#GIDSresearch 2/2025

Stefan Messingschlager

Innen robust, außen anschlussfähig

Deutschlands Handlungsfähigkeit im Cyber- und Informationsraum

#GIDSresearch | Nr. 2/2025 | Dezember 2025 | ISSN 2699-4380

GIDS GERMAN INSTITUTE FOR DEFENCE AND STRATEGIC STUDIES

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie, detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

ISSN 2699-4380

Dieses #GIDSresearch wird vom German Institute for Defence and Strategic Studies (GIDS) herausgegeben.

Die Beiträge sind auf der Website des GIDS kostenfrei abrufbar: www.gids-hamburg.de

#GIDSresearch gibt die Meinung der AutorInnen wieder und stellt nicht zwangsläufig den Standpunkt des GIDS dar.

Zitiervorschlag:

Stefan Messingschlager, Innen robust, außen anschlussfähig: Deutschlands Handlungsfähigkeit im Cyber- und Informationsraum, #GIDSresearch 2/2025, GIDS: Hamburg.

GIDS
German Institute for Defence and Strategic Studies
Führungsakademie der Bundeswehr
Manteuffelstraße 20 · 22587 Hamburg
Tel.: +49 (0)40 8667 6801
buero@gids-hamburg.de · www.gids-hamburg.de

Inhalt

Stefan Messingschlager* | German Institute for Defence and Strategic Studies

Innen robust, außen anschlussfähig

Deutschlands Handlungsfähigkeit im Cyber- und Informationsraum

1 Deutschland im Cyber- und Informationsraum: Problemstellung und Logiken politischer Handlungsfähigkeit

Staat, Wirtschaft und Öffentlichkeit sind heutzutage digital eng verflochten und damit auf breiterer Linie angreifbar. Konflikte werden folglich nicht nur an physischen Infrastrukturen, sondern auch im Cyberraum und in der öffentlichen Wahrnehmung ausgetragen. Unterhalb der Gewaltschwelle überlagern sich technische Angriffe, Sabotage und orchestrierte Einflussnahmen zu einem persistenten Störrauschen.[1] Deutschland ist in dieser Lage doppelt gefordert: als hochvernetzte Volkswirtschaft mit großer Angriffsfläche und als zentraler Pfeiler europäischer Stabilität, der gegenüber Partnern berechenbar handeln muss.[2]

Um sich Deutschlands Handlungsfähigkeit im Cyber- und Informationsraum (CIR)[3] annähern zu können, bedarf es im ersten Schritt eines Rahmens, der die Logik moderner Konflikte mit den Bedingungen liberal-demokratischen Regierens verbindet. Vier miteinander verschränkte Dimensionen tragen diesen Rahmen.

Erstens: Bedrohungslogik. Hybride Operationen kombinieren technische Eingriffe, physische Sabotage und kognitive Effekte unterhalb klarer Gewaltschwellen; sie zielen zugleich auf die Funktionsfähigkeit von Staatlichkeit, die Integrität Kritischer Infrastrukturen (KRITIS) und die Legitimität politischer Entscheidungen.[4] Der Fokus auf das

---

* Stefan Messingschlager forscht als Historiker und Politikwissenschaftler an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg und ist Non-Resident Fellow am Global Public Policy Institute (GPPi), Berlin. Seine Forschungsschwerpunkte umfassen die Geschichte und Gegenwart der deutsch-chinesischen Beziehungen, Chinas Rolle in der globalen Ordnung sowie Europas außen- und sicherheitspolitische Herausforderungen im Kontext des sino-amerikanischen Großmachtkonflikts.
Besonderer Dank gilt den anonymen Gutachter:innen für ihr konstruktives Feedback sowie zahlreichen Freund:innen und Kolleg:innen aus Universitäten, Ministerien und Thinktanks für den intensiven Austausch, der diesen Beitrag in seiner jetzigen Form überhaupt erst ermöglicht hat. Verbliebene Fehler oder Unklarheiten liegen selbstverständlich in der alleinigen Verantwortung des Verfassers.

1 Siehe dazu die Diagnoselage des Bundesamts für Sicherheit in der Informationstechnik (BSI), von NATO und European Union Agency for Cybersecurity (ENISA): BSI 2024; NATO 2022; ENISA 2025b; Bendiek/Bossong 2022; Mumford/Carlucci 2023.

2 Vgl. dazu einführend: International Institute for Strategic Studies (IISS) 2023.

3 Aus Gründen der Lesbarkeit und allgemeinen Verständlichkeit werden Fachbegriffe in diesem Beitrag grundsätzlich ausgeschrieben. Soweit Bezeichnungen im politisch-administrativen oder fachwissenschaftlichen Diskurs überwiegend in abgekürzter Form verwendet werden, wird bei der ersten Nennung die gebräuchliche Abkürzung in Klammern angegeben (z. B. „Kritische Infrastrukturen“ (KRITIS)). Auf ein gesondertes Abkürzungsverzeichnis wird daher verzichtet.

4 Vgl.: ENISA 2025b; EEAS 2025.

sogenannte *Informationsumfeld* schärft den Blick für die Schnittstelle von Plattformdynamiken, öffentlicher Kommunikation und staatlicher Reaktionsfähigkeit.

Zweitens: Handlungslogik. Der Cyberraum ist ein permanenter Wettbewerbsraum; reine Reaktivität unterschätzt Tempo und Taktung gegnerischer Akteure. Konzepte wie „Defend Forward" und „Persistent Engagement" markieren eine proaktive Verteidigungslogik, die gegnerische Aktivitäten früh beobachtet und stört – technisch, organisatorisch und kommunikativ –, ohne die rechtliche und politische Einbettung zu unterlaufen.[5] Für eine offene Gesellschaft folgt daraus keine Abkehr vom Recht, sondern die Notwendigkeit prozeduraler Vorsorge: Zuständigkeiten, Prüfschritte und Freigabeketten müssen so vorbereitet sein, dass im Ereignisfall schnelles Handeln rechtmäßig bleibt.

Drittens: Governance- und Legitimationslogik. In liberalen Demokratien ist strategische Kommunikation (StratCom) Sicherheitsfunktion. Sie synchronisiert technische Lagebilder, Attribution und politische Bewertung, macht Normverletzungen sichtbar und legitimiert Maßnahmen – nach innen gegenüber Bürgerinnen und Bürgern, nach außen gegenüber Partnern oder Gegnern.[6] Handlungsfähigkeit erwächst dementsprechend nicht allein aus Technik, sondern aus der Verzahnung von Technik, Organisation, Recht und Kommunikation: aus einem gehärteten Grundbetrieb, einer mandatierenden Führungs- und Eingriffsordnung mit klaren Schwellen, einer institutionell verankerten Fähigkeit zur strategischen Kommunikation sowie geübten, rechtsklaren Verfahren. Genau an diesen Nahtstellen setzen hybride Angriffe politisch an – und genau hier zeigt Deutschland bislang Reibungsverluste.

Viertens: Interoperabilitäts- und Messlogik. Leistung wird im Verbund gemessen. Auf Bündnisseite (North Atlantic Treaty Organization – NATO) existieren Mechanismen kollektiver Handlungsfähigkeit (Unterstützung, Lagefeststellung und Führung);[7] auf Seite der Europäischen Union verdichtet sich ein Ordnungsrahmen aus Mindeststandards, Aufsicht und solidarischen Hilfen zu einem regulatorischen und kapazitären Unterbau.[8] Nationale Souveränität bewährt sich in diesem Kontext vor allem als anschlussfähige Souveränität: Verfahren, Technik und Freigabeketten müssen so konstruiert sein, dass sie friktionsarm andocken. Wirkung zählt erst, wenn sie belegbar ist – nicht durch Zahlenfetischismus, sondern über wenige robuste Indikatoren, die Fortschritt und Engstellen sichtbar machen.

Die Ordnungslogik ist damit gesetzt: Bedrohungen werden nicht nur beschrieben, sondern durch eine persistente Handlungslogik adressiert; Geschwindigkeit wird durch rechtlich-organisatorische Klarheit ermöglicht; Legitimation entsteht über eine operativ verankerte strategische Kommunikation; Interoperabilität und Messbarkeit sichern Verlässlichkeit im Verbund.

Im Weiteren entfaltet der Beitrag diese Ordnung in vier Schritten: Abschnitt 2 zeichnet die Verdichtung auf NATO- und EU-Ebene nach und präzisiert den daraus entstehenden transatlantisch-europäischen Erwartungsraum; Abschnitt 3 analysiert die Partnerarchitekturen und die Verschränkung offensiver Optionen, Governance und strategischer Kommunikation. Abschnitt 4 wendet das Raster auf den deutschen Befund an und

5 Vgl. vor allem deren Verankerung in der U.S. Cyber Strategy: U.S. Cyber Command 2018; U.S. Department of Defense 2018.
6 Vgl. dazu einführend: NATO StratCom COE o.D. c; Bolt 2023.
7 Vgl.: NATO 2024a; NATO 2023; Goździewicz 2019.
8 Vgl.: Europäische Union 2022 a, b; Europäische Union 2024 a; Europäische Union 2025.

identifiziert Nahtstellenverluste. Abschnitt 5 operationalisiert abschließend die Lehren zu einer messbaren Umsetzungsarchitektur für die kommenden Jahre – von gehärteten Grundlagen über rechtsklare Eingriffsschwellen bis zur geübten Bündnisfähigkeit.

2 Der transatlantisch-europäische Erwartungsraum: Zur Verdichtung von NATO-Mechanismen und EU-Regime, 2007 – 2025

Wer verstehen will, weshalb der Cyber- und Informationsraum heute zum Kernbestand transatlantischer Sicherheitspolitik gehört, muss die graduelle, aber stetige Verdichtung der letzten eineinhalb Jahrzehnte nachvollziehen.[9] Ein entscheidender Wendepunkt war der großangelegte Cyberangriff auf Estland im Jahr 2007, der heute als „Stunde null" militärischer Konfliktaustragung im digitalen Raum gilt.[10] Auslöser der Attacke war die politisch umstrittene Verlegung eines sowjetischen Kriegsdenkmals in Tallinn, woraufhin massive, wochenlange Cyberoperationen Regierungseinrichtungen, Banken, Telekommunikationsnetze sowie Medien nahezu vollständig lahmlegten. Dieses Ereignis machte erstmals drastisch deutlich, dass digitale Angriffe nicht nur technische, sondern auch staatliche und gesellschaftliche Strukturen existenziell bedrohen können. Als unmittelbare Konsequenz gründete die NATO bereits 2008 in Tallinn das Cooperative Cyber Defence Centre of Excellence (CCDCOE), das seither als zentrales Kompetenzzentrum für Forschung, Ausbildung und strategische Beratung fungiert.[11] Seit 2010 organisiert das Cooperative Cyber Defence Centre of Excellence zudem regelmäßig die Großübung „Locked Shields", eine der weltweit größten Cyberabwehrübungen, in deren Rahmen die Verteidigungsfähigkeit der NATO-Staaten gegen simulierte Angriffe geprüft und geschult wird. Dennoch verharrte das Bündnis zunächst in einer primär defensiven Grundhaltung, die den Schutz eigener Infrastrukturen priorisierte, ohne proaktive oder offensive Maßnahmen strategisch zu verankern.

