige Auswertungen zu weiblichen Opfern (ggf. mit weiteren Filtersetzungen)

hinausgehen, müssen entsprechend eindeutig und in der Praxis anwendbar definiert und hinsichtlich der Zielsetzung beschrieben werden, um dementsprechend eine fachliche und technische Umsetzung im KPMD-PMK und/oder in der PKS zu prüfen und geeignete Kennzeichnungs- bzw. Differenzierungsmöglichkeiten zu identifizieren.

---

familiären oder partnerschaftlichen Beziehung zusammenwohnen. Sie liegt auch vor, wenn sie unabhängig von einem gemeinsamen Haushalt innerhalb der Familie oder in aktuellen oder ehemaligen Partnerschaften geschieht.“ s. Anlage 8, Ergebnisbericht der BLAG „Gewalt im familiären Umfeld“ vom 27.07.2021, Ziff. 4.2, S. 7

[35] vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 5

[36] Aktuell liegt noch keine bundeseinheitliche Definition zu Femiziden vor. Diese wäre Voraussetzung für eine entsprechende Eingrenzung. Gem. Beschluss der 31. Konferenz der Gleichstellungs- und Frauenministerinnen und -minister, -senatorinnen und -senatoren der Länder (GFMK) am 23./24. Juni 2021 (TOP 10.8) ist vorgesehen, dass sich die AG „Gewaltschutz“ mit der Definition des Begriffs „Femizid“ befassen wird.

8 PRÄVENTION UND BEKÄMPFUNGSSTRATEGIEN[37]

AUSGANGSLAGE

Der Auftrag der IMK sieht unter Beschlussziffer 7 vor,

*„das Erfordernis zu prüfen, welche **Konzepte oder Handlungsempfehlungen** dazu beitragen könnten, der Begehung solcher Straftaten zukünftig noch nachdrücklicher zu begegnen. Dabei erachtet [die IMK] es insbesondere für zielführend,*

*- bereits **vorhandene Präventions- und Bekämpfungsmaßnahmen sowie -schwerpunkte** der Polizeien des Bundes und der Länder **darzustellen** sowie*

*- **kurz- und langfristig** umsetzbare **Präventions- und Bekämpfungsmaßnahmen inklusive etwaigen Forschungsbedarfs** zu **formulieren** und diesbezüglich konkrete Handlungsempfehlungen vorzulegen.“*[38]

Bislang liegt noch keine abschließende Definition zu „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ vor. Eine solche Definition bzw. eine Festlegung auf bestimmte Phänomene oder Fallgruppen ist jedoch Grundlage, um die Komplexität der Gesamtthematik in den Grundzügen zu erfassen, im Zuge der weiteren Bearbeitung geeignete und wirksame Präventions- und Bekämpfungsmaßnahmen gemäß dem Auftrag zu entwickeln und in der Folge effektiv umsetzen zu können.

AKTUELLER SACHSTAND

Polizeiliche Kriminalprävention dient der Vorbeugung von Straftaten. Zu unterscheiden sind dabei Maßnahmen aus den Bereichen universeller, selektiver und indizierter Prävention oder auch der täter-, situations- und opferbezogenen Prävention.

Die vorbeugende Bekämpfung von Straftaten kann sich thematisch mit den Zielen von Kriminalprävention überschneiden, erfolgt jedoch situations- und lagebedingt durch polizeiliche Maßnahmen. Bekämpfungsmaßnahmen können dabei in klassische repressive Tätigkeiten münden.

Ausgehend vom dargestellten Auftragsverständnis kann, nach Sichtung der Präventions- und Bekämpfungsmaßnahmen der an der UAG teilnehmenden Bundesländern zusammenfassend festgestellt werden, dass für den Bereich „Häusliche Gewalt“ umfangreiche Präventions- und Bekämpfungskonzepte der Polizeien der Länder existieren. Der „polizeiliche Blick“ auf dieses Phänomen kann durchaus als umfassend angesehen werden. Explizit zu anderen „geschlechtsspezifisch (gezielt) gegen Frauen gerichteten Straftaten“ dürften in den Bundesländern (außer in einzelnen Deliktsbereichen wie z. B. Sexualdelikten und Hasskriminalität) jedoch bislang wenige konkrete Maßnahmenkonzepte existieren. Wesentliche Aspekte der Thematik wurden allerdings bereits im Vorfeld der BLAG „Bekämpfung von geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ durch

[37] *vgl. Anlage 9, Sachstandsbericht UAG Präventions- und Bekämpfungsmaßnahmen*

[38] *s. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff.7*

das LKA BW im Konzeptpapier „Konzeptionelle Überlegungen zur Gestaltung von Maßnahmen gegen frauenfeindliche Kriminalität“[39] zusammengetragen. Im Rahmen einer UAG-Sitzung im Präsenzformat wurden diese Überlegungen durch alle beteiligten Länder bewertet und im Nachgang durch das LKA BW dementsprechend ergänzt.

