VDI Technologiezentrum

# Deutsche Cybersicherheitsstrategie im Diskurs: Anforderungen und Impulse aus Europa


Bildquelle: © GettyImages/gorodenkoff

VDI Research

November 2023 | vditz.de

# Deutsche Cybersicherheitsstrategie im Diskurs: Anforderungen und Impulse aus Europa

Der aktuelle Bericht zur **IT-Sicherheitslage in Deutschland**[1] zeichnet ein **besorgniserregendes Bild** der Cybersicherheit: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert täglich etwa **250.000 neue Schadprogramm-Varianten** und 21.000 infizierte Systeme. Im Durchschnitt treten **täglich 70 neue Sicherheitslücken** auf, von denen die Hälfte als hoch oder kritisch eingestuft wird, eine Steigerung um 24 Prozent im Vergleich zum Vorjahr. Ransomware-Angriffe verursachen erhebliche wirtschaftliche Schäden und beeinträchtigen ganze Wertschöpfungsketten, insbesondere für kleine und mittlere Unternehmen sowie Kommunen. Datendiebstähle prägen die Gefährdungslage für Verbraucher, oft in Verbindung mit Ransomware-Angriffen zur Erpressung.

Bundesinnenministerin Nancy Faeser betonte die **entscheidende Rolle der Cybersicherheit** für die Gesellschaft und befürwortet angesichts der wachsenden Cyberkriminalität und der sich vollziehenden Zeitenwende **eine strategische Neuausrichtung.**[2]

Das vorliegende VDI Research Paper ordnet den Sachstand zur Deutschen Cybersicherheitsstrategie vor dem Hintergrund der europäischen Informationssicherheits-Richtlinien ein und gibt Impulse im Diskurs zu deren Weiterentwicklung.

## (Eine) Cybersicherheitsstrategie für Deutschland 2021

Im September 2021, kurz vor der Bundestagswahl, verabschiedete die alte Bundesregierung die **„Cybersicherheitsstrategie für Deutschland 2021“,** die als Fortführung der 2016 veröffentlichten Strategie fungiert und einen neuen, ressortübergreifenden strategischen Rahmen bis 2026 setzt.

**Vier Leitlinien der Deutschen Cybersicherheitsstrategie:**

1. Cybersicherheit als gemeinsame Aufgabe: Diese Leitlinie etabliert Cybersicherheit als eine kollektive Aufgabe von Staat, Wirtschaft, Gesellschaft und Wissenschaft.
2. Stärkung der digitalen Souveränität: Die Strategie setzt sich dafür ein, die digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft zu stärken.
3. Sichere Gestaltung der Digitalisierung: Hier liegt der Fokus auf der sicheren Umsetzung der Digitalisierung.
4. Messbare und transparente Ziele: Die Strategie zielt darauf ab, klare, messbare und transparente Ziele zu setzen.

Diese Strategie ist entstanden aus einem Evaluierungs- und Fortschreibungsprozess unter Beteiligung von über 70 Akteuren aus verschiedenen Bereichen der Gesellschaft. Sie skizziert die grundlegende, langfristige Ausrichtung der Cybersicherheitspolitik in Deutschland durch Leitlinien, Handlungsfelder und strategische Ziele. Hierbei soll eine effektive Zusammenarbeit aller Akteure ermöglicht werden.[3]

**Kritiker,** darunter Verbände und Wissenschaftler, bezweifelten frühzeitig, ob die Ziele der Strategie unter einer neuen Regierung umsetzbar seien. Kritisiert wurde insbesondere der geplante Ausbau geheimdienstlicher Befugnisse und

[1] BSI 2023: Die Lage der IT-Sicherheit in Deutschland 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf
[2] BMI 2023: PM, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2023/11/bsi-lagebericht2023.html
[3] SNV 2020: Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik, snv_papier_cybersicherheits-architektur_final.pdf (stiftung-nv.de)

die Offenhaltung von Sicherheitslücken zu Überwachungszwecken.[4] Auch **vernachlässige die Strategie den EU-Kontext** und fokussiere sich hauptsächlich auf innenpolitische Aspekte. Dies stehe im Kontrast zu globalen Herausforderungen im Cybersicherheitsbereich. Die Einbindung internationaler Expertise sei ein Schlüsselfaktor für eine erfolgreiche Sicherheitsstrategie im zunehmend komplexen geopolitischen Umfeld.