Die entscheidende strategische Zäsur erfolgte erst auf dem NATO-Gipfel in Wales 2014, als die Allianz festhielt, dass besonders gravierende Cyberangriffe unter Umständen den Bündnisfall nach Artikel 5 auslösen können.[12] In Warschau 2016 erkannte die NATO den Cyberraum als Operationsdomäne an und verabschiedete den Cyber Defence Pledge – einen politischen Taktgeber, der die Mitgliedstaaten auf messbaren Fähigkeitsaufbau verpflichtet.[13] In der Folge wurden planerische und operative Grundlagen ausgebaut: 2018 nahm in Mons das Cyberspace Operations Centre (CyOC)[14] seine Arbeit auf, und mit dem Mechanismus „Sovereign Cyber Effects Provided Voluntarily by Allies" (SCEPVA)[15] wurde seit 2019 ein Format etabliert, in dem Verbündete nationale offensive Cyber-Kräfte freiwillig und unter eigener Souveränität in

9 Vgl.: für den historischen Überblick: Pfannenstiel/Cox 2024: 1–10.
10 Vgl. dazu u. a.: Ottis 2008; NATO StratCom COE o.D. a.
11 Vgl.: Gold 2019.
12 Vgl.: NATO 2014.
13 Vgl.: NATO 2016a; NATO 2016b.
14 Vgl.: NATO 2024a.
15 Vgl.: NATO 2018; Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2018; Goździewicz 2019.

NATO-Operationen einbringen können – ohne die politische Kontrolle über sensible Instrumente aus der Hand zu geben.

Die jüngste Wegmarke war der Gipfel von Washington (Juli 2024). Dort beschlossen die Alliierten, ein NATO Integrated Cyber Defence Centre (NICC) zu schaffen, das die Verteidigung der eigenen Netze und die gemeinsame Lagefeststellung beschleunigen soll – ein Schritt von reiner Abwehr hin zu vernetzter Verteidigungsorganisation.[16] Parallel priorisierte die Allianz den Schutz maritimer Verwundbarkeiten: Bereits im Februar 2023 richtete die NATO am Hauptquartier eine Critical Undersea Infrastructure Coordination Cell (CUICC) ein. Sie kartiert Verwundbarkeiten, vernetzt militärische, zivile und industrielle Akteure und bildet den Koordinationsknoten für Informationsaustausch und Best-Practice-Transfer – anschlussfähig an die 2023 gestartete EU-NATO-Task-Force zur Resilienz Kritischer Infrastrukturen. 2024 folgten die operative Verdichtung über das Critical Undersea Infrastructure Network sowie das Maritime Centre for the Security of Critical Undersea Infrastructure bei MARCOM (Northwood). Seitdem ist die Sicherung von Unterseekabeln und Pipelines als Daueraufgabe verankert.[17] 2025 flankierte die NATO diese Linie mit Initiativen zur besseren Überwachung sensibler Seegebiete bis hin zu einsatzähnlichen Aktionen in der Ostsee.[18]

Zur operativen Unterfütterung gehört auch die im Vilnius-Kommuniqué 2023 verankerte „Virtual Cyber Incident Support Capability“ (VCISC): Ein Clearing-House, das angegriffenen Alliierten schnell Expertise, Forensik und Intelligence zuführt (u. a. Malware-Analyse & CTI).[19] 2025 wurde der Mechanismus in Übungen und realitätsnahen Formaten weiter operationalisiert – mit der Konsequenz, dass nationale Prozeduren, Rechtsgrundlagen und technische Schnittstellen „VCISC-fähig“ sein müssen, wenn Hilfe schnell anlaufen soll. Inhaltlich rückt zugleich die kognitive und technologische Dimension stärker in den Fokus. Künstliche Intelligenz wirkt als Verstärkerin beider Seiten: Sie erhöht die Schlagzahl und Adaptivität von Angriffsketten, eröffnet aber auch Chancen für frühzeitige Detektion und automatisierte Abwehr.[20] Die NATO hat 2021 eine KI-Strategie vorgelegt und 2024 überarbeitet;[21] parallel treiben der Defence Innovation Accelerator for the North Atlantic (DIANA) und der NATO Innovation Fund (NIF) Beschaffungs- und Innovationspfade für Schlüsseltechnologien wie KI, Robotik und Weltraum-Technologien voran.[22]

Parallel hat die Europäische Union (EU) ihr Regulierungs- und Fähigkeitsfundament spürbar ausgehärtet. Die zweite Richtlinie über Netz- und Informationssicherheit (NIS-2) setzt seit Ende 2022 den gemeinsamen Mindeststandard für ein breites Spektrum kritischer und wichtiger Einrichtungen.[23] Mit dem Digital Operational Resilience Act (DORA) gilt seit dem 17. Januar 2025 ein sektorspezifischer, unmittelbar anwendbarer Resilienzrahmen für den Finanzsektor (Risikomanagement, Meldewesen, Tests,

16 Vgl.: NATO 2024b; NATO 2024c.
17 Vgl.: NATO Allied Maritime Command 2024.
18 Vgl.: AP News 2025.
19 Vgl.: NATO 2023; UK Ministry of Defence 2023.
20 Vgl.: Reynolds/Atalan 2024; NATO 2024d.
21 Vgl.: NATO 2021; NATO 2024e.
22 Vgl.: NATO 2025.
23 Vgl.: Europäische Union 2022a.

Steuerung von Drittparteien).[24] Auf der Produktebene setzt der Cyber Resilience Act (CRA; Verordnung (EU) 2024/2847)[25] horizontale Sicherheitsanforderungen für „Produkte mit digitalen Elementen“ – einschließlich Verpflichtungen für Schwachstellen-Management, Sicherheits-Updates und Vorfallmeldungen – und wird durch das EU-„Common-Criteria“-Zertifizierungsschema (EUCC)[26] als gemeinsame Referenz für vertrauenswürdige Informations- und Kommunikationstechnologie-Produkte ergänzt. Beide Instrumente adressieren strukturelle Ursachen von Angriffsflächen, bevor diese in operative Lagen diffundieren.

Mit dem Cyber Solidarity Act (CSA)[27] ist darüber hinaus seit Februar 2025 eine neue Solidar- und Einsatzarchitektur in Kraft: ein europäisches Alarm- und Lagebildsystem auf Basis vernetzter nationaler und grenzüberschreitender Security Operations Center (SOCs) („European Cybersecurity Shield“), ein Notfallmechanismus mit gemeinsamer Beschaffung und EU-Cyber-Reserve sowie ein institutionalisiertes Review großer Vorfälle unter Führung der European Union Agency for Cybersecurity (ENISA). In der Governance der Informationsräume wurde die Aufsicht durch den Digital Services Act (DSA)[28] substanziell geschärft: Der European Board for Digital Services koordiniert seit Februar 2024 die Behördenpraxis; die Europäische Kommission hat 2024 Leitlinien für sehr große Plattformen und Suchmaschinen zur Absicherung von Wahlprozessen vorgelegt und 2025 ein Elections-Toolkit für nationale Koordinatoren bereitgestellt, spürbare Vollzugsentscheidungen haben der Regulierung greifbare Konturen gegeben.

Transatlantisch ist der Übergang zur Post-Quanten-Kryptografie (PQC) konkret geworden. Das US-Normeninstitut National Institute of Standards and Technology (NIST) hat im August 2024 mit FIPS 203 (Module-Lattice-based Key Encapsulation Mechanism, ML-KEM), FIPS 204 (Module-Lattice-based Digital Signature Algorithm, ML-DSA) und FIPS 205 (Stateless Hash-Based Digital Signature Standard, SLH-DSA) die ersten PQC-Standards finalisiert;[29] im Juni 2025 folgte die EU mit einer koordinierten PQC-Roadmap der NIS-Kooperationsgruppe, die Meilensteine und Migrationspfade für besonders schutzbedürftige Anwendungsfälle definiert.[30] Für Betreiber kritischer Funktionen entsteht damit ein klarer, abgestimmter Rahmen, in dem Migrationsentscheidungen rechtzeitig, interoperabel und risikogesteuert zu treffen sind.

Die Bedrohungslage rechtfertigt diese Verdichtung: Das europäische Lagebild konstatiert für 2025 eine anhaltend hohe Angriffstätigkeit mit volumetrisch dominierenden „Distributed-Denial-of-Service“ (DDoS-)Kampagnen, während Ransomware unter Wirkgesichtspunkten die folgenreichste Bedrohung bleibt.[31] Dass die EU ihre Instrumente für Vorfallsanalyse, Frühwarnung und Unterstützung parallel ausgebaut hat, ist deshalb nicht nur ordnungspolitisch bedeutsam, sondern unmittelbar operativ relevant. Zugleich bleiben Umsetzungslücken der Maßstab, an dem sich Handlungsfähigkeit

24 Vgl.: Europäische Union 2022b.
25 Vgl.: Europäische Union 2024a.
26 Vgl.: Europäische Union 2024b.
27 Vgl.: Europäische Union 2025.
28 Vgl.: Europäische Union 2022c; Europäische Kommission 2025a.
29 Vgl.: NIST 2024a; NIST 2024b; NIST 2024c; NIST 2024d.
30 Vgl.: Europäische Kommission 2025b.
31 Vgl. dazu die Berichte von EEAS 2025 und ENISA 2025a, b; zum Umgang anderer europäischer Staaten mit Ransomware vgl. die Leitlinien Irlands bzw. der Niederlande: National Cyber Security Centre (Irland) o.D. und National Cyber Security Centrum (Niederlande) 2022.

messen lassen muss. Mehrere Mitgliedstaaten – darunter Deutschland – verfehlten die Umsetzungsfrist der NIS-2-Richtlinie; die Europäische Kommission reagierte am 7. Mai 2025 mit begründeten Stellungnahmen an 19 Staaten, während der deutsche Regierungsentwurf erst am 30. Juli 2025 vom Bundeskabinett beschlossen wurde.[32]

Europa ist im Herbst 2025 widerstandsfähiger als noch vor wenigen Jahren. Jetzt kommt es darauf an, die neuen Regeln in verlässliche Routine zu überführen. Für die NATO heißt das: Ihre neuen Cyber-Einrichtungen für Lagehilfe, Unterstützung und freiwillige Beiträge der Mitgliedstaaten mit klaren Standardabläufen, regelmäßigen Vollübungen und realitätsnahen Tests in den Betrieb zu bringen. Für die EU heißt es: Die zentralen Cyber-Regelwerke so umzusetzen, dass die Zeiten bis zur Reaktion und bis zur Eindämmung eines Vorfalls messbar sinken; im Informationsraum muss der Digital Services Act zügig, einheitlich und gerichtsfest angewandt werden. Der gemeinsame Nenner ist Anschlussfähigkeit: solide technische „Basishygiene“ mit geprüften Bausteinen, klare rechtliche Schwellen und eine eingeübte Zusammenarbeit zwischen NATO-Mechanismen und EU-Krisenstrukturen. Genau an dieser Nahtstelle zeigt sich im Ernstfall, ob Regelwerke sich in Handlungsfähigkeit übersetzen.

