Deutscher Bundestag **Drucksache 21/5456**

21. Wahlperiode 16.04.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Ayse Asar, Dr. Andrea Lübcke, Claudia Müller, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 21/5183 –

Fortführung des Forschungsrahmenprogramms der Bundesregierung zur Cybersicherheit

Vorbemerkung der Fragesteller

Die fortschreitende Digitalisierung durchdringt alle Lebensbereiche und schafft neben Chancen auch neue Abhängigkeiten und Verwundbarkeiten. Sie ist von großer Bedeutung für Bürgerinnen und Bürger, Unternehmen, staatliche Behörden sowie Forschungseinrichtungen. Die Gefahren reichen von Datenmissbrauch und digitaler Erpressung über die Verbreitung von Desinformation und Spionage bis hin zu Sabotage von kritischer Infrastruktur. Im Jahr 2024 verursachten Datendiebstahl und Industriespionage einen wirtschaftlichen Schaden von rund 267 Milliarden Euro (https://de.statista.com/themen/2371/internetkriminalitaet-in-deutschland/#topicOverview). Da sich Angriffsmethoden stetig weiterentwickeln und neue Technologien wie Künstliche Intelligenz zusätzliche Risiken bringen, wächst der Handlungsdruck weiter. Dies erfordert eine unabhängige, gut ausgestattete IT-Sicherheitsforschung, die nur durch eine solide und langfristige Finanzierung gesichert werden kann. Das vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) geförderte Forschungsrahmenprogramm „Digital. Sicher. Souverän.“ läuft im Jahr 2026 aus. Die Bundesregierung hat ein erstes Eckpunktepapier (Cybersicherheit – Forschungspolitische Impulse) für ein Nachfolgeprogramm vorgelegt; die Veröffentlichung des Nachfolgeprogramms ist jedoch erst für das erste Quartal 2027 geplant. Nach Ansicht der Fragestellerinnen und Fragesteller könnte die Entwicklung elementarer Forschungsergebnisse zu neuen IT-Sicherheitstechnologien gefährdet werden, sollte das Nachfolgeprogramm nicht rechtzeitig und mit klarer Zielsetzung auf- bzw. umgesetzt werden.

1. Mit welchem Fördervolumen plant die Bundesregierung für das Fortsetzungsprogramm zur Cybersicherheit in den kommenden Jahren (bitte jährliches Fördervolumen für den gesamten Förderzeitraum aufgeschlüsselt angeben) – auch vor dem Hintergrund, dass die IT-Sicherheit explizit mit in das 500-Mrd.-Euro-Sondervermögen aufgenommen wurde?

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Forschung, Technologie und Raumfahrt vom 16. April 2026 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

2. Wie stellt die Bundesregierung die finanzielle Verstetigung der IT-Sicherheitsforschung über das Jahr 2026 hinaus sicher, und welche Rolle spielen dabei Mittel aus dem Kernhaushalt im Vergleich zu Mitteln aus etwaigen Sondervermögen oder zweckgebundenen Fonds (z. B. Klima- und Transformationsfonds)?

Die Fragen 1 und 2 werden im Zusammenhang beantwortet.

Die IT-Sicherheitsforschung ist bereits seit langem fest im Haushalt des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR, Epl. 30 des Bundeshaushalts) verankert und konnte insbesondere durch das letzte Konjunkturpaket verstärkt werden. Aktuell ist für das Fortsetzungsprogramm eine Laufzeit von 2027 bis 2032 vorgesehen, und darin unter der Annahme einer Fortschreibung der bestehenden Finanzplanung ein Bewilligungsvolumen für Forschungsvorhaben von voraussichtlich ca. 700 Mio. Euro aus dem Epl. 30 und ca. 200 Mio. Euro aus dem Sondervermögen Investitionen und Klimaschutz (SVIK). Damit leistet die IT-Sicherheitsforschung einen wesentlichen Beitrag zur Umsetzung der Hightech Agenda Deutschland.

Zusätzlich fördert die Bundesregierung die Cybersicherheitsforschung über die institutionelle Förderung des CISPA Helmholtz-Zentrums für Cybersicherheit, des ATHENE Nationalen Forschungszentrums für angewandte Cybersicherheit sowie der dort beteiligten und weiterer Institute der Fraunhofer-Gesellschaft, des KASTEL – Institut für Informationssicherheit und Verlässlichkeit des Karlsruher Instituts für Technologie und der Max-Planck-Gesellschaft, insbesondere am Max-Planck-Institut für Sicherheit und Privatsphäre Bochum.