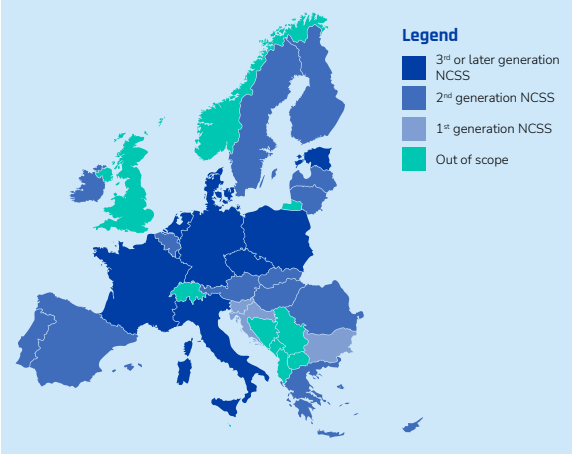
**Vier Handlungsfelder der Deutschen Cybersicherheitsstrategie:**

1. Mensch und Gesellschaft: Hier steht das sichere und selbstbestimmte Handeln in einer digitalisierten Umgebung im Vordergrund, um den Menschen die sichere Nutzung digitaler Technologien zu ermöglichen.
2. Staat und Wirtschaft: Das Handlungsfeld betont den gemeinsamen Auftrag von Staat und Wirtschaft, insbesondere mit Blick auf die Sicherheit von kritischen Infrastrukturen und kleinen sowie mittleren Unternehmen.
3. Strukturen und Verantwortlichkeiten: Die staatlichen Akteure der Cybersicherheit stehen im Fokus dieses Handlungsfelds, und zwar mit dem Ziel, die Zusammenarbeit und Kompetenzverteilung zwischen den Behörden zu stärken.
4. Deutschland in EU und NATO: Dieses Handlungsfeld betont die Notwendigkeit einer aktiven Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik.

## (Eine) Cybersicherheitsstrategie für Europa 2022

Die Network-and-Information-Security(NIS-2)-Richtlinie der Europäischen Union vom Dezember 2022[5] ist eine Aktualisierung der bereits existierenden NIS-Richtlinie von 2017, wonach alle EU-Mitgliedsstaaten bis 2018 eine konkrete nationale Cybersicherheitsstrategie (NCSS) zu etablieren hatten. Dabei unterstützt die „European Union Agency for Cybersecurity“ (ENISA)[6] die EU-Mitgliedsstaaten.[7, 8]

Viele dieser Strategien wurden seither aktualisiert: Von den 27 Mitgliedsstaaten haben inzwischen neun Mitgliedstaaten eine NCSS der dritten Generation oder höher, 14 Mitgliedsstaaten eine NCSS der Zweiten Generation und vier Mitgliedsstaaten ihre erste NCSS. **(Siehe hierzu auch die Übersicht derzeit existierender NCSS in der EU im Anhang.)**




**Quelle: https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies/@@download/fullReport**

[4] Heise 2021: https://www.heise.de/news/Cybersicherheitsstrategie-Kritik-an-Regierung-als-groesstem-Sicherheitsrisiko-6188168.html; Bitkom 2021: https://www.bitkom.org/sites/main/files/2021-04/210414_css_stellungnahme_bitkom.pdf; PSW 2021: https://www.psw-consulting.de/blog/2021/11/17/cybersicherheitsstrategie-2021/; EURACTIV 2021: https://www.euractiv.de/section/innovation/news/bleibt-die-neue-deutsche-cybersicherheitsstrategie-ohne-wirkung/

[5] EC 2022 „The Network and Information Security (NIS) Directive“: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&qid=1694687690563, https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

[6] ENISA 2023: www.enisa.europa.eu

[7] ENISA 2023: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[8] EU 2023, Cybersecurity: how the EU tackles cyber threats – Consilium (europa.eu), https://www.consilium.europa.eu/de/policies/cybersecurity/

Die aktuellen NCSS dieser Länder weisen konzeptionelle Gemeinsamkeiten auf, darunter

- Verbindung zu nationalen Sicherheitsstrategien,
- Fokus auf defensive Cyberfähigkeiten,
- Betonung der internationaler Kooperation,
- Betonung der Zusammenarbeit mit dem Privatsektor,
- Notwendigkeit umfassender Sensibilisierung der Gesellschaft und Bildung.

Die Hauptunterschiede liegen in

- den Verantwortlichkeiten für Cybersicherheit innerhalb staatlicher Strukturen (einschließlich des Zentralisierungsgrades),
- der Beziehung zwischen zivilen und militärischen Kräften sowie in
- den Aufgaben von Nachrichtendiensten und Strafverfolgungsbehörden.

