



Bundesministerium  
des Innern  
und für Heimat

POSTANSCHRIFT Bundesministerium des Innern und für Heimat, 10557 Berlin

Mitglied des Deutschen Bundestages  
Frau Anke Domscheit-Berg  
Platz der Republik 1  
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin

POSTANSCHRIFT 10557 Berlin

INTERNET [www.bmi.bund.de](http://www.bmi.bund.de)

DATUM 28. Juli 2023

BETREFF **Schriftliche Frage Monat Juli 2023**  
HIER Arbeitsnummer 7/350

Anlage: -1-

Sehr geehrte Frau Abgeordnete,

auf die mir zur Beantwortung zugewiesene schriftliche Frage übersende ich Ihnen die beigefügte Antwort.

Mit freundlichen Grüßen  
in Vertretung

Johann Saathoff

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin

VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof

Bushaltestelle Berlin Hauptbahnhof

Schriftliche Frage der Abgeordneten Anke Domscheit-Berg  
vom 21. Juli 2023  
(Monat Juli 2023, Arbeits-Nr. 7/350)

---

Frage

*Wie lautet der aktuelle Umsetzungsstand der in der Cybersicherheitsagenda formulierten Maßnahmen und Ziele für die 20. Legislaturperiode (bitte je Maßnahme und Ziel den aktuellen Stand anführen) und wann plant die Bundesregierung die von ihr weiterentwickelte, sowie im Einklang mit der Nationalen Sicherheitsstrategie stehende, Cybersicherheitsstrategie zu veröffentlichen?*

Antwort

Hinsichtlich des aktuellen Umsetzungsstands der Cybersicherheitsagenda wird auf die Anlage verwiesen.

Im Koalitionsvertrag wurde vereinbart, dass die Cybersicherheitsstrategie für Deutschland 2021 weiterentwickelt wird. Der Prozess dauert an.

## Umsetzungsstand: Cybersicherheitsagenda

### 1. Cybersicherheitsarchitektur modernisieren und harmonisieren

Nr.	Bezeichnung	Umsetzungsstand
1.1	Ausbau des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu einer Zentralstelle im Bund-Länder-Verhältnis	In Umsetzung
1.2	Anpassung der Zuständigkeitsverteilung im Bereich der Gefahrenabwehr im Cyberraum	In Umsetzung
1.3	Weiterentwicklung der Nationalen Cybersicherheitsstrategie für Deutschland 2021	In Umsetzung
1.4	Fortentwicklung des Nationalen Cyberabwehrzentrums	In Umsetzung
1.5	Stärkung des Nationalen Cyber-Sicherheitsrates	In Umsetzung
1.6	Unabhängigere Aufstellung des BSI	In Umsetzung

## 2. Cyberfähigkeiten und digitale Souveränität der Sicherheitsbehörden stärken

Nr.	Bezeichnung	Umsetzungsstand
2.1	Erstellen einer umfassenden Digitalisierungsstrategie für das Bundesamt für Verfassungsschutz (BfV)	In Umsetzung
2.2	Modernisierung der IT-Infrastruktur im BfV	In Planung
2.3	Fortentwicklung der Cyberfähigkeiten des BfV und deren Nutzbarmachung im Verfassungsschutzverbund, insbesondere Modernisierung von <ul style="list-style-type: none"> <li>• Recherche-Tools zur Aufklärung von Extremismus in sozialen Medien sowie Datenhaltungs- und Analysesystemen bzw. –tools in der Aufklärung und Früherkennung staatlich gesteuerter Cyberangriffe</li> </ul>	In Planung
2.4	Verbesserte Befugnisse zur Aufklärung technischer Sachverhalte bei Cyberangriffen fremder Mächte	In Planung
2.5	Stärkung und Ausbau der Zentralstellenfunktion des BfV im Verfassungsschutzverbund	In Planung
2.6	Ausbau und Modernisierung der Ermittlungsfähigkeiten und -instrumente des BKA und der Bundespolizei im digitalen Raum in den Bereichen Automotive IT, Internet der Dinge und Verschlüsselung sowie bei der polizeilichen Nutzung Künstlicher Intelligenz	In Planung (für BKA)
2.7	Etablierung eines wirksamen Schwachstellenmanagements, inklusive Installation der behördlichen Prozesse	In Umsetzung
2.8	Schaffung einer gesetzlichen Grundlage für die ZITiS	In Umsetzung
2.9	Ausbau der ZITiS als zentraler Dienstleister für die Sicherheitsbehörden sowie Auf- und Ausbau eigener nationaler Entwicklungsfähigkeiten und Bewertungskompetenzen bei der ZITiS.	In Planung

### 3. Cybercrime und strafbare Inhalte im Internet bekämpfen

Nr.	Bezeichnung	Umsetzungsstand
3.1	Weiterer Ausbau der Abteilung Cybercrime beim BKA	In Umsetzung
3.2	Ausbau der zentralen Kompetenz- und Service-Dienstleistungen des BKA zur Bekämpfung von Cybercrime	In Planung
3.3	Stärkung der internationalen Zusammenarbeit des BKA im Bereich Cybercrime, u.a. im Rahmen internationaler Counter-Ransomware-Initiativen	In Umsetzung
3.4	Förderung eines EU-weiten Rechtsrahmens zur Verhinderung und Bekämpfung des sexuellen Missbrauchs von Kindern, dabei insbesondere Verhinderung der Verbreitung von Kindesmissbrauchsdarstellungen im Internet	In Umsetzung
3.5	Entwicklung einer nationalen Strategie zur Bekämpfung der sexuellen Gewalt gegen Kinder	In Planung
3.6	Erstellung eines jährlichen Bundeslagebildes „Sexuelle Gewalt gegen Kinder“	für 2022 abgeschlossen (geplante Veröffentlichung Ende August / Anfang September), für 2023 in Planung
3.7	Personelle und technische Stärkung des BKA bei der Bekämpfung der sexuellen Gewalt gegen Kinder	In Planung
3.8	Erstellung eines zentral durch das BKA koordinierten und bundesweit abgestimmten Melde- und Löschprozesses bei Missbrauchsdarstellungen im Internet.	In Umsetzung
3.9	Intensivere Bekämpfung strafbarer, insbesondere rechtsextremistischer Internetinhalte, u.a. durch Stärkung vorhandener Strukturen beim BKA	In Umsetzung