3 Partnerarchitekturen im Vergleich: USA, Vereinigtes Königreich, Frankreich und die baltischen Staaten

Wer den Stand des militärisch-zivilen Handelns im Cyber- und Informationsraum nüchtern bemessen will, kommt an einem internationalen Vergleich nicht vorbei. Die im Folgenden schlaglichtartig in den Blick genommenen Fallstudien USA, Vereinigtes Königreich (UK), Frankreich und das Baltikum setzen an unterschiedlichen Punkten an – gemeinsam ist ihnen jedoch, dass Technik, Organisation, Recht und strategische Kommunikation als aufeinander bezogene Hebel gedacht werden. Entscheidend ist dabei nicht die Nachahmung einzelner Leuchtturm-Projekte, sondern die Ordnungsleistung dahinter: Eine Architektur, die Basisschutz, Führung und Rechtsklarheit, strategische Kommunikation und Bündnisfähigkeit als Bedingungen von Handlungsfähigkeit begreift.

Die Vereinigten Staaten koppeln eine vorwärtsgerichtete Doktrin mit diszipliniertem Betrieb.[33] „Defend Forward“ und „Persistent Engagement“ beschreiben eine proaktive Verteidigung, die gegnerische Aktivitäten früh beobachtet und stört – technisch, organisatorisch und kommunikativ.[34] Cyber-Kräfte sichern den Betrieb des Department of Defense Information Network (DoDIN), stören gegnerische Infrastruktur frühzeitig und gewinnen in Partnernetzen durch Hunt-Forward-Einsätze Lagebilder und Verteidigungsfähigkeit zurück.[35] 2022 entsandte die Cyber National Mission Force ihr bislang größtes Team nach Kiew; 2024 bilanzierte das United States Cyber Command (USCYBERCOM) Dutzende solcher Missionen mit Partnern in Europa und Asien.[36] Bemerkenswert ist die kommunikative Offenheit: Strategiedokumente und

32 Vgl.: Europäische Kommission 2025c.
33 Vgl.: U.S. Cyber Command 2018.
34 Vgl.: Nakasone 2019: 10–14; Fischerkeller/Harknett 2019: 267–287.
35 Vgl.: U.S. Cyber Command o.D.
36 Vgl.: U.S. Cyber Command 2024.

Kommandoerklärungen benennen Ziele, Grenzen und rechtliche Verankerung – das stärkt innenpolitische Akzeptanz und setzt nach außen glaubhafte Signale.

Das Vereinigte Königreich hat mit der National Cyber Force (NCF) eine eigenständige Organisation geschaffen, unter deren Dach Streitkräfte und der Nachrichtendienst Government Communications Headquarters (GCHQ) – rechtsgetrennt, operativ aber synchronisiert – defensive wie offensive Operationen führen.[37] Leitend ist das Selbstverständnis als „Responsible Cyber Power“: Ziele, Prinzipien und Grenzen werden transparent benannt, an Völkerrecht und parlamentarische Kontrolle gebunden und kommunikativ genutzt, um Legitimation und Abschreckung zu stärken.[38] Die Architektur koppelt defensive und offensive Optionen, ohne Zuständigkeiten zu verwischen – das GCHQ operiert nach Nachrichtendienstrecht, die Streitkräfte nach Militärrecht. Für Verbündete erzeugt das Vorhersehbarkeit; nach innen wie außen spannt es eine Brücke zwischen Abwehr, Attribution und öffentlicher Kommunikation.[39]

Frankreich setzt dem eine klare institutionelle Trennung entgegen: Die zivile Cybersicherheitsbehörde Agence nationale de la sécurité des systèmes d’information (ANSSI) verantwortet Schutz und Aufsicht in Staat und Wirtschaft, während das militärische Commandement de la cyberdéfense (COMCYBER) offensive Wirkungsmöglichkeiten führt.[40] Die Verteidigungsministerin legte 2019 die militärische Cyber-Doktrin offen – inklusive Bereitschaft zu offensivem Wirken im Konfliktfall, rechtlich eingehegt und politisch verantwortet.[41] Damit zielt Frankreich nicht auf Entgrenzung, sondern auf Normbindung: Offensive bleibt unterstützende Fähigkeit innerhalb verfassungs- und völkerrechtlicher Leitplanken.

Besonders instruktiv sind die baltischen Staaten, die Resilienz als Gesellschaftsaufgabe praktizieren.[42] Estland verbindet eine digitalisierte Verwaltung mit architektonischen Sicherungen – von der X-Road-Logik bis zur „Data Embassy“ in Luxemburg – und verankert zivilgesellschaftliche Expertise in der Cyber Defence Unit der Kaitseliit.[43] Diese Freiwilligenstruktur trainiert regelmäßig, kann im Krisenfall eingebunden werden und erleichtert es dem Staat, Kompetenzen aus der Privatwirtschaft in Plan- und Lageprozesse hineinzuziehen.[44] Entscheidend ist die Normalität des Einübens: Technik, Verfahren und Kommunikation werden gemeinsam erprobt, Lücken diskutiert. So entsteht ein robuster Grundbetrieb, der Störungen absorbiert und Wiederanlaufzeiten verkürzt. Zugleich ermöglicht die Datenarchitektur staatliche Handlungsfähigkeit unter physischem Druck; Sicherungskopien außerhalb der Landesgrenzen machen die Verwaltung dauerhaft anschluss- und rekonfigurationsfähig.

Lettland und Litauen haben parallel die kognitive Flanke institutionell stark gemacht. In Riga bündelt das NATO Strategic Communications Centre of Excellence (NATO StratCom COE) Forschung, Ausbildung und Doktrinentwicklung zu

37 Vgl.: National Cyber Force (UK) 2023; Clark 2025.
38 Vgl.: Clark 2025.
39 Vgl.: Stevens et al. 2023.
40 Vgl.: Agence nationale de la sécurité des systèmes d’information (ANSSI) 2023; Ministère des Armées (COMCYBER) o.D.; vertiefend zur französischen Cyberarchitektur: International Institute for Strategic Studies (IISS) 2021: 57–67.
41 Vgl.: Parly 2019; Ministère des Armées/COMCYBER 2019.
42 Vgl.: Magnuson/Keay/Metcalf 2022: 27–52.
43 Siehe Estonian Defence League o.D.
44 Vgl.: Kaska/Osula/Stinissen 2013.

strategischer Kommunikation und Desinformationsabwehr;[45] seine Arbeit fließt über Standardisierung, Kurse und Übungen in die Allianz zurück und schärft den Blick auf Wahl- und Krisenkontexte. Litauen beschleunigte die Verzahnung von Nachrichtengewinnung, technischer Abwehr und öffentlicher Kommunikation und übt regelmäßig ressortübergreifend.[46] Beide Staaten investieren in Medienkompetenz und Bürgerbeteiligung, um die Anfälligkeit für Manipulation zu verringern. Politisch entscheidend ist der Modus: Statt spektakulärer Leuchtturmprojekte steht eine Pflege der Alltagsrobustheit im Vordergrund – Lagebeobachtung, frühzeitige Attribution, Verfahrenslinien und das Einbinden privater Betreiber. So entsteht eine widerstandsfähige Gesamtarchitektur, die digitale, physische und kognitive Dimensionen zusammenführt und Bündnisinteroperabilität herstellt.

Was lässt sich aus diesen Fallskizzen abstrahieren? *Erstens*: Wirkung im Cyber- und Informationsraum entsteht aus gehärteten Grundlagen und eingeübten Übergängen; wo standardisierte Wiederanlaufverfahren (Recovery-Standard Operating Procedures, SOPs), konsequente Netzsegmentierung sowie eine durchgängige Führung von IT-Beständen, Patch-Ständen und Konfigurationen gelebte Praxis sind, schrumpfen die Zeit bis zur Reaktion („Time to React“) und bis zur Eindämmung eines Vorfalls („Time to Contain“). *Zweitens*: Aktive Optionen – also Maßnahmen, die gegnerische Aktivitäten frühzeitig beobachten, stören oder öffentlich adressieren – gewinnen strategische Qualität nur, wenn Führung, Recht und Kommunikation vorausgebaut sind; andernfalls erzeugen sie innenpolitische Fragilität und außenpolitische Ambivalenz. *Drittens*: Bündnisfähigkeit ist Designvorgabe; Zusagen müssen technisch, rechtlich und prozedural so hinterlegt sein, dass sie im Verbund ohne Reibungsverlust greifen. *Viertens*: Strategische Kommunikation ist Sicherheitsfunktion – sie beschleunigt Attribution, macht Normverletzungen sichtbar, erklärt Verfahren und stabilisiert Legitimation im Alltag wie in der Krise.

4 Deutschland im Belastungstest: Nahtstellenverluste, Strukturdefizite, Lernfelder

Im Spiegel des voranstehenden Vergleichs zeigt sich Deutschlands Schwäche im Cyber- und Informationsraum weniger als Mangel an Einsicht oder Strukturen denn als Defizit von Systemintegration: Koordinations- und Lageformate bestehen, doch die Verzahnung von Doktrin, Organisation, Recht und strategischer Kommunikation bleibt an föderalen Schnittstellen unvollständig – genau dort, wo hybride Lagen schnelle, rechtsklare Übergänge von der Lagekoordination zur mandatierten Führungs- und Eingriffsarchitektur verlangen.[47] Das ist besonders folgenreich, weil Deutschland doppelt exponiert ist: innen als hochvernetzte, innovations- und exportstarke Volkswirtschaft mit großer Angriffsfläche, außen als tragender Pfeiler europäischer Stabilität mit hohem Erwartungsdruck auf Resilienz und Bündnisfähigkeit.[48] Die im Folgenden skizzierten empirischen Befunde – wiederkehrende Vorfälle in staatlichen Institutionen und

45 Vgl.: NATO StratCom COE o.D. b.
46 Vgl.: Ministry of National Defence of the Republic of Lithuania 2025.
47 Zu Deutschland vgl. einführend vor allem die Arbeiten Sven Herpigs: Herpig 2023; Herpig/Dutke 2023.
48 Vgl.: Deutscher Bundestag 2025a, c; Bundesregierung 2023.