Diese Unterschiede werden größtenteils durch die jeweilige politische Kultur und die Organisation der politischen Systeme beeinflusst.

Auch die Debatte um sogenannte „Hack Backs“ – offensive Cyberoperationen als Reaktion auf Cyberangriffe – hat in den letzten Jahren weltweit an Bedeutung gewonnen. Hack Backs sind zu einem umstrittenen Instrument in der Cybersicherheitspolitik geworden und einige Staaten befürworten offensivere Maßnahmen als Teil ihrer Verteidigungsstrategien, während andere zurückhaltender agieren und auf internationale Kooperation setzen. Die Dynamik dieses Themas hat zu unterschiedlichen nationalen Ansätzen geführt.

Die NIS-2-Richtlinie (NIS-2) setzt neue Standards für die Cybersicherheit in Europa und stellt einen wichtigen Schritt zur Harmonisierung der Cybersicherheitsanforderungen in der gesamten EU dar.[9]

Sie verpflichtet Mitgliedsstaaten zu einer Überarbeitung ihrer nationalen Strategien und zu einer Benennung kritischer Infrastrukturen sowie zu einer verstärkten Kooperation mit den anderen Mitgliedsstaaten. Darüber hinaus verschärft sie die Cybersicherheitsanforderungen und legt strengere Anforderungen für Cyber-Risikomanagement, Kontrolle, Überwachung, Umgang mit Zwischenfällen und Geschäftskontinuität fest. Der Anwendungsbereich wird erweitert und es werden strengere Haftungsregeln für die Geschäftsleitungen betroffener Organisationen festgelegt.

Die EU plant, NIS-2 mit beispiellosen Investitionen von bis zu 4,5 Milliarden Euro über sieben Jahre zu unterstützen. Dies umfasst Programme wie Digital Europe und Horizon Europe sowie den EU-Wiederaufbauplan.[10]

## Zukunft der Deutschen Cybersicherheitsstrategie

Gegenwärtig befindet sich die **Cybersicherheitsstrategie in einer Weiterentwicklung,** um die Vorgaben des **aktuellen Koalitionsvertrags** umzusetzen.[11] Bundesinnenministerin Nancy Faeser präsentierte im **Juli 2022** die **„Cybersicherheitsagenda“**[12] Deutschlands mit dem Ziel, die Sicherheit von IT-Infrastrukturen zu gewährleisten und effektiv gegen Cyberangriffe und  kriminalität vorzugehen. Die neue Agenda umfasst die Schaffung einer modernen Cybersicherheitsarchitektur, die das BSI zu einer zentralen Anlaufstelle ausbaut und das Nationale Cyberabwehrzentrum sowie den Nationalen Cyber-Sicherheitsrat stärkt und darüber hinaus eine entsprechende Kommunikationsplattform beim BSI etabliert.

Das Bundesinnenministeriums hat im Juni 2023 einen **Referentenentwurf für ein Gesetz zur Umsetzung von NIS-2 (NIS2UmsuCG)**[13] und

[9] ENISA 2023: A Governance Framework for National Cybersecurity Strategies: https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies

[10] Europäisches Kompetenzzentrum für Cybersicherheit (ECCC): https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-competence-centre

[11] BMI 2022, Cybersicherheitspolitik: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html

[12] BMI 2022, Cybersicherheitsagenda: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4

[13] BMI 2023: Referentenentwurf des NIS2UmsuCG, https://intrapol.org/wp-content/uploads/2023/07/230703_BMI_RefE_NIS2UmsuCG.pdf

im September 2023 ein **Diskussionspapier**[14] vorgelegt, die beide darauf abzielen, die bestehenden Steuerungsinstrumente für das Informationssicherheitsmanagement in der Bundesverwaltung zu verstärken und den Sicherheitsrahmen für kritische Anlagen und Unternehmen zu erweitern: Durch die Umsetzung der NIS-2-Richtlinie sollen neue Kategorien von Einrichtungen festgelegt werden, die erweiterten Anforderungen unterliegen.

Eine wesentliche Neuerung von NIS-2 besteht darin, dass die Definition sogenannter „kritischer Dienste" präzisiert und erweitert wird. Es wird nun zwischen „wesentlichen Einrichtungen" und „wichtigen Einrichtungen" unterschieden.[15]

Neben einer Meldepflicht für Sicherheitsvorfälle sieht NIS-2 auch eine Erhöhung der Sanktionen vor. Unternehmen, die den Vorgaben nicht nachkommen, können mit Bußgeldern belegt werden. In Deutschland allein sind etwa 30.000 Unternehmen von den Anforderungen der NIS-2 betroffen.