3. Wie plant die Bundesregierung, einen „nahtlos[en]“ (Cybersicherheit – Forschungspolitische Impulse, S. 2) Anschluss zwischen dem Ende des aktuellen Forschungsrahmenprogramms und dem Beginn des geplanten Nachfolgeprogramms sicherzustellen?

4. Zu welchem Datum plant die Bundesregierung den Förderbeginn des Nachfolgeprogramms?

Die Fragen 3 und 4 werden im Zusammenhang beantwortet.

Das aktuelle Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ läuft Ende des Jahres 2026 aus. In der Nachfolge ist ein neues Forschungsprogramm der Bundesregierung zur Cybersicherheit ab dem Jahr 2027 gegenwärtig in Vorbereitung (Initiativ- und Entwicklungsphase). Die Kabinettbefassung ist im ersten Quartal des Jahres 2027 vorgesehen. Parallel werden bereits die ersten Fördermaßnahmen konzipiert. Der Förderbeginn ist im Laufe des Jahres 2027 vorgesehen. Die „Agenda Cybersicherheitsforschung“ ergänzt bereits seit Ende des Jahres 2022 das auslaufende Forschungsrahmenprogramm. Durch diese Elemente ist ein nahtloser Übergang zwischen den Programmen sichergestellt.

5. Welche alternativen Maßnahmen evaluiert die Bundesregierung zur Unterstützung der Forschung im Bereich IT-Sicherheit, und mit welchem Gesamtfördervolumen werden diese umgesetzt?

Im Rahmen der in der Initiativphase durchzuführenden ex-ante Evaluation erfolgt eine vorausschauende Bewertung des neuen Forschungsprogramms. Ein Bestandteil dieser Evaluation ist eine Alternativenprüfung, bei der untersucht wird, ob das angestrebte Ziel durch alternative Maßnahmen erreicht werden kann. Die ex-ante Evaluation befindet sich derzeit in Vorbereitung.

Die seit dem Jahr 2020 etablierte Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) vergibt Forschungsprojekte mit Fokus auf Cybersicherheit. Sie reagiert auf die Bedarfe der Sicherheitsbehörden. Dies kann als ergänzendes Instrument gesehen werden. Es erfolgt jedoch keine Forschungsförderung, sondern eine Beauftragung im Vergabeverfahren. Für weitere Informationen zur Cyberagentur wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 21/3729 verwiesen.

6. Welche Expertinnen und Experten, Forschungseinrichtungen und Forschungsgesellschaften und welche Vertreterinnen und Vertreter von Unternehmen, Verbänden oder Beratungsgesellschaften hat die Bundesregierung bereits in den Prozess der Entwicklung des Nachfolgeprogramms zur Cybersicherheit einbezogen, und welche weiteren Akteure wird sie in Zukunft involvieren?

In der aktuellen Initiativphase zur Erarbeitung des künftigen Forschungsprogramms zur Cybersicherheit sind rund 400 Expertinnen und Experten aus Wissenschaft, Wirtschaft, Politik und Zivilgesellschaft eingebunden. In der darauffolgenden Entwicklungsphase wird ein Beirat die inhaltliche Erarbeitung des Programms begleiten. Die Zusammensetzung des Beirats befindet sich derzeit in Abstimmung. Zudem sind Abstimmungen mit den Ressorts, betroffenen nachgeordneten Behörden und den Ländern vorgesehen.

7. Inwiefern plant die Bundesregierung, die Schwerpunkte der neuen Forschungsförderung am aktuellen Programm „strategisch und nachhaltig neu“ (Cybersicherheit – Forschungspolitische Impulse, S. 2) auszurichten, insbesondere im Hinblick darauf, dass Künstliche Intelligenz und Quantentechnologien, wie etwa die Post-Quanten-Kryptografie, im bestehenden Forschungsrahmenprogramm bereits schwerpunktmäßig gefördert wurden?