Unter den nicht-polizeilichen Präventionsmaßnahmen gibt es eine Vielzahl an Beratungs- und Betreuungsangeboten mit unterschiedlichen Vorgehensweisen im Kontext von „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“. Diese beinhalten beispielsweise täterorientiere, opferorientierte, situative und ganzheitliche Angebote.[40]

AUSBLICK

Der Phänomenbereich „geschlechtsspezifisch gegen Frauen gerichteter Straftaten“ ist umfangreich und vielschichtig. Diese Komplexität wird sich im Hinblick auf die zukünftige Erarbeitung von möglichen Präventions- und Bekämpfungsmaßnahmen widerspiegeln und dürfte eine Vielzahl an möglichen Ansätzen bieten.

Vor diesem Hintergrund wird die UAG Präventions- und Bekämpfungsmaßnahmen in einem nächsten Schritt, mit Vorliegen der Ergebnisse der UAG Definition, einen vollumfassenden Ist-Stand der derzeit in den Bundesländern und im Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) vorhandenen Präventions- und Bekämpfungskonzepte erheben, bewerten und sinnhafte Ergänzungsbedarfe für mögliche bundesweite Handlungsempfehlungen im Kontext des BLAG-Auftrages formulieren.

[39] vgl. Anlage 10, „Konzeptionelle Überlegungen zur Gestaltung von Maßnahmen gegen frauenfeindliche Kriminalität“ vom 18.08.2021

[40] vgl. Anlage 10; „Konzeptionelle Überlegungen zur Gestaltung von Maßnahmen gegen frauenfeindliche Kriminalität“ vom 18.08.2021, Kap. „Projektumfeldanalyse“, Rd.Nr. 475 ff., S. 16

9 FORSCHUNG[41]

AUSGANGSLAGE

Der Auftrag der UAG Forschung ergibt sich aus TOP 24 der Beschlussniederschrift zur 214. IMK. Unter Beschlussziffer 7 erachtet es die IMK für zielführend

*„kurz- und langfristig umsetzbare Präventions- und Bekämpfungsmaßnahmen inklusive etwaigen **Forschungsbedarfs zu formulieren** und diesbezüglich **konkrete Handlungsempfehlungen vorzulegen**“*[42].

Zur Ausgangslage der Arbeit der UAG Forschung lässt sich feststellen, dass die Facetten der gegen Frauen gerichteten Straftaten in der Forschung sehr unterschiedlich intensiv bearbeitet wurden. Während das Phänomen der Gewalt gegen Frauen in der Kriminologie, der Soziologie und der Psychologie sehr intensiv erforscht wird und insbesondere die kriminologische Forschung zur Gewalt gegen Frauen in Partnerschaften eine lange Tradition hat, befindet sich die Forschung zu Ursachen, Umfang und Auswirkungen frauenfeindlich motivierter Straftaten bislang in einem Frühstadium.

AKTUELLER SACHSTAND

Um einen solchen Forschungsbedarf zielführend zu ermitteln, ist eine konkrete Begriffsbestimmung des Phänomenbereichs „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ unabdingbar[43]. Erst daran anknüpfend können der aktuelle Forschungsstand erfasst und etwaige Forschungslücken und Forschungsbedarfe identifiziert werden. Vorab hat die UAG Forschung damit begonnen, Ansatzpunkte der anderen UAGen zu erheben, bei welchen die UAG Forschung im laufenden Prozess die eigenen Handlungsbedarfe sieht.

Die im Beschluss der IMK, Ziff. 6,[44] genannte, vorgesehene Durchführung einer geschlechtervergleichenden Opferbefragung zu Gewalterfahrungen in Kooperation zwischen dem Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ), dem BMI und dem BKA befindet sich derzeit in der Konzeptionierungsphase.

Die zu erarbeitende Definition, z.B. auf Basis von Fallgruppen, wird als rahmenstiftend für eine umfängliche systematische Literaturrecherche betrachtet. Letztere wäre aus Sicht der UAG Forschung dazu geeignet, die formulierte Arbeitsdefinition zu bewerten und Impulse zur Anpassung bzw. Erweiterung zu geben.