Kritischer Infrastruktur, die vorhandenen Strukturmechanismen sowie die Evaluierung der „Cybersicherheitsstrategie für Deutschland 2021“ (CSS) von August 2025 – deuten konsistent auf dieselbe Nahtstelle: Es fehlen rechtsklare, geübte Schwellen-Standard Operating Procedures und eine operativ verankerte Fähigkeit zur strategischen Kommunikation, die Koordination in verantwortliche Führung übersetzen.[49]

Seit 2019 mehren sich Störungen in Verwaltung, staatlichen Institutionen und Daseinsvorsorge: Beim Berliner Kammergericht führten kompromittierte IT-Systeme zu monatelangen Ausfällen, fehlende Backups und Notfallpläne erschwerten die Wiederherstellung.[50] Ein vertraulicher Bericht des Bundesrechnungshofs vom Juli 2025 konstatiert ein „dramatisches Umsetzungsdefizit“: Weniger als zehn Prozent von rund einhundert Bundesrechenzentren erfüllen die Mindeststandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI); teils fehlt Notstrom, Recovery-Tests und belastbare Asset-Verzeichnisse sind häufig unzureichend.[51] In der Kritischen Infrastruktur legte Anfang 2022 ein Angriff auf die Firma Oiltanking Teile der Tanklogistik lahm[52] – mit Auswirkungen auf hunderte Tankstellen –, und im Oktober 2022 verursachten koordinierte Kabelsabotagen bei Herne und Berlin-Karow einen großflächigen Ausfall des Zugfunks[53] (GSM-R) mit massiven Störungen im Bahnverkehr Norddeutschlands. Zusammengenommen weisen diese Befunde auf Lücken im Basisschutz, in der Wiederanlauf- und Prüfpraxis sowie in der Bestandsführung hin – quer durch Verwaltung und Betreiberumfelder.

Digitale und physische Wirkdimensionen überlagern sich zunehmend: Störungen an Energie- und Kommunikationsnetzen, das Ausspähen und Stören durch unbemannte Luftfahrtsysteme (Unmanned Aircraft Systems, UAS) über sensiblen Arealen sowie die Verwundbarkeit maritimer/submariner Infrastrukturen (Unterseekabel, Pipelines) erweitern das Angriffsspektrum über den Cyberraum hinaus in die physische Domäne.[54] Solche Lagen sind nicht allein technisch zu lösen; sie verlangen rechtsklare, geübte Übergänge zwischen Lagekoordination und mandatierter Eingriffsbefugnis – mit eindeutig beschriebenen Zuständigkeiten, Prüfschritten, Freigabeketten und Amtshilfewegen zwischen Polizei, Verfassungsschutz, Nachrichtendiensten, Bundeswehr und Ländern unterhalb der Landes- und Bündnisverteidigung (LV/BV).[55] Konkret fehlen bundeseinheitliche Schwellen-Standard-Operating-Procedures, also standardisierte Abläufe für klar definierte Eingriffs- und Eskalationspunkte – etwa für das zeitkritische Eindämmen komplexer, langfristig angelegter Cyberoperationen (Advanced Persistent Threat, APT), für die Abwehr unbemannter Luftfahrtsysteme im Inland (UAS-Abwehr, einschließlich abgestufter Optionen bis hin zum kinetischen, also physischen Eingriff) sowie für den Schutz maritimer und submariner Infrastrukturen wie Unterseekabel und Pipelines. Vorhandene Koordinations- und Lageformate verbessern

49 Vgl.: Bundesministerium des Innern 2025.
50 Vgl.: Senatsverwaltung für Justiz Berlin 2020; T-Systems 2019; Kiesel/Keilani 2019.
51 Vgl.: Kannenberg 2025; Hensiek 2025; Menhard/Meister 2025.
52 Vgl.: Pearson 2022; Payne 2022.
53 Vgl.: Litschko 2022.
54 Vgl.: ENISA 2025b; Kim 2024; Voelsen (Hg.) 2024; vgl. in diesem Zusammenhang auch die Gründung des Maritime Centre for Security of Critical Undersea Infrastructure: NATO Allied Maritime Command 2024; das Fallbeispiel Finnlands ist hier besonders eindrücklich (Klarhoefer, Lavinia/Leuchtenmüller 2025).
55 Vgl. vor diesem Hintergrund den jüngst beschlossenen Gesetzentwurf zum KRITIS-Dachgesetz: Bundesministerium des Innern 2025a.

Informationsaustausch und Sensibilisierung, ersetzen jedoch keine exekutiv mandatierte Führungs- und Eingriffsarchitektur, die diese Übergänge bundeseinheitlich beschreibt, anordnet und regelmäßig übt.

Parallel hat sich die kognitive Dimension zur strategischen Flanke entwickelt: Professionalisierte Desinformationskampagnen, „Hack-&-Leak"-Formate und einschüchternde Phishing-Operationen zielen nicht nur auf Informationsdiebstahl, sondern auf Legitimität, Vertrauen und Entscheidungsfähigkeit.[56] Zäsuren – vom „Fall Lisa" (2016)[57], auf Mandatsträgerinnen und Mandatsträger zielende „Ghostwriter"-Aktivitäten[58] bis zu verstärkten Operationen im Umfeld der Bundestagswahl 2021 – zeigen, dass hier Attribution, rechtliche Einordnung und öffentliche Kommunikation in Stunden- und nicht in Wochenlogik zusammenfinden müssen.

Deutschland verfügt über leistungsfähige Inseln (u. a. im Auswärtigen Amt und in der Taskforce gegen Desinformation im BMI), es existiert jedoch keine mandatierte operative Fähigkeit zur strategischen Kommunikation mit Krisen-Standard Operating Procedures, geübten Freigabeketten und ressort-/ebenenübergreifender Führungslinie, die technische Lage, juristische Bewertung, Plattform-Liaison und Krisenkommunikation integriert. Anders als Staaten mit ausgewiesenen Kapazitäten – etwa die britische 77th Brigade[59] oder Schwedens Myndigheten för psykologiskt försvar (MPF)[60] – bleibt die deutsche Reaktionsarchitektur in der kognitiven Dimension fragmentiert: Vorhandene Koordinationsformate sensibilisieren, ersetzen aber keine dauerhafte Einsatz- und Verantwortungsstruktur, die Attribution beschleunigt, Normverletzungen sichtbar macht und legitime Gegenmaßnahmen kommunikativ trägt.

Flankierend wirkt eine persistente Lage von Cyber- und Wirtschaftsspionage, die weniger in spektakulären Einzelfällen als in kumulativen Erosionsprozessen sichtbar wird: Staatlich gesteuerte oder geduldete Akteure – vornehmlich aus Russland und China – zielen systematisch auf Schlüsselindustrien, Forschungseinrichtungen und behördennahe Schnittstellen.[61] Ausgenutzt werden veraltete, schwer modernisierbare IT-Infrastrukturen (Legacy-Systeme), unzureichend gesicherte Administrator- und Hochprivilegienkonten (Privileged-Access-Kontrollen), Abhängigkeiten von Dienstleistern und Zulieferern (Third-Party-/Supply-Chain-Risiken) sowie manipulative Angriffe auf Beschäftigte (Social Engineering); unvollständige Verzeichnisse der IT-Bestände und lückenhafte Update- und Patch-Routinen erleichtern diese Operationen.

Die Folgen reichen über unmittelbare Schäden hinaus: Know-how-Abflüsse schwächen technologische Souveränität – also die Fähigkeit, zentrale Schlüsseltechnologien eigenständig zu entwickeln, zu betreiben und weiterzuentwickeln –, verschieben Wettbewerbsvorteile und erhöhen strategische Abhängigkeiten. Positiv ist die deutsche Mitwirkung am EU-Sanktionsregime gegen Cyber-Akteure seit 2020 – etwa im Kontext der China zugeschriebenen Spionagekampagne „Operation Cloud Hopper" (2020/21)[62]

56 Vgl. dazu einführend: Smirnova 2025.
57 Vgl.: Meister 2016; Schaubert 2018.
58 Vgl.: Cerulus/Klingert 2021; German Marshall Fund, Alliance for Securing Democracy (ASD) o.D.; Verfassungsschutz Baden-Württemberg 2021.
59 Vgl.: British Army o.D.
60 Vgl.: Swedish Psychological Defence Agency (MPF) 2025.
61 Vgl: Bundesamt für Verfassungsschutz (BfV) 2025: 303–323; siehe dazu auch den BfV-Sicherheitshinweis für Wirtschaft, Politik & Verwaltung 2023 (Bundesamt für Verfassungsschutz 2023).
62 Vgl.: Europäischer Rat/Rat der Europäischen Union 2020.

–, doch bleibt ohne robuste Schutzprogramme in Verwaltung und Unternehmen, ohne standardisierten Informationsaustausch zwischen Staat und Wirtschaft sowie klare außenpolitische Signale an staatlich gesteuerte Tätergruppen ein schleichender Verlust an Innovations- und Sicherheitsfähigkeit bestehen. Damit verstärkt diese Spionagelage die bereits diagnostizierten Grundbetriebslücken (unzureichender Basisschutz, langsamer Wiederanlauf, lückenhafte Bestandsführung) und verschärft die Anforderungen an rechtsklare, geübte Verfahren, die an der Schnittstelle von technischer Abwehr, Strafverfolgung, Nachrichtengewinnung und strategischer Kommunikation Zuständigkeiten, Meldewege und Entscheidungsbefugnisse eindeutig beschreiben.

Querschnittlich treten Struktur- und Schnittstellenprobleme zutage, die weniger das Ob von Zuständigkeiten als deren Verzahnung betreffen: Im föderalen Gefüge teilen sich Polizei/Gefahrenabwehr, Verfassungsschutz und Nachrichtendienste, das Bundesamt für Sicherheit in der Informationstechnik sowie die Bundeswehr Aufgaben im Cyber- und Informationsraum. Vorhandene Gremien und Lageformate koordinieren – eine exekutiv mandatierte Führungs- und Eingriffsarchitektur unterhalb von Landesverteidigung/Bündnisverteidigung, die rechtsklare, geübte Schwellen-Standard Operating Procedures definiert und anordnet, fehlt jedoch. Dadurch ziehen sich Entscheidungswege an neuralgischen Übergängen in die Länge, insbesondere dort, wo Prüfschritte, Freigabeketten und Amtshilfe ressort- und ebenenübergreifend zusammenfallen müssen. Ein typischer Belastungstest ist eine laufende APT-Operation (Advanced Persistent Threat) gegen Regierungsnetze: Sie verlangt strafprozessuale Maßnahmen (Bundeskriminalamt), abwehr- und nachrichtendienstliche Aufklärung (Bundesamt für Verfassungsschutz/Bundesnachrichtendienst) sowie – je nach Lage – militärische Fähigkeiten, die zeitkritisch orchestriert werden müssen. Ohne bundeseinheitlich geübte Übergangs- und Eingriffsverfahren bleiben Zuständigkeitsgrenzen im Graubereich unscharf. Vor diesem Hintergrund ist nicht die Existenz von Koordinationsstrukturen das Problem, sondern deren operative Anschlussfähigkeit an eine verantwortliche Führungslinie, die Geschwindigkeit rechtssicher macht.