Geopolitische Veränderungen, verschärfte Sicherheitslagen und neue technologische Entwicklungen erfordern eine kontinuierliche Überprüfung und Anpassung der forschungspolitischen Ziele und Maßnahmen der Bundesregierung im Bereich der Cybersicherheitsforschung. Die hochdynamische Entwicklung von künstlicher Intelligenz und Quantentechnologien bietet gleichzeitig neue Sicherheitslösungen, aber auch neue Angriffsflächen und -vektoren. Von besonderer Bedeutung für die Cybersicherheit im Quantenzeitalter wird die abhörsichere Quantenkommunikation sein. Ohne strategische und langfristige Förderung würde die Forschung hinter die globale Entwicklung von Abwehr- und Angriffstechnologien zurückfallen. Mit dem künftigen Forschungsrahmenprogramm sollen zudem Maßnahmen für gesellschaftliche Cyberresilienz sowie der effiziente und wirkungsvolle Transfer von neuen Sicherheitslösungen aus der Forschung in die Anwendung verstärkt und strukturell verankert werden.

8. Plant die Bundesregierung im künftigen Forschungsrahmenprogramm auch einen Schwerpunkt zur Abwehr hybrider Bedrohungen und Desinformationen?

Hybride Angriffe und Bedrohungslagen verbinden Cyberoperationen, Informationsmanipulation und Sabotage und gefährden damit sowohl staatliche Handlungsfähigkeit als auch demokratisches Vertrauen. Die Abwehr hybrider Bedrohungen und von Desinformationen wird daher ein wichtiger Schwerpunkt im künftigen Forschungsprogramm sein.

9. Wie plant die Bundesregierung, das Nachfolgeprogramm zur Cybersicherheit mit der nationalen Cybersicherheitsstrategie sowie der „Agenda Cybersicherheitsforschung“ zu verzahnen, und wie werden Doppelstrukturen beim Bundesministerium für Forschung, Technologie und Raumfahrt und bei anderen Bundesministerien vermieden?

Die Cybersicherheitsstrategie bildet den Rahmen für das strategische Handeln der Bundesregierung im Bereich Cybersicherheit für die kommenden Jahre. Die derzeitige Strategie wird aktuell weiterentwickelt. Sie wird einen Maßnahmenkatalog enthalten, der verschiedene Bereiche der Cybersicherheit breit abdeckt. Sowohl in der derzeit gültigen als auch in der kommenden Strategie wird Cybersicherheitsforschung thematisiert. Insbesondere vor dem Hintergrund der Anforderungen der NIS2-Richtlinie an Nationale Cybersicherheitsstrategien, unter anderem die Förderung und Integration fortgeschrittener Technologien und die Unterstützung von Hochschul- und Forschungseinrichtungen, wird Cybersicherheitsforschung ein verpflichtender Bestandteil der neuen Strategie werden. In die Erarbeitung der Cybersicherheitsstrategie der Bundesregierung sind alle Ressorts involviert, sodass Doppelstrukturen vermieden werden.

10. Inwieweit sieht die Bundesregierung inhaltliche Schnittmengen zwischen den im Eckpunktepapier des Forschungsprogramms für Cybersicherheit gesetzten Schwerpunkten und den Forschungsprogrammen der „Agentur für Innovation in der Cybersicherheit“?

11. Inwiefern werden das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS), die Bundesagentur für Sprunginnovationen, die Agentur für Innovation in der Cybersicherheit oder auch die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) in die Entwicklung der im Rahmen des Forschungsprogramms Cybersicherheit vorgesehenen Transfermaßnahmen und Forschungsprojekte eingebunden, und wie erfolgt die Abstimmung mit diesen Behörden und Organisationen?

Die Fragen 10 und 11 werden im Zusammenhang beantwortet.

Die Erarbeitung des künftigen Forschungsrahmenprogramms erfolgt in enger Abstimmung mit den Ressorts sowie den nachgeordneten Behörden. Während der Laufzeit des Programms werden die Ressorts sowie die nachgeordneten Behörden themenbezogen und bedarfsgerecht eingebunden z. B. über Ressortabstimmungen, die Beteiligung an Fachgesprächen und -beiräten, Begutachtungen und Evaluationen sowie als Partner in Transfer- und Forschungsprojekten. Das BMFTR beteiligt insbesondere das Bundesministerium des Innern (BMI) über den üblichen Weg der Ressortabstimmung. Das BMI bindet dabei die relevanten Behörden (BSI, Zitis) ein.