Unter Berücksichtigung der Arbeiten der UAG Statistik plant die UAG Forschung, sich zur Formulierung etwaigen Forschungsbedarfs einen Überblick über die bisherige Datenlage zu „geschlechtsspezifisch gegen Frauen gerichteten Straftaten“ zu verschaffen und Aufschluss darüber zu

[41] *vgl. Anlage 11, Sachstandsbericht UAG Forschung*

[42] *s. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 7*

[43] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 4*

[44] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 6*

gewinnen, ob und in welchen Bereichen ggf. Wissenslücken oder Ergänzungsbedarf bei der quantitativen Erfassung des Problembereichs vorliegen. Auch Phänomene, wie die kurz- oder langfristige Zu- oder Abnahme von Delikthäufigkeiten, können insofern Forschungsansätze bieten, als diese zur Identifizierung von Ursachen und Zusammenhängen beitragen können. In Kombination mit der genannten Literaturrecherche wäre es zudem erkenntnisbringend zu überprüfen, ob Unterschiede zwischen den Daten aus PKS bzw. KPMD-PMK und den Erkenntnissen aus der Forschung vorliegen (z.B. Vergleich Hell- und Dunkelfeld).

Hinsichtlich der UAG Präventions- und Bekämpfungsmaßnahmen sieht die UAG Forschung starke Parallelen im Arbeitsprozess, da empirische Forschungsergebnisse eine wichtige Basis für die präventivpolizeiliche Arbeit bilden und die Wirksamkeit präventiver Maßnahmen mittels wissenschaftlicher Evaluation überprüft werden kann. Die in beiden Bereichen notwendige und bereits genannte, umfängliche Literaturrecherche könnte eine erste Möglichkeit zur Zusammenarbeit bieten, welche sich bei Bedarf ausbauen ließe.

AUSBLICK

In der UAG Forschung besteht Konsens darüber, dass die auf der Definition der UAG Definition fußende systematische Literaturrecherche den Grundstein für weitere Arbeitsschritte bildet. Eine solche Recherche soll dem Zweck dienen, Fragen wie die folgenden zu beantworten:

1. Welche Forschungsergebnisse liegen zum Themenfeld „geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ vor? Welche Aspekte und Phänomene wurden bereits umfassend erforscht? Welche Forschungslücken lassen sich identifizieren?
2. Welche theoretischen Ansätze und Forschungsmethoden wurden zum Erkenntnisgewinn genutzt? Unterscheiden sie sich bezüglich ihrer Effektivität bzw. gibt es bezüglich bestimmter Themen zu bevorzugende Designs und Methoden?
3. Welche Ergebnisse liegen in der internationalen Forschungslandschaft vor und inwiefern lassen sie sich in den deutschen Raum übertragen?
4. Gibt es einen bevorzugten Forschungsfokus (z.B. Risikofaktoren der Opfer vs. Motive und Risikofaktoren der Täter) und falls ja, wäre ein Fokuswechsel lohnenswert?

Auf Basis der Antworten zu diesen und möglicherweise weiteren Fragen und in Kooperation mit den anderen UAGen können konkrete Forschungsideen entwickelt werden. Ergänzend zieht die UAG Forschung eine Bund-Länder-Abfrage zu abgeschlossenen bzw. laufenden themenrelevanten Forschungsprojekten in Erwägung. Diese könnte, neben Ergänzungen zur Literaturrecherche, die Chance auf Kooperationen mit bisher in der BLAG nicht involvierten Bundesländern bieten.

Die im Beschluss der IMK, Ziff. 6,[45] genannte vorgesehene Durchführung einer geschlechtervergleichenden Opferbefragung zu Gewalterfahrungen in Kooperation zwischen dem BMFSFJ, dem BMI und dem BKA befindet sich derzeit in der Konzeptionierungsphase. Ende 2021 soll das Ausschreibungsverfahren für die Vergabe der Datenerhebung in die Wege geleitet werden. Im Anschluss folgen Stichprobenziehung, Pretest und Fragebogenprogrammierung. Die Datenerhebung/Befragung wird voraussichtlich 2023 beginnen. Der Abschlussbericht soll Anfang 2025 vorliegen.