In Summe ergibt sich also, dass das BSI erweiterte Kompetenzen für Aufsichtsmaßnahmen erhalten wird und wesentliche nationale Anforderungen an das Informationssicherheitsmanagement des Bundes gesetzlich verankert werden.[16]

## Ausblick

Auf dem Berliner Cybersicherheitsgipfel des Nationalen Cyber-Sicherheitsrats der Bundesregierung[17] wurde Ende November 2023 über die demokratische Legitimation und Kontrolle von Macht im digitalen Raum diskutiert. Dabei war es Tenor, dass europäische Staaten angesichts eines globalen Bedrohungsumfelds vor vergleichbaren Herausforderungen bei der Entwicklung und Umsetzung ihrer Cybersicherheitsstrategien stehen.[18] Diese Herausforderungen umfassen die vertikale Integration in den Rahmen nationaler Sicherheit, die horizontale Koordination verschiedener Stellen, die Förderung internationaler Zusammenarbeit, den Aufbau solider Krisenmanagementstrukturen, das Erstellen zuverlässiger Bedrohungsanalysen, den Ausbau von Kapazitäten und Bildungsangeboten, die Schaffung eines kooperativen Rahmens mit der Privatwirtschaft sowie eine Harmonisierung der Gesetzgebung zur Bekämpfung von Cyberkriminalität.

Insgesamt zeigt sich Deutschland angesichts der aktuellen Herausforderungen entschlossen, seine Cybersicherheitsstrategie zu stärken und durch eine breite Palette von Maßnahmen auf nationaler und europäischer Ebene auf die wachsenden Cyberbedrohungen zu reagieren.

Durch die Umsetzung des NIS2UmsuCG positioniert sich Deutschland als Vorreiter in der fristgerechten Umsetzung der NIS-2-Richtlinie.

Bleibt zu wünschen, dass die neue Deutsche Cybersicherheitsstrategie auch eine verstärkte länderübergreifende Cyberkriminalitätsbekämpfung vorsieht, denn angesichts der grenzüberschreitenden Natur von Cyberbedrohungen ist eine koordinierte – zumindest europäische – Antwort unerlässlich.

[14] BMI2023: Diskussionspapier des BMI, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-UmsetzungWirtschaft_DisP.pdf;jsessionid=148D027854E223453CB3A6F3E-6062AD3.live891

[15] Wesentliche Einrichtungen erstrecken sich über verschiedene Sektoren, darunter Energie, Verkehr, Wasser, digitale Infrastruktur, Bankwesen, Gesundheit, öffentliche Verwaltung und Raumfahrt. Wichtige Einrichtungen hingegen umfassen Bereiche wie Abfallwirtschaft, Postdienste, chemische Erzeugnisse, Lebensmittelproduktion, Herstellung von Computern und Elektronik, digitale Anbieter und Forschungseinrichtungen.

[16] Es sei darauf hingewiesen, dass es sich bei dem Diskussionspapier um ein Arbeitspapier des BMI handelt, das noch nicht innerhalb der Bundesregierung abgestimmt ist. Das Gesetz zur Umsetzung der NIS-Richtlinie soll im März 2024 offiziell bekannt gegeben werden und anschließend wie vorgesehen im Oktober 2024 in Kraft treten. Es gibt keine klaren Hinweise auf Übergangsfristen für die Umsetzung oder ähnliche Regelungen. Die ersten Überprüfungen zur Nachweisführung würden frühestens ab Oktober 2027 stattfinden.