Die Bundesregierung verfolgt mit dem Eckpunktepapier des Forschungsprogramms für Cybersicherheit wie auch dem Forschungsprogramm der Cyberagentur das gemeinsame Ziel der Sicherung der technologischen Souveränität und Cyberresilienz Deutschlands im digitalen Raum. Die Forschungsprogramme der Cyberagentur weisen daher thematische Schnittmengen mit den Schwerpunkten des Programms der Bundesregierung zur Cybersicherheitsforschung auf. Dabei decken die von der Cyberagentur unterhaltenen Forschungsprogramme Bedarfe der Sicherheitsbehörden im Kontext der Cybersicherheit zur Sicherung der Äußeren und Inneren Sicherheit. Zur Verzahnung dieser Maßnahmen und zur Vermeidung von Redundanzen erfolgt eine Abstimmung zwischen dem BMFTR und der Cyberagentur über deren Beteiligungsführung im BMI und Bundesministerium der Verteidigung.

12. Welche Erkenntnisse hat die Bundesregierung aus der Evaluation des auslaufenden Programms „Digital. Sicher. Souverän.“ gewonnen, und wie fließen diese konkret in künftige Planungen ein?

Nach Abschluss des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ ist eine ex-post-Evaluation vorgesehen, die die erzielten Ergebnisse, die Wirkung (Impact) und die Effizienz des Mitteleinsatzes bewertet. Die Ergebnisse werden in die kontinuierliche Optimierung und Adaption des künftigen Programms sowie der konkreten Ausgestaltung von Fördermaßnahmen während der Programmlaufzeit einfließen. Einfließen werden ebenfalls die Erkenntnisse aus dem externen ex-post-Evaluationsbericht des Vorgängerprogramms „Selbstbestimmt und sicher in der digitalen Welt 2015 – 2020“ aus dem Juli 2024. Darin wurde der Aufbau der nationalen Cybersicherheits-Forschungszentren CISPA, ATHENE und KASTEL aus der Projektförderung hervorgehoben; die Rolle der institutionellen Förderung der Cybersicherheitsforschung wird in künftigen Planungen berücksichtigt. Auch die Ausgründungsförderung wurde positiv evaluiert, ebenso die hohe Vernetzungs- und Konzentrationswirkung der Förderung, die Auswirkungen auf den gesellschaftlichen Dialog und die Qualifizierung von wissenschaftlichen Nachwuchskräften.

13. Welche Erkenntnisse liegen der Bundesregierung darüber vor, wie viele der im Förderzeitraum von 2021 bis 2026 durch das Programm „Digital. Sicher. Souverän.“ geförderten Projekte bereits in die Anwendung überführt wurden (bitte nach Anwendungsbereichen aufschlüsseln)?

Das BMFTR fördert im genannten Programm weit überwiegend vorwettbewerbliche Verbundvorhaben mit einer durchschnittlichen Laufzeit von drei bis vier Jahren. Für einen Transfer in konkrete Anwendungen ist üblicherweise eine darauffolgende Entwicklungsphase hin zur Marktreife nötig, die erneut mehrere Jahre dauern kann. Insbesondere aus der Fördermaßnahme StartUpSecure lassen sich bereits einige Beispiele für einen erfolgreiche 1:1 Überführung von Forschungsergebnisse in marktfähige Produkte nennen:

– Der Consenter ist der bundesweit erste offiziell anerkannte Dienst für Einwilligungsmanagement, der Cookie-Banner im Browser nach den Entscheidungen der Nutzer automatisch und rechtsverbindlich beantwortet. Aus staatlich geförderter Spitzenforschung wurde eine regulatorische Innovation, die Bürgerinnen und Bürger direkt entlastet.
– Die technologischen Grundlagen für das sogenannte Confidential Computing wurden in marktfähigen Produkten verankert und unterstützen den öffentlichen Sektor und privatwirtschaftliche Unternehmen bei der sicheren Cloud-Nutzung.
– Aus der Forschung im Bereich der Quantenkommunikation sind erste kommerzielle Lösungen für eine abhörsichere Kommunikation entstanden.