Ansätze zur besseren Koordinierung existieren – als Lage- und Austauschformate, nicht als operative Einsatzführung. Den übergreifenden Rahmen bildet die „Cybersicherheitsstrategie für Deutschland 2021“[63] (CSS); sie ersetzt die Fassung von 2016, richtet das Regierungshandeln bis 2026 aus, bündelt vier Leitlinien (gemeinsame Aufgabe, digitale Souveränität, sichere Digitalisierung, Messbarkeit/Transparenz) und hinterlegt Ziele mit Indikatoren, Berichtswesen und Evaluierung.[64] Unter Leitung des BMI steuert die Arbeitsgruppe „Hybride Bedrohungen“ (AG Hybrid)[65] den strategischen Umgang; auf Arbeitsebene koordiniert eine wöchentlich tagende Taskforce gegen Desinformation[66] und weitere hybride Bedrohungen das operative Vorgehen – einschließlich des Schutzes von Wahlen. In der Struktur der Innenministerkonferenz vernetzt die Bund-Länder-offene Arbeitsgruppe „Hybride Bedrohungen“ (BLoAG Hybrid)[67] Bund, Länder, Sicherheitsbehörden und kommunale Spitzenverbände und erarbeitet den „Gemeinsamen Aktionsplan von Bund und Ländern gegen Desinformation und für eine

63 Vgl.: Bundesminister des Innern, für Bau und Heimat 2021; zur Kritik vgl.: Bendiek/Schulze 2021.
64 Zur Kritik an der anfänglichen Vernachlässigung des Cyberraums: Schulze/Herpig 2018.
65 Vgl.: Deutscher Bundestag 2025c.
66 Vgl.: ebd.
67 Vgl.: ebd.

wehrhafte Demokratie“. Ergänzend erstellt die Bundesregierung im Regelfall zweiwöchentlich einen Lagebericht „Hybride Bedrohungen“ (VS NfD); ein ressortübergreifendes Lagebild von Bundesamt für Verfassungsschutz/Bundeskriminalamt sollte zur IMK-Herbstsitzung 2025 vorliegen. Seit Februar 2024 betreibt das Bundesamt für Sicherheit in der Informationstechnik das Nationale IT-Lagezentrum[68] als dauerhaftes Lage- und Kooperationshub; in Krisensituationen wird es zum Nationalen IT-Krisenreaktionszentrum[69] hochgefahren. Flankierend wirken der Nationale Cyber-Sicherheitsrat (NCSR)[70] – strategische Bündelung unter Vorsitz des Beauftragten der Bundesregierung für Informationstechnik (BfIT) – und das Nationale Cyber-Abwehrzentrum (NCAZ)[71] als behördenübergreifende Kooperationsplattform. Diese Formate verbessern Informationsaustausch und Sensibilisierung, ersetzen aber keine rechtsklare, mandatierte Führungs- und Eingriffsarchitektur für schwere Cyber- und Hybridlagen.

Die Evaluation der Cybersicherheitsstrategie 2021 (Datenstand: Juni 2025) zieht ein gemischtes Fazit:[72] Von 178 Maßnahmen sind nach Ressortangaben rund drei Viertel abgeschlossen oder in Arbeit; spürbare Fortschritte gibt es bei Wirtschaft/Kritischer Infrastruktur und in der EU-Zusammenarbeit – etwa durch eine intensivere Nutzung von Angeboten des Bundesamts für Sicherheit in der Informationstechnik und Fortschritte bei der Umsetzung der Richtlinie NIS-2 zur Netz- und Informationssicherheit. Schwachpunkt bleibt die föderale Architektur: Eine Verfassungsänderung zur Stärkung des Bundesamts für Sicherheit in der Informationstechnik kam nicht zustande, kooperative Formate wachsen nur schrittweise. Externe Rückmeldungen verdeutlichen zudem eine Wirkungslücke: Die Effekte „abgeschlossener“ Maßnahmen werden mehrheitlich bestätigt (82 Prozent), „laufende“ Maßnahmen erzielen deutlich seltener wahrnehmbare Wirkung (35 Prozent), und bei „geplanten“ Maßnahmen sehen rund zwei Drittel der Befragten noch keine Effekte. Kritik richtet sich unter anderem gegen den Nationalen Cyber-Sicherheitsrat als strategisches Steuerungsgremium, gegen unklare Zertifizierungspfade sowie die geringe Einbindung kleiner und mittlerer Unternehmen (KMU); besonders umstritten sind die Ausgestaltung der Telematikinfrastruktur im Gesundheitswesen und der Umgang mit Coordinated Vulnerability Disclosure (CVD), also koordinierte Verfahren zum verantwortlichen Melden und Schließen von IT-Schwachstellen. Insgesamt bestätigt die Evaluation damit den Engpass an föderalen Nahtstellen: Koordination funktioniert, doch ohne rechtsklare, regelmäßig geübte Standardverfahren an den Eingriffsschwellen und eine exekutiv mandatierte Eingriffsarchitektur bleibt die operative Handlungsfähigkeit begrenzt.

Vor dem Hintergrund dieses Befunds markiert die Aufwertung des Cyber- und Informationsraums zur eigenständigen Teilstreitkraft (TSK CIR)[73] im Frühjahr 2024 einen wichtigen – gleichwohl sektoral begrenzten – Fortschritt. Der seit 2017 bestehende Organisationsbereich steht nun formal auf einer Stufe mit Heer, Luftwaffe und Marine.

---

68 Vgl.: BSI o.D. c.
69 Vgl.: BSI o.D. a.
70 Vgl.: Der Beauftragte der Bundesregierung für Informationstechnik (BfIT) o.D.
71 Vgl.: BSI o.D. b.
72 Vgl.: Bundesministerium des Innern 2025b; methodisch stützt sich die Evaluation auf standardisierte Befragungen von 21 Ressorts sowie Akteuren aus Ländern, Wirtschaft, Wissenschaft und Zivilgesellschaft.
73 Vgl.: Bundeswehr o.D. b; zu den Herausforderungen für die Bundeswehr vgl. die konzise Bestandsaufnahme von Ludwig Leinhos (2020), die auch 2025 noch aktuell ist.

Zentraler operativer Kern ist das Zentrum Cyber-Operationen (ZCO): Es bündelt die Vorbereitung und Durchführung militärischer Cyber-Operationen – von der Aufklärung über unterstützende Maßnahmen bis hin zu Wirkungen in fremden Systemen; in klar definierten rechtlichen und politischen Grenzen umfasst dies auch offensive Fähigkeiten im Rahmen von Landes- und Bündnisverteidigung.[74] Militärisch ist damit ein Offensivpfad eingehegt und kommunizierbar.[75] Unterhalb dieser Schwelle bleibt jedoch die zivilbehördliche aktive Cyberabwehr im Frieden nicht kodifiziert: Es fehlen bundeseinheitliche, rechtsklare Standard Operating Procedures, Zuständigkeits- und Freigabeketten samt parlamentarischer Einbettung. Die oft politisierte Chiffre „Hackback" verfehlt insofern den Kern des Problems; erforderlich ist eine präzise, abgestufte Eingriffsordnung, die Recht, Kontrolle und Kommunikation zusammenführt. Konsequenz: Die Teilstreitkraft Cyber- und Informationsraum bzw. das Zentrum Cyber-Operationen schließen eine militärische Fähigkeitslücke, ersetzen aber keine nationale Führungs- und Eingriffsarchitektur für hybride Lagen unterhalb von Landes- und Bündnisverteidigung – und beantworten auch nicht die offene Frage der institutionellen Aufstellung strategischer Kommunikation, die für Attribution, Legitimation und internationale Anschlussfähigkeit nötig wäre.

Die Summe der Befunde ergibt ein nüchternes Zwischenurteil: Nicht Einsicht fehlt, sondern Implementierungs- und Kohärenzfähigkeit. Deutschland verfügt zwar über starke Elemente – von der neuen Bundeswehr-Teilstreitkraft Cyber mit ihrem Zentrum für Cyber-Operationen über Bund-Länder-Formate zu hybriden Bedrohungen bis zum IT-Lage-/Krisenzentrum, dem Cyber-Sicherheitsrat und dem Cyber-Abwehrzentrum –, doch ohne eine rechtsklare, mandatierte Führungs- und Eingriffsordnung unterhalb von Landes- und Bündnisverteidigung, ohne bundeseinheitlich geübte Standardabläufe an den entscheidenden Schwellen und ohne eine operativ verankerte strategische Kommunikation bleibt es bei Koordination ohne Führungsfähigkeit – daher rührt die Wirkungslücke in der CSS-Evaluierung 2025. Fortschritt muss über wenige robuste Größen sichtbar und steuerbar werden: Erfüllung der Mindeststandards des Bundesamts für Sicherheit in der Informationstechnik, kürzere Patch-Fristen sowie sinkende Zeiten bis zur Eindämmung und bis zur Wiederherstellung, flächendeckende Standardabläufe (etwa für die Eindämmung komplexer Angriffe, die Drohnenabwehr im Inland und den Schutz von Untersee-Infrastruktur), höhere Übungsdichte einschließlich Kommunikationsmodulen sowie nachgewiesene Anschlussfähigkeit an NATO-Unterstützungsmechanismen wie freiwillig bereitgestellte Cyber-Wirkungen und die virtuelle Unterstützungsfähigkeit bei Cyber-Zwischenfällen. An diesen Indikatoren sind Handlungsempfehlungen auszurichten – damit Wirkung nicht behauptet, sondern regelmäßig nachgewiesen und politisch verbindlich gesteuert wird.

---

74 Vgl.: Bundeswehr o.D. a; zum Verhältnis von Cyber-Operationen und internationalem Recht vgl.: Mačák/Dias/Kasper 2025.

75 Zum Diskurs um die juristische Bewertung von Hackbacks/Offensiv-Operationen vgl.: Schmoldt 2024: 165–182; Schulze 2020; Herpig 2023; Kipker 2019; gegen Hackbacks als Verteidigung positioniert sich Constanze Kurz 2024; vgl. in diesem Zusammenhang auch das Positionspapier des Auswärtigen Amts (2021); wichtige Grundlage dafür war der Band von Michael N. Schmitt 2017.