[45] *vgl. Anlage 2, Beschlussniederschrift der 214. IMK, TOP 24, Ziff. 6*

10 ANLAGEN

ANLAGE 1: MITGLIEDER DER BLAG

Leitung der BLAG

Sigurd Jäger (Leitung)	LKA Baden-Württemberg
Maren-Sophie Seifermann	LKA Baden-Württemberg
Jan-Niclas Jedinat	LKA Baden-Württemberg

UAG Definition

Sigurd Jäger (Leitung)	LKA Baden-Württemberg
Maren-Sophie Seifermann	LKA Baden-Württemberg
Jan-Niclas Jedinat	LKA Baden-Württemberg
Constanze Schober	LKA Baden-Württemberg
Dr. Constanze Stieper	BMI
Nikolaus Müllershausen	BMI
Tobias Neugebauer	BMI
Heike Lippert	BKA
Frank Passia	BKA
Sarah-Marisa Wegener	LKA Berlin
Simone Klemm	LKA Berlin
Wiro Nestler	LKA Hamburg
Iris Dechant	LKA Hamburg

UAG Statistik

Heike Lippert (Leitung)	BKA
Jna Knauß (Stv. Leitung)	BKA
Ralph Richter	BKA
Frank Passia	BKA

Simon Bildstein	BKA
Dr. Julia Stehle	BKA
Dr. Constanze Stieper	BMI
Nikolaus Müllershausen	BMI
Tobias Neugebauer	BMI
Michael Huber	LKA Baden-Württemberg
Constanze Schober	LKA Baden-Württemberg
Ramona Leis	LKA Baden-Württemberg
Frank Wehen	LKA Bayern
Harald Edtbauer	LKA Bayern
Sarah-Marisa Wegener	LKA Berlin
Simone Klemm	LKA Berlin
Corinna Balke	LKA Berlin

UAG Präventions-/Bekämpfungsmaßnahmen

Silvia Staller (Leitung)	LKA Bayern
Michael Weinzierl (Stv. Leitung)	LKA Bayern
Peter Mehltretter (Stv. Leitung)	LKA Bayern
Christian Sugar	LKA Bayern
Franziska Haase	LKA Bayern
Bettina Rommelfanger	LKA Baden-Württemberg
Frank Buchheit	LKA Baden-Württemberg
Thomas Broy	LKA Hamburg
Andrea Sieverding	LKA Niedersachsen
Christina Georges	LKA Saarland
Melanie Bill	LKA Saarland

UAG Forschung

Liane Hentschke (Leitung)	LKA Sachsen-Anhalt
Dr. Constanze Stieper	BMI
Angela Nienierza	BKA
Nicole Weiß	LKA Baden-Württemberg
Dr. Johannes Luff	LKA Bayern
Simone Rabitz-Suhr	LKA Hamburg
Andrea Sieverding	LKA Niedersachsen
Alexander Gluba	LKA Niedersachsen

ANLAGE 2: BESCHLUSSNIEDERSCHRIFT DER 214. IMK, TOP 24, VOM 16. BIS 18.06.21

ANLAGE 3: AUFTRAG IM-LPP BW VOM 29. JUNI 2021

ANLAGE 4: AUFTRAG AK II VOM 15. JULI 2021

ANLAGE 5: ÜBEREINKOMMEN DES EUROPARATS ZUR VERHÜTUNG UND BEKÄMPFUNG VON GEWALT GEGEN FRAUEN UND HÄUSLICHER GEWALT VOM 7. APRIL 2011 (ISTANBUL-KONVENTION) - ERLÄUTERNDER BERICHT

ANLAGE 6: DEFINITIONSSYSTEM POLITISCH MOTIVIERTE KRIMINALITÄT, STAND: 09.09.20, GÜLTIG: AB 01.01.21

ANLAGE 7: SACHSTANDSBERICHT DER UAG STATISTIK

ANLAGE 8: ERGEBNISBERICHT DER BLAG „GEWALT IM FAMILIÄREN UMFELD“ VOM 27.07.2021

ANLAGE 9: SACHSTANDSBERICHT DER UAG PRÄVENTIONS- UND BEKÄMPFUNGSMAßNAHMEN

ANLAGE 10: „KONZEPTIONELLE ÜBERLEGUNGEN ZUR GESTALTUNG VON MAßNAHMEN GEGEN FRAUENFEINDLICHE KRIMINALITÄT“ VOM 18.08.2021, LKA BADEN-WÜRTTEMBERG

ANLAGE 11: SACHSTANDSBERICHT DER UAG FORSCHUNG

STABSBEREICH GRUNDSATZ/GREMIEN/GEHEIMSCHUTZ (020)

E-Mail stuttgart.lka.stab.gs@polizei.bwl.de

Sigurd Jäger

Telefon 0711 5401-2020

E-Mail sigurd.jaeger@polizei.bwl.de

Maren-Sophie Seifermann

Telefon 0711 5401-2042

E-Mail maren-sophie.seifermann@polizei.bwl.de

Jan-Niclas Jedinat

Telefon 0177 5401-2017

E-Mail jan-niclas.jedinat@polizei.bwl.de