14. Welche Erkenntnis liegt der Bundesregierung darüber vor, inwiefern bilateralen Forschungsmaßnahmen und Forschungsinitiativen durch das Programm „Digital. Sicher. Souverän.“ ausgebaut und etabliert werden konnten, insbesondere hinsichtlich beteiligter Partnerländer und Institutionen?

Im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“ wurden bilaterale Forschungsvorhaben mit Institutionen aus Wissenschaft und Wirtschaft aus Frankreich im Bereich

der privatheitsfördernden Technologien gefördert. Für innereuropäische Kooperationsvorhaben bestehen zudem EU-Programme, insbesondere das EU-Rahmenprogramm für Forschung und Innovation Horizont Europa, an denen sich Unternehmen, Hochschulen und Forschungseinrichtungen aus Deutschland beteiligen.

15. Wie bewertet die Bundesregierung die Stellung des Forschungsstandorts Deutschland bei Cybersicherheitsforschung und Cybersicherheitsinnovationen, und welche Merkmale müssen noch erfüllt werden, damit Deutschland zum „Nukleus der Cybersicherheitsinnovationen“ (Cybersicherheit – Forschungspolitische Impulse, S. 9) wird?

Deutschland ist ein exzellenter Forschungsstandort mit einer weltweit führenden Wissenschaftslandschaft mit Spitzeninstituten wie CISPA, ATHENE, Max-Planck-Institut für Sicherheit und Privatsphäre und dem Exzellenzcluster CASA. Die Bundesregierung setzt sich intensiv dafür ein, dass auch der Transfer in die Anwendung am Standort Deutschland weiter befördert und beschleunigt wird. Die Ausgründungsförderung StartUpSecure des BMFTR trägt unmittelbar zum Transfer in die Anwendungen bei, ebenso die Anwendungsorientierung von ATHENE. Diese Transferorientierung wird auch im zukünftigen Forschungsprogramm für Cybersicherheit noch stärker fokussiert.

16. Wann wird die Bundesregierung das IT-Recht modernisieren und den seit Jahren in der Kritik befindlichen „Hackerparagrafen“, der IT-Sicherheitsforschung unverhältnismäßig kriminalisiert, reformieren bzw. abschaffen, was plant die Bundesregierung, planen einzelne Bundesministerien, und bis wann konkret?

Im Koalitionsvertrag ist vereinbart, im Computerstrafrecht Rechtssicherheit für die IT-Sicherheitsforschung zu schaffen, wobei insbesondere Missbrauchsmöglichkeiten verhindert werden sollen. Das Bundesministerium der Justiz und für Verbraucherschutz prüft derzeit, wie dieses Vorhaben am besten umgesetzt werden kann. Dabei werden auch die Rückmeldungen berücksichtigt, die zu dem in der vergangenen Legislaturperiode veröffentlichten, aber nicht vom Deutschen Bundestag verabschiedeten, Gesetzentwurf zur Modernisierung des Computerstrafrechts eingegangen sind.

17. Inwieweit plant die Bundesregierung, den Transfer von Forschungsergebnissen in kleine und mittlere Unternehmen (KMU) im Rahmen künftiger Förderrichtlinien stärker zu priorisieren, um die digitale Resilienz der breiten Wirtschaft gegenüber Ransomware und Spionage zu erhöhen?

Die Bundesregierung verfolgt das Ziel, die digitale Resilienz des deutschen Mittelstands als Teil einer souveränen europäischen Wirtschaftsregion in erheblichem Maße zu stärken. Im künftigen Forschungsprogramm wird der Transfer wissenschaftlicher Exzellenz in die breite Praxis von KMU konsequent ausgebaut und strukturell verankert. Ausgewählte themenbezogene und themenoffene Förderrichtlinien sollen auf die spezifischen Bedarfe des Mittelstands zugeschnitten werden.

18. Ist die Bundesregierung der Auffassung, dass vor dem Hintergrund des Dual-Use Charakters von Cybersicherheitsforschung die Forschungssicherheit der geförderten Projekte durch geeignete Maßnahmen gewährleistet werden muss, und wenn ja, wie?