5 Umsetzungsarchitektur 2025–2030: kohärent, messbar, bündnisfähig

Die Analyse der vorangegangenen Abschnitte hat die Nahtstellenverluste sichtbar gemacht: Zwischen Technik, Organisation, Recht und strategischer Kommunikation entstehen gerade an föderalen Übergängen jene Reibungen, die in hybriden Konfliktlagen Zeit kosten und Verantwortung verunklaren. Der folgende Abschnitt setzt genau hier an. Er übersetzt die gewonnenen Einsichten in eine Umsetzungsarchitektur, die die Lücken in der Reihenfolge schließt, in der sie operative Wirkung entfalten: zuerst ein gehärteter Grundbetrieb und verlässlicher Wiederanlauf, dann rechtsklare Führung mit beschriebenen Eingriffsschwellen und Standardabläufen, sodann eine mandatierte operative strategische Kommunikation und schließlich die nachweislich eingeübte Anschlussfähigkeit an Bündnis- und EU-Verfahren.

(1) Nationale Führungsarchitektur: Führung bündeln, Schwellen klären. Eine ständige Führungsordnung im Kanzleramt verbindet strategische Lagebeurteilung und operative Einsatzführung und kann binnen Stunden in den Krisenmodus schalten. Herzstück ist eine dreistufige Eingriffsschwellen-Matrix – präventiv (Vorsorge, Härtung, Visibilität), aktiv (zeitkritische Gefahrenabwehr unter Aufsicht), reaktiv (bündnis- und völkerrechtskonforme Gegenmaßnahmen) – mit klaren Zuständigkeiten, Prüfschritten und Freigabeketten sowie festen Amtshilfewegen zwischen Bund und Ländern. Standard Operating Procedures sind für jede Stufe verbindlich; bestehende Formate werden eingebunden statt ersetzt: die Arbeitsgruppe „Hybride Bedrohungen“ im Bundesministerium des Innern, die Bund-Länder-offene Arbeitsgruppe „Hybride Bedrohungen“ in der Struktur der Innenministerkonferenz, der Nationale Cyber-Sicherheitsrat als strategisches Dach, das Nationale Cyber-Abwehrzentrum als Kooperationsplattform, das Computer Emergency Response Team des Bundes (CERT-Bund) als operative Drehscheibe und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) als Forschungs- und Entwicklungspartner. Das beim Bundesamt für Sicherheit in der Informationstechnik angesiedelte Nationale IT-Lagezentrum fungiert kontinuierlich als Lage- und Kooperationshub und wird im Notfall zum Nationalen IT-Krisenreaktionszentrum hochgefahren.

(2) Rechtsklarheit: Handlungsformen staffeln, Kontrolle sichern. Ein Cyber-Einsatzgesetz kodifiziert abgestufte Handlungsformen, vermeidet Eskalationsrhetorik und verankert parlamentarische Kontrolle. Präventive Maßnahmen dienen der Gefahrenvorsorge in eigenen und unterstützten Netzen, knüpfen an enge Voraussetzungen und strenge Dokumentations- und Berichtspflichten an. Aktive Maßnahmen erlauben zeitkritische Gefahrenabwehr im Inland mit Aufsichts- und gegebenenfalls richterlicher Kontrolle. Reaktive Maßnahmen – Gegenmaßnahmen im Rahmen des Völkerrechts – werden vorzugsweise bündniseingebettet gedacht; sie setzen auf klare Freigabeketten und transparente Kommunikation. Flankierend präzisiert das Gesetz Abwehrbefugnisse gegenüber unbemannten Luftfahrtsystemen (Unmanned Aircraft Systems, UAS) im Inland, Schutz- und Eingriffsrechte in maritimen und submarinen Infrastrukturen sowie standardisierte Amtshilfewege, damit Verantwortlichkeit greifbar und Geschwindigkeit rechtssicher wird.

(3) Robuster Grundbetrieb: Betriebssicherheit als Priorität. Ein Programm „Basisschutz & Wiederanlauf“ verpflichtet Verwaltungen und Betreiber Kritischer Infrastrukturen, Redundanzen bei Energieversorgung und Netzanbindung vorzuhalten, Netze konsequent zu segmentieren, IT-Bestände, Patch-Stände und Konfigurationen durchgängig zu führen sowie gehärtete Offline-Backups und regelmäßig geübte Wiederanlauf-Prozeduren zu etablieren. Die Messgrößen bleiben bewusst knapp: Audit-Erfüllung gegenüber einschlägigen Mindeststandards, sinkende Patch-Latenzen, eine halbierte durchschnittliche Wiederanlaufzeit (Mean Time to Recover, MTTR) und eine verkürzte Zeit bis zur Eindämmung schwerer Vorfälle („Time to Contain“). Entscheidend ist, dass diese Kennziffern nicht nur erhoben, sondern aktiv gesteuert werden – als Grundlage einer Betriebskultur, die das Einüben von Verfahren zur Routine macht.

(4) Personal und Reserve: Fähigkeiten modular und abrufbar machen. Eine Personal- und Reservestrategie verbindet Seiteneinstieg mit klaren Kompetenzprofilen in Betrieb, Forensik und Incident Response sowie attraktiven Wechsel- und Qualifizierungspfaden zwischen Hochschulen, Verwaltung und Bundeswehr. Eine rechtsklare, regelmäßig übende Cyber-Reserve wird modular aufgebaut – etwa in CERT-, Forensik- und Lage-Teams – und über definierte Abrufkorridore in die Führungsarchitektur integriert. Das verkürzt die Zeit bis zur Einsatzfähigkeit, stabilisiert Wiederanlaufprozesse und schließt Schnittstellen zu Wirtschaft und Wissenschaft, ohne Zuständigkeiten zu verwischen.

(5) Strategische Kommunikation: Kognition als Sicherheitsfunktion. Strategische Kommunikation ist hier eine operative Fähigkeit, die technische Lage, Attribution, rechtliche Bewertung, Plattform-Liaison und Krisenkommunikation synchronisiert und ressort- wie ebenenübergreifend führt. Ein entsprechend ausgestattetes Zentrum hält belastbare Standard Operating Procedures für Wahl- und Krisenkontexte vor, ist in Übungen von NATO und EU eingebunden und macht Normverletzungen rasch sichtbar. So werden Legitimation gesichert, Entscheidungen beschleunigt und Desinformationskampagnen ihrer politischen Dividende beraubt.

(6) Bündnisfähigkeit: Andocken ohne Reibung, Beiträge verlässlich liefern. Nationale Verfahren und Systeme müssen an das NATO Integrated Cyber Defence Centre friktionsarm andocken, um Verteidigungs-, Lagefeststellungs- und -beurteilungsprozesse zu beschleunigen.[76] Für die „Sovereign Cyber Effects Provided Voluntarily by Allies“ beschreibt Deutschland ein Beitragsprofil mit Anwendungsfällen, Rules of Engagement und Freigabeketten, das Souveränität wahrt und parlamentarische Kontrolle sichert. Die „Virtual Cyber Incident Support Capability“ wird organisatorisch und technisch als „Clearing-House“ verankert, damit Expertise, Forensik und Nachrichtengewinnung im Ernstfall schnell zufließen – und aus Deutschland heraus bereitgestellt werden können. Militärisch bieten die Teilstreitkraft Cyber- und Informationsraum und das Zentrum Cyber-Operationen Planungsfähigkeit; entscheidend ist deren rechtsklare, kommunikativ flankierte Nutzung im Bündnisrahmen.

76 In diesem Zusammenhang dürfte die Auswertung der diesjährigen Cyber-Abwehrübung „Locked Shields 2025“ einige interessante Einsichten bringen, vgl.: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2025.

(7) Innovation: „Pilot-to-Production“ mit Sicherheitsgitter. Prototypen werden unter Realbedingungen erprobt, erst nach belastbarem Übungs- und Red-Teaming-Nachweis in den Wirkbetrieb gehoben und anschließend über einen Beschleunigungspfad skaliert. Lieferkettenprüfungen, verpflichtende Software-Stücklisten (Software Bill of Materials, SBOM) und Zertifizierung verankern Security-by-Design in Vergaben. Prioritäten liegen auf Post-Quanten-Kryptografie in Regierungsnetzen – anschlussfähig an internationale Standardisierungen – und auf lernender Detektion in Security Operations Center. So werden die europäischen Ordnungen – die zweite Richtlinie über Netz- und Informationssicherheit, der Cyber Resilience Act, der Cyber Solidarity Act sowie sektorspezifische Rahmen wie der Digital Operational Resilience Act und die Aufsichtslogik des Digital Services Act – nicht nur formal erfüllt, sondern operativ wirksam.

(8) Rechenschaft und Steuerung: Wenige Kennzahlen, klare Ampel. Damit Fortschritt steuerbar bleibt, braucht es eine einfache, aber verbindliche Rechenschaftslogik. Ein jährlicher Fähigkeitsbericht zum Cyber- und Informationsraum an Bundestag und Bundesrat verknüpft wenige robuste Kennziffern, Übungsdichte einschließlich eines Moduls für strategische Kommunikation sowie den dokumentierten Status der „Sovereign Cyber Effects Provided Voluntarily by Allies“- und „Virtual Cyber Incident Support Capability“-Readiness – mit einer Ampellogik, die Engstellen priorisiert und Ressourcen dorthin lenkt, wo die Wirkung noch ausbleibt. Das ist die nationale Übersetzung des Cyber Defence Pledge: Fortschritte sichtbar machen, Lücken schließen, Zusagen einlösen.

(9) Zeitlogik: Geschwindigkeit an Tragfähigkeit binden. Bis Ende 2026 steht die Führungsarchitektur im Regelbetrieb, die Eingriffsschwellen-Matrix ist verbindlich, erste Audit-Wellen laufen, und ein nationales Vollszenario testet Lage-, Einsatz- und Kommunikationsfähigkeit. Bis Ende 2029 sind das Cyber-Einsatzgesetz in Kraft, Abwehrbefugnisse gegenüber UAS, der Schutz maritimer und submariner Infrastrukturen sowie standardisierte Amtshilfewege rechtsklar, das Zentrum Strategische Kommunikation arbeitet im Schichtbetrieb, eine funktionsfähige Cyber-Reserve ist etabliert, und das „Sovereign Cyber Effects Provided Voluntarily by Allies“-Beitragsprofil wie auch die „Virtual Cyber Incident Support Capability“-Andockfähigkeit sind eingeübt. Ab 2030 beginnt der Wirkbetrieb: Prüfkriterien werden in großer Breite erfüllt, Patch- und Wiederanlaufzeiten sinken, lernende Detektion ist in zentralen Security Operations Center produktiv, und die jährliche Vollübung integriert Bund, Länder, Betreiber und Verbündete.