[17] BDI 2023: https://bdi.eu/termin/news/berliner-cybersicherheitsgipfel-2023

[18] ENISA 2023: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

## Anhang: Übersicht derzeit existierender NCSS in der EU

| Land | Zeitraum | NCSS/URL |
|---|---|---|
| **Belgien** | 2021-2025 | Cybersicherheitsstrategie Belgien 2.0, https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_DTS_WEB.pdf |
| **Bulgarien** | 2016-2020 | Cyber Resilient Bulgaria 2020, http://cyberbg.eu/doc/20161024_Cyber_strat_proekt.pdf |
| **Dänemark** | 2022-2024 | The Danish National Strategy for Cyber and Information Security, cfcs.dk/globalassets/cfcs/dokumenter/2022/ncis_2022-2024_en.pdf |
| **Deutschland** | 2021-2026 | Cybersicherheitsstrategie für Deutschland 2021, https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf |
| **Estland** | 2019-2022 | Cybersecurity Strategy Republic of Estonia https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/4533045a80ce44cea39c62b1d93f0e1b/file_en |
| **Finnland** | 2019-ongoing | Finland's Cyber Security Strategy 2019 https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf |
| **Frankreich** | 2021-2025 | Cybersécurité, faire à la menace: la stratégie française https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=2A6148DF-BF21-4A64-BDF8-79BACE2AE255&filename=686%20-DP%20cyber.pdf |
| **Griechenland** | 2020-2025 | National Cybersecurity Strategy https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf |
| **Irland** | 2019-2024 | National Cyber Security Strategy https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf |
| **Italien** | 2022-2026 | Strategia Nazionale Di Cybersicurezza https://www.acn.gov.it/ACN_EN_Strategia.pdf |
| **Kroatien** | 2022-ongoing | Nationale Cybersicherheitsstrategie der Republik Kroatien https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvje%C5%A1%C4%87e%20o%20provedbi%20mjera%20Akcijskog%20plana%20NSKS%20u%202022..pdf?vel=997919 |
| **Lettland** | 2023-2026 | Cybersecurity Strategy https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf |

| Land | Zeitraum | NCSS/URL |
|---|---|---|
| **Litauen** | 2018-2023 | National Cyber Security Strategy https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf |
| **Luxembourg** | 2021-2025 | National Cybersecurity Strategy IV https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/strategie-nationale-cybersecurite-4/National-Cybersecurity-Strategy-IV.pdf |
| **Malta** | 2023-2026 | Maltese National Cybersecurity Strategy economy.gov.mt/wp-content/uploads/2023/05/National-Cyber-security-2023-2026.pdf |
| **Niederlande** | 2022-2028 | Netherlands Cybersecurity Strategy https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028/TheNetherlandsCybersecurityStrategy2022-2028.pdf |
| **Österreich** | 2021-ongoing | Austrian Strategy for Cybersecurity (ÖSCS) https://www.bundeskanzleramt.gv.at/dam/jcr:29c42767-3198-45e9-94c0-0ef2348430b3/cyberstrategie2021_en.pdf |
| **Polen** | 2019-2024 | Cybersecurity Strategy of the Republic of Poland https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8 |
| **Portugal** | 2019-2023 | Nationale Strategie für die Sicherheit des Cyberspace https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf |
| **Rumänien** | 2022-2027 | Romania's new Cybersecurity Strategy and Action Plan https://gov.ro/ro/guvernul/sedinte-guvern/informatie-de-presa-privind-actele-normative-aprobate-in-sedinta-guvernului-romaniei-din-30-decembrie-2021 |
| **Schweden** | 2019-2022 | Comprehensive Information and Cyber Security Action Plan https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213 |
| **Slowakei** | 2021-2025 | The National Cybersecurity Strategy https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf |
| **Slowenien** | 2016-ongoing | Cybersecurity Strategy https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf |
| **Spanien** | 2019-ongoing | Estrategia Nacional de Ciberseguridad dsn.gob.es/sites/dsn/files/Estrategia Nacional de Ciberseguridad 2019.pdf |
| **Tschechien** | 2021-2025 | National Cyber Security Strategy of the Czech Republic https://www.nukib.cz/en/cyber-security/strategy-action-plan |

| Land | Zeitraum | NCSS/URL |
|---|---|---|
| **Ungarn** | 2013-2018 | National Cyber Security Strategy of Hungary https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy/@@download_version/f8bf5151996d4de595299ae21b626297/file_en |
| **Zypern** | 2020-ongoing | Revised Cybersecurity Strategy of the Republic of Cyprus https://www.cyberwiser.eu/sites/default/files/cy%20ncss%20greek.pdf |

**Quelle: eigene Recherche und https://www.cyberwiser.eu/cartography; https://ccdcoe.org/library/strategy-and-governance/; https://dig.watch/resource; https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map**

## VDI Research

VDI Research versteht sich als Informationsdienstleister, Impulsgeber und Vernetzer zu neuen Themen, Methoden und längerfristiger Vorausschau.

Weitere Publikationen von VDI Research und des VDI TZ unter: vditz.de/service/publikationen

## Ihre Ansprechpersonen

VDI Research
Dr. Anette Braun
Dr. Dirk Holtmannspötter
Dr. Dr. Axel Zweck
E-Mail: braun_a@vdi.de

VDI Technologiezentrum GmbH
VDI-Platz 1, 40468 Düsseldorf

www.vditz.de
@technikzukunft · in