Die Bundesregierung misst der Forschungssicherheit eine zentrale Bedeutung bei und betrachtet sie als unverzichtbare Voraussetzung für den Schutz der technologischen Souveränität Deutschlands. Um die Risiken von unerwünschtem Wissens- und Technologieabfluss, unzulässiger Einflussnahme und der missbräuchlichen Zweckentfremdung von Forschungsergebnissen zu reduzieren, setzt die Bundesregierung auf eine Kombination aus verstärkter Eigenverantwortung der Forschungsinstitutionen und verbesserter Beratungsinfrastruktur. Bis Anfang des Jahres 2027 wird dazu vom BMFTR gemeinsam mit den Wissenschaftsministerien der Länder und der Allianz der Wissenschaftsorganisationen die „Nationale Plattform für Forschungssicherheit“ aufgebaut.

19. Welche sind aus Sicht der Bundesregierung die „relevanten Akteure in Deutschland“ (Cybersicherheit – Forschungspolitische Impulse, S. 8), mit denen sie den Dialog zur Cybersicherheitsforschung vorantreiben möchte, und welche Maßnahmen sieht sie dafür vor?

Die Bundesregierung sieht als relevante Akteure unter anderem Universitäten, Forschungsinstitute sowie angewandte Forschungsorganisationen, Hardware- und Softwarehersteller, die Anwender, insbesondere Betreiber kritischer Infrastrukturen, die Industrie sowie staatliche Anwender, Versicherungen und Standardisierungsgremien sowie deren vertretende Institutionen wie Verbände und Vereine, staatliche Akteure und Regulierungsbehörden sowie Institutionen der Zivilgesellschaft.

Um die verschiedenen Akteure entlang der Wertschöpfungskette effektiv einzubinden, ist der Aufbau einer vertrauensbasierten Kooperationskultur entscheidend. Die konkreten Maßnahmen werden in der Entwicklungsphase des künftigen Forschungsprogramms ausgestaltet.

20. Welche konkreten Maßnahmen plant die Bundesregierung im Rahmen des Cybersicherheit-Nachfolgeprogramms, um dem akuten Fachkräftemangel in der IT-Sicherheitsforschung entgegenzuwirken, und wie soll die Ausbildung sowie die langfristige Bindung von wissenschaftlichem Nachwuchs in diesem Bereich am Standort Deutschland sichergestellt werden?

Um dem akuten Fachkräftemangel in der IT-Sicherheitsforschung zu begegnen, setzt die Bundesregierung im Rahmen des künftigen Forschungsrahmenprogramms auf eine umfassende Strategie aus Qualifizierung, Standortattraktivität und modernisierten Rahmenbedingungen. Die akademische Ausbildung wird durch eine engere Verzahnung von Theorie und Praxis sowie interdisziplinäre Projekte an der Schnittstelle von Schlüsseltechnologien gestärkt. Zur Bindung des wissenschaftlichen Nachwuchses fördert das BMFTR den Auf- und Ausbau spezialisierter Forschungszentren und Innovationhubs, die modernste Infrastrukturen bieten und den Technologietransfer beschleunigen. Auch die Ausgründungsförderung StartUpSecure des BMFTR trägt zur Gewinnung qualifizierten Nachwuchses bei. Ein übergreifendes Element ist das vom BMFTR aufgelegte „1000-Köpfe-Plus-Programm“, das gezielt zur Gewinnung internationaler Spitzenforscher sowie herausragender Forschertalente für den Standort Deutschland beiträgt.

21. Inwiefern setzt sich die Bundesregierung für eine verstärkte europäische Zusammenarbeit und Koordinierung bei der IT-Sicherheitsforschung ein, und welche konkreten Initiativen, Rahmenwerke oder Finanzierungsinstrumente werden auf EU-Ebene unterstützt oder initiiert?

Die Bundesregierung forciert eine verstärkte europäische Zusammenarbeit in der IT-Sicherheitsforschung, um die technologische Souveränität Europas zu festigen und Abhängigkeiten von Drittstaaten zu minimieren. Ein zentrales Element dieser Strategie ist die aktive Mitgestaltung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) sowie die Einbindung in dessen Netzwerk nationaler Koordinierungszentren. Die Bundesregierung bringt sich entsprechend in die Verhandlungen zum nächsten EU-Rahmenprogramm für Forschung und Innovation und verwandter EU-Programme ein. Darüber hinaus wird auf die Antwort zu Frage 14 verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333