Am Ende zählt, ob Deutschland innen robust und außen anschlussfähig ist. Die hier skizzierte Ordnung ersetzt Schlagworte durch Verfahren, baut auf die Beharrlichkeit des Einübens statt auf Ankündigungen und hält das Versprechen liberaler Staatlichkeit ein: schnell zu handeln, ohne das Recht zu verlassen; wirksam zu sein, ohne die Kontrolle zu verlieren; Bündnisfähigkeit zu zeigen, ohne Souveränität zu verspielen. Darin liegt der nüchterne Kern strategischer Handlungsfähigkeit im Cyber- und Informationsraum.

6 Fazit: Innen robust, außen anschlussfähig

Deutschlands Handlungsfähigkeit im Cyber- und Informationsraum hat einen doppelten Prüfstein: Innen muss Staatlichkeit mit Wirtschaft und Gesellschaft unter Dauerlast verlässlich funktionieren, außen braucht es berechenbare Anschlussfähigkeit im Verbund. Der nüchterne Befund dieses Beitrags lautet daher: Es fehlt weniger an Einsicht oder Gremien als an konsequenter Systemintegration – an den Nahtstellen von Technik, Organisation, Recht und strategischer Kommunikation; genau dort erfordern hybride Lagen Tempo und Verantwortlichkeit. Daran müssen Reformen gemessen werden.

Der Blick auf Partner (USA, Vereinigtes Königreich, Frankreich, Baltikum) schärft drei tragende Prinzipien: Erstens gilt, dass es ohne robusten Grundbetrieb keine verantwortbare operative Handlungsfähigkeit gibt. Zweitens gewinnen aktive Optionen erst dann Qualität, wenn Führung, Recht und Kommunikation vorausgebaut sind. Drittens ist strategische Kommunikation Sicherheitsfunktion – sie beschleunigt Attribution, stützt Legitimation und erklärt Verfahren. Bündnisfähigkeit ist dabei Designvorgabe, nicht späte Zertifizierung. Das ist keine Blaupause, aber ein belastbarer Ordnungsrahmen für deutsche Entscheidungen.

Für Deutschland zeigt sich das Defizit als Integrations-, nicht Erkenntnisproblem: Koordinations- und Lageformate existieren; militärisch sind die Teilstreitkraft Cyber- und Informationsraum und das Zentrum Cyber-Operationen verlässlich verankert. Doch bundeseinheitlich eingeübte Standard Operating Procedures, ein rechtsklarer Freigabeprozess unterhalb der Landes- und Bündnisverteidigung und eine operativ mandatierte Fähigkeit strategischer Kommunikation fehlen im Verbund. Die Evaluierung der *Cybersicherheitsstrategie 2021* bestätigt die Wirkungslücke zwischen formaler Umsetzung und externer Wirkung – besonders in der föderalen Architektur. Konsequenz: nicht mehr Koordination, sondern mehr Verbindlichkeit in Führung, Recht und Übung.

Die in Abschnitt 5 gebündelte Umsetzungsarchitektur schließt genau diese Lücken: Sie koppelt gehärteten Grundbetrieb und Wiederanlauf mit einer ständigen Führungsordnung (inklusive klarer Eingriffsschwellen), einer rechtsstaatlich kodifizierten Eingriffsordnung und einer operativen strategischen Kommunikation; Anschlussfähigkeit an NATO- und EU-Verfahren ist Konstruktionsbedingung. Innovation fließt über einen disziplinierten „Pilot-to-Production“-Pfad in den Wirkbetrieb. Nicht das Etikett („Hack-back“) ist der Punkt, sondern rechtsklare, kontrollierte und erklärbare Handlungsfähigkeit in abgestuften Lagen.

Politisch ist dies Zumutung und Ordnungsversprechen zugleich. Die Zumutung: Geschwindigkeit an Recht und Routine binden – wer im Ereignisfall schnell sein will, muss vorher geübt haben, operativ wie kommunikativ. Das Ordnungsversprechen: Eben diese Bindung erzeugt Legitimität; eine kodifizierte, parlamentarisch eingebettete Eingriffsordnung nimmt der Debatte die Schlagwort-Schärfe und ersetzt sie durch prüf- und verantwortbare Befugnisse. Föderalität wird so nicht zum Hindernis, sondern zum Konstruktionsrahmen, sofern Rollen, Amtshilfewege und Übungsroutinen verbindlich definiert sind.

Auch die Messlogik braucht Maß: Kennzahlen steuern, sie dekorieren nicht. Wenige robuste Indikatoren machen Fortschritt sichtbar – ohne die Kapitel zuvor zu wiederholen. Audits prüfen Substanz, nicht Papier; Übungen dürfen realitätsnah scheitern; Kommunikationsleistung wird an Glaubwürdigkeit und Konsistenz, nicht an Sichtbarkeit bemessen. So wird Wirkung belegt, statt behauptet – und politisch steuerbar gemacht.

Schließlich ist Bündnisfähigkeit innenpolitische Klugheit: Wer nationale Verfahren spiegelbildlich zu NATO- und EU-Mechanismen aufsetzt, reduziert innen Entscheidungslatenzen und gewinnt außen Vertrauen. Dieselben Klarheiten, die international Reibung verringern, schaffen national Verlässlichkeit – in kürzeren Ausfallzeiten, geringeren Schadenssummen, robusteren Wahl- und Krisenprozessen und einer glaubwürdigen öffentlichen Kommunikation. Damit wird die politische Ökonomie der Resilienz von der Sonderaufgabe zur Basisarbeit, die sich rechnet.

Die anvisierte Ordnung markiert den Übergang von Koordination zu Führung, von Maßnahmenlisten zu Wirkbetrieb – entschieden an der Nahtstelle von Grundbetrieb, Freigabeprozess und strategischer Kommunikation. Gelingt dieser Übergang, bleibt die Schlussformel schlicht und anspruchsvoll zugleich: innen robust, außen anschlussfähig.

Literaturverzeichnis

Agence nationale de la sécurité des systèmes d'information (ANSSI) (2023): Missions, 04.10.2023, https://cyber.gouv.fr/missions, zuletzt aufgerufen am 10.10.2025.

AP News (2025): NATO announces a new mission to protect undersea cables in the Baltic Sea region, 14.01.2025, https://apnews.com/article/nato-finland-baltic-undersea-cables-b8d351fa018d703fe9dbc50459211e61, zuletzt aufgerufen am 10.10.2025.

Der Beauftragte der Bundesregierung für Informationstechnik (BfIT) (o.D.): Der Nationale Cyber-Sicherheitsrat (NCSR), https://www.cio.bund.de/Webs/CIO/DE/it-sicherheit-und-netze/it-sicherheit/nationaler-cybersicherheitsrat/nationaler-cybersicherheitsrat-node.html, zuletzt aufgerufen am 10.10.2025.

Bendiek, Annegret/Bossong, Raphael (2022): „Hybride Bedrohungen": Vom Strategischen Kompass zur Nationalen Sicherheitsstrategie (SWP Aktuell 2022/A 40), in: Stiftung Wissenschaft und Politik vom 23.06.2022, Berlin, https://www.swp-berlin.org/10.18449/2022A40/, zuletzt aufgerufen am 10.10.2025.

Bendiek, Annegret/Schulze, Matthias (2021): Schwachstellen der deutschen Cybersicherheitsstrategie (SWP Kurz gesagt), in: Stiftung Wissenschaft und Politik vom 20.09.2021, Berlin, https://www.swp-berlin.org/publikation/schwachstellen-der-deutschen-cybersicherheitsstrategie-2021, zuletzt aufgerufen am 10.10.2025.

Bolt, Neville (2023): Bolt's paradigm of strategic communications, in: ders. (Hg.): Understanding Strategic Communications. Terminology Working Group Publication No. 3, S. 19–21, NATO Strategic Communications Centre of Excellence (StratCom COE), Riga, https://stratcomcoe.org/publications/download/Terminology-Report-No3-DIGITAL.pdf, zuletzt aufgerufen am 10.10.2025.

British Army (o.D.): 77th Brigade – Groups within 77th Brigade, https://www.army.mod.uk/learn-and-explore/about-the-army/formations-divisions-and-brigades/field-army-troops/77th-brigade-information-operations/groups-within-77th-brigade/, zuletzt aufgerufen am 10.10.2025.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024): Die Lage der IT-Sicherheit in Deutschland 2024, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf, zuletzt aufgerufen am 10.10.2025.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.D. a): Das Nationale IT-Krisenreaktionszentrum im BSI,

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/IT-Krisenreaktionszentrum/it-krisenreaktionszentrum_node.html, zuletzt aufgerufen am 10.10.2025.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.D. b): Das Nationale Cyber-Abwehrzentrum, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html, zuletzt aufgerufen am 10.10.2025.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.D. c): Nationales IT-Lagezentrum, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/nationales-it-lagezentrum_node.html, zuletzt aufgerufen am 10.10.2025.

Bundesamt für Verfassungsschutz (BfV) (2023): Spionage gegen den Verteidigungssektor, 30.06.2023, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschaftswissenschaftsschutz/2023-30-06-sicherheitshinweis-6.pdf, zuletzt aufgerufen am 10.10.2025.

Bundesamt für Verfassungsschutz (BfV) (2025): Verfassungsschutzbericht 2024, Juni 2025, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2025-06-10-verfassungsschutzbericht-2024.html, zuletzt aufgerufen am 10.10.2025.

Bundesminister des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021, 08.09.2021, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/09/cybersicherheitsstrategie-2021.html, zuletzt aufgerufen am 10.10.2025.

Bundesministerium des Innern (2025a): Bundeskabinett beschließt Gesetzentwurf zum KRITIS Dachgesetz, Pressemitteilung vom 10.09.2025, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2025/09/kritis-dg-kabinett.html, zuletzt aufgerufen am 10.10.2025.

Bundesministerium des Innern (2025b): Evaluierung der Cybersicherheitsstrategie 2021, 08.09.2025, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/BMI25069-evaluierung-cybersicherheitsstrategie2021.html, zuletzt aufgerufen am 10.10.2025.

Bundesregierung (2023): Nationale Sicherheitsstrategie. Integrierte Sicherheit für Deutschland, Berlin, 14.06.2023, https://www.nationalesicherheitsstrategie.de/, zuletzt aufgerufen am 10.10.2025.

Bundesregierung/Auswärtiges Amt (2021): On the Application of International Law in Cyberspace – Positionspapier des Auswärtigen Amtes, März 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf, zuletzt aufgerufen am 10.10.2025.

Bundeswehr (o.D. a): Zentrum Cyber-Operationen (ZCO), https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum/kommando-aufklaerung-wirkung/zentrum-cyber-operationen, zuletzt aufgerufen am 10.10.2025.

Bundeswehr (o.D. b): Die vierte Teilstreitkraft: Der Cyber- und Informationsraum (TSK CIR), https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum, zuletzt aufgerufen am 10.10.2025.