Nr.	Bezeichnung	Umsetzungsstand
3.10	Ausbau der Ermittlungsfähigkeiten der Bundespolizei im Phänomenbereich Cyberkriminalität durch personelle und technische Stärkung	In Umsetzung
3.11	Konsequenter Ausbau der ZITiS, um digitale Ermittlungswerkzeuge für die Sicherheitsbehörden zur Stärkung der Auswerte- und Analysefähigkeiten im Kampf gegen Cybercrime zu entwickeln.	In Umsetzung

#### 4. Cybersicherheit der Behörden des Bundes stärken

Nr.	Bezeichnung	Umsetzungsstand
4.1	Stärkere gesetzliche Verankerung der Informationssicherheit und Umsetzung eines Verstärkungsprogramms für die Cybersicherheit des Bundes mit der Einrichtung eines Chief Information Security Officers für den Bund (CISO BUND) und eines Kompetenzzentrums zur operativen Sicherheitsberatung des Bundes	In Planung
4.2	Etablierung des Grundsatzes „security by design and by default“ in der Bundesverwaltung	In Planung
4.3	Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und -Systemen für sichere Kommunikation sowie Investition in Quantencomputing und Post-Quanten-Kryptografie	In Planung
4.4	Investition in Quantencomputing beim BSI zur Gewährleistung der sicheren Regierungskommunikation	In Planung
4.5	Steigerung der Hochverfügbarkeit der Rechenzentren des Bundes	In Planung
4.6	Weiterentwicklung des Informationssicherheitsmanagements des Bundes	In Planung

## 5. Cyber-Resilienz Kritischer Infrastrukturen stärken

Nr.	Bezeichnung	Umsetzungsstand
5.1	Förderung von Investitionen für Cyber-Resilienz-Maßnahmen in KMU, die dem KRITIS-Sektor angehören	In Planung
5.2	Einrichtung von Awareness und Cyber-Resilienz-Projekten, die vom BSI und von externen Dienstleistern angeboten werden	eingestellt
5.3	Berücksichtigung der Sicherheit von IT-Lieferketten im Rahmen der gesetzlichen KRITIS Regulierung	In Umsetzung
5.4	Prüfung der Etablierung sektorspezifischer CERTs für KRITIS-Betreiber und enge Anknüpfung an das BSI-Lagezentrum	In Umsetzung

## 6. Schutz ziviler Infrastrukturen vor Cyberangriffen

Nr.	Bezeichnung	Umsetzungsstand
6.1	Aufbau eines BSI Information Sharing Portals (BISP)	In Planung
6.2	Konzeption und initialer Aufbau eines zivilen Cyberabwehrsystems (ZCAS)	eingestellt



## 7. Digitale Souveränität in der Cybersicherheit stärken

Nr.	Bezeichnung	Umsetzungsstand
7.1	Stärkung der deutschen Cybersicherheitsforschung zur Erhöhung der Resilienz bei existentiellen Bedrohungen	In Planung
7.2	Förderung der Digitalen Souveränität insbesondere mit Blick auf die Kommunikationstechnologien 5G/6G	In Umsetzung
7.3	Erweiterungen der Prüfmöglichkeiten des BMI im Hinblick auf die Vertrauenswürdigkeit von Herstellern, die sogenannte „kritische Komponenten“ für KRITIS-Betreiber bereitstellen (zum Beispiel im Energie-, Gesundheits- oder Finanzwesen)	In Planung
7.4	Verstärkte Beauftragung von innovativen Forschungsvorhaben auf der Grundlage von (projizierten) Anwendungsfällen der Sicherheitsbehörden und der Cyberverteidigung (Agentur für Innovation in der Cybersicherheit GmbH)	eingestellt (im Hinblick auf „ <u>Verstärkte</u> Beauftragung“)

## 8. Krisenfeste Kommunikationsfähigkeit schaffen und Sicherheit der Netze ausbauen

Nr.	Bezeichnung	Umsetzungsstand
8.1	Modernisierung der Weitverkehrsnetze gemäß der „Netzstrategie 2030 für die öffentliche Verwaltung“	In Planung / nicht möglich
8.2	Zentrale Unterstützung der Behörden bei der Einführung von IPv6 gemäß der „Netzstrategie 2030 für die öffentliche Verwaltung“	In Umsetzung
8.3	Einführung eines zentralen Videokonferenzsystems für die Bundesverwaltung	eingestellt
8.4	Modernisierung des Digitalfunknetzes für Behörden und Organisationen mit Sicherheitsaufgaben (Sprachkommunikation)	In Umsetzung
8.5	Erweiterung des Digitalfunknetzes für die Behörden und Organisationen mit Sicherheitsaufgaben (Datenkommunikation)	In Umsetzung