Cerulus, Laurens/Klingert, Liv (2021): Russia's „Ghostwriter" hacker group takes aim at German election, in: Politico Europe vom 21.09.2021, https://www.politico.eu/article/russia-brash-hackers-turn-to-german-election, zuletzt aufgerufen am 10.10.2025.

Clark, Adam (2025): Cybersecurity in the UK (Research Briefing CBP 9821), in: House of Commons Library vom 01.05.2025, https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf, zuletzt aufgerufen am 10.10.2025.

Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2018): Cyber defence at the 28th NATO Summit in Brussels, 11.–12.07.2018, https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018/, zuletzt aufgerufen am 10.10.2025.

Deutscher Bundestag (2025a): Drucksache 21/1823 vom 25.09.2025, 21. Wahlperiode, Kleine Anfrage der Abgeordneten Jörg Zirwes, Hannes Gnauck, Sascha Lensing und der Fraktion der AfD: Sabotageakte gegen kritische Infrastrukturen in Deutschland seit 2020 – Häufigkeit, Einordnung und Maßnahmen zur Resilienzsteigerung, https://dserver.bundestag.de/btd/21/018/2101823.pdf, zuletzt aufgerufen am 10.10.2025.

Deutscher Bundestag (2025b): Neues Lagebild zu hybriden Bedrohungen (Parlamentsnachrichten, Inneres – Antwort – hib 331/2025), 04.08.2025, https://www.bundestag.de/presse/hib/kurzmeldungen-1103890, zuletzt aufgerufen am 10.10.2025.

Deutscher Bundestag (2025c): Drucksache 21/995 vom 24.07.2025, 21. Wahlperiode, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Irene Mihalic, Agnieszka Brugger, Dr. Konstantin von Notz, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN (Drucksache 21/769): Fragen zur Notwendigkeit eines umfassenden Lagebilds zu Sabotage, Spionage und Desinformation, https://dip.bundestag.de/vorgang/fragen-zur-notwendigkeit-eines-umfassenden-lagebilds-zu-sabotage-spionage-und/323345, zuletzt aufgerufen am 10.10.2025.

Estonian Defence League (o.D.): Cyber Defence Unit, https://kaitseliit.ee/en, zuletzt aufgerufen am 10.10.2025.

Europäische Kommission (2025a): DSA Elections Toolkit for Digital Services Coordinators, 21.02.2025, https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators, zuletzt aufgerufen am 10.10.2025.

Europäische Kommission (2025b): A Coordinated Implementation Roadmap for the Transition to Post Quantum Cryptography, 23.06.2025, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography, zuletzt aufgerufen am 10.10.2025.

Europäische Kommission (2025c): Commission calls on 19 Member states to fully transpose the NIS2 Directive, Pressemitteilung, 07.05.2025, https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive, zuletzt aufgerufen am 10.10.2025.

Europäische Union (2022a): Richtlinie (EU) 2022/2555 (NIS 2) vom 27.12.2022, https://eur-lex.europa.eu/eli/dir/2022/2555/oj, zuletzt aufgerufen am 10.10.2025.

Europäische Union (2022b): Verordnung (EU) 2022/2554 (Digital Operational Resilience Act, DORA) vom 14.12.2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj, zuletzt aufgerufen am 10.10.2025.

Europäische Union (2022c): Verordnung (EU) 2022/2065 (Digital Services Act, DSA) vom 27.10.2022, https://eur-lex.europa.eu/eli/reg/2022/2065/oj, zuletzt aufgerufen am 10.10.2025.

Europäische Union (2024a): Verordnung (EU) 2024/2847 (Cyber Resilience Act, CRA) vom 20.11.2024, http://data.europa.eu/eli/reg/2024/2847/oj, zuletzt aufgerufen am 10.10.2025.

Europäische Union (2024b): Durchführungsverordnung (EU) 2024/482 (EUCC –

Common-Criteria-Zertifizierungsschema) vom 07.02.2024, https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj, zuletzt aufgerufen am 10.10.2025.

Europäische Union (2025): Verordnung (EU) 2025/38 (Cyber Solidarity Act, CSA) vom 15.01.2025, https://eur-lex.europa.eu/eli/reg/2025/38/oj, zuletzt aufgerufen am 10.10.2025.

Europäischer Rat/Rat der Europäischen Union (2020): EU imposes the first ever sanctions against cyber attacks, Pressemitteilung vom 30.07.2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/, zuletzt aufgerufen am 10.10.2025.

European External Action Service (EEAS) (2025): 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats, März 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf, zuletzt aufgerufen am 10.10.2025.

European Union Agency for Cybersecurity (ENISA) (2025a): EU consistently targeted by diverse yet convergent threat groups, Oktober 2025, https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups, zuletzt aufgerufen am 10.10.2025.

European Union Agency for Cybersecurity (ENISA) (2025b): Threat Landscape 2025 (Juli 2024–Juni 2025), Athen, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025, zuletzt aufgerufen am 10.10.2025.

Fischerkeller, Michael P./Harknett, Richard J. (2019): Persistent Engagement and Agreed Competition, and Cyberspace Interaction Dynamics and Escalation, in: The Cyber Defense Review 3(2), S. 267–287.

German Marshall Fund/Alliance for Securing Democracy (o.D.): Ghostwriter targets German politicians ahead of elections, https://securingdemocracy.gmfus.org/incident/russia-linked-hacking-group-ghostwriter-targets-german-politicians-ahead-of-elections/, zuletzt aufgerufen am 10.10.2025.

Gold, Josh (2019): How Estonia uses Cybersecurity to Strengthen its Position in NATO (ICDS Commentary), in: International Centre for Defence and Security vom 27.05.2019, https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato, zuletzt aufgerufen am 10.10.2025.

Goździewicz, Wiesław (2019): Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), in: Cyber Defense Magazine vom 11.11.2019, https://www.cyberdefensemagazine.com/sovereign-cyber/, zuletzt aufgerufen am 10.10.2025.

Hensiek, Joerg (2025): Massive IT-Sicherheitslücken in der Bundesverwaltung – Bundesrechnungshof kritisiert Bundes IT, in: Haufe vom 23.07.2025, https://www.haufe.de/oeffentlicher-dienst/digitalisierung-transformation/bundesrechnungshof-it-sicherheitsluecken-in-bundesverwaltung_524786_656758.html, zuletzt aufgerufen am 10.10.2025.

Herpig, Sven (2023): Active Cyber Defense. Toward Operational Norms, Stiftung Neue Verantwortung (SNV): Berlin (November 2023), https://www.interface-eu.org/storage/archive/files/snv_active_cyber_defense_toward_operational_norms.pdf, zuletzt aufgerufen am 10.10.2025.

Herpig, Sven/Dutke, Frederic (2023): Deutschlands staatliche Cybersicherheitsarchitektur, Stiftung Neue Verantwortung: Berlin (19.10.2023), https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_elfteauflage1123.pdf, zuletzt aufgerufen am 10.10.2025.

International Institute for Strategic Studies (IISS) (2021): Cyber Capabilities and National Power: France, S. 57–67, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-

capabilities-and-national-power---france.pdf, zuletzt aufgerufen am 10.10.2025.

International Institute for Strategic Studies (IISS) (2023): Cyber Capabilities and National Power – Volume 2: 6. Germany, S. 47–59, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_06-germany.pdf, zuletzt aufgerufen am 10.10.2025.

Kannenberg, Axel (2025): Sogar Notstrom fehlt: Schlechte Sicherheitsstandards in Rechenzentren des Bundes, in: Heise Online vom 04.07.2025, https://www.heise.de/news/Bundesrechnungshof-Sicherheitsniveau-der-Bundes-IT-unzureichend-10475018.html, zuletzt aufgerufen am 10.10.2025.

Kaska, Kadri/Osula, Anna Maria/Stinissen, Jan (2013): The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis, CCDCOE: Tallinn, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf, zuletzt aufgerufen am 10.10.2025.

Kiesel, Robert/Keilani, Fatina (2019): IT-Katastrophe am Berliner Kammergericht kam mit Ansage, in: Tagesspiegel vom 29.10.2019, https://www.tagesspiegel.de/berlin/it-katastrophe-am-berliner-kammergericht-kam-mit-ansage-5039224.html, zuletzt aufgerufen am 10.10.2025.

Kim, Maurus (2024): Bislang 75 Vorfälle mit Drohnen im Jahr 2024, in: Frankfurter Allgemeine Zeitung vom 09.07.2024, https://www.faz.net/aktuell/gesellschaft/ungluecke/bislang-75-vorfaelle-mit-drohnen-im-jahr-2024-19845133.html, zuletzt aufgerufen am 10.10.2025.

Kipker, Dennis Kenji (2019): Hackback in Deutschland: Wer, was, wie und warum?, in: Verfassungsblog vom 03.06.2019, https://verfassungsblog.de/hackback-in-deutschland-wer-was-wie-und-warum, zuletzt aufgerufen am 10.10.2025.

Klarhoefer, Lavinia/Leuchtenmüller, Christine (2025): Finnlands Reaktion auf hybride Bedrohungen in der Ostsee (Länderbericht März 2025), in: Konrad Adenauer Stiftung vom 27.03.2025, https://www.kas.de/de/laenderberichte/detail/-/content/finnlands-reaktion-auf-hybride-bedrohungen-in-der-ostsee, zuletzt aufgerufen am 10.10.2025.

Kurz, Constanze (2024): Hackbacks: Zurückhacken ist keine Verteidigung, in: netzpolitik.org vom 07.05.2024, https://netzpolitik.org/2024/hackbacks-zurueckhacken-ist-keine-verteidigung, zuletzt aufgerufen am 10.10.2025.

Leinhos, Ludwig (2020): Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr, in: Connections: The Quarterly Journal 19(1), S. 9–19.

Litschko, Konrad (2022): Signalkabel durchtrennt: Bahnchaos wegen Sabotage, in: taz vom 08.10.2022, https://taz.de/Signalkabel-durchtrennt/!5886558, zuletzt aufgerufen am 10.10.2025.

Mačák, Kubo/Dias, Talita/Kasper, Ágnes (Hgg.) (2025): Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States, CCDCOE: Tallinn, https://ccdcoe.org/uploads/2025/05/Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf, zuletzt aufgerufen am 10.10.2025.

Magnuson, Salamah/Keay, Morgan/Metcalf, Kimberly (2022): Countering Hybrid Warfare: Mapping Social Contracts to Reinforce Societal Resiliency in Estonia and Beyond, in: Texas National Security Review 5(2), S. 27–52.

Meister, Stefan (2016): The „Lisa case“: Germany as a target of Russian disinformation, in: NATO Review vom 25.07.2016, https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html, zuletzt aufgerufen am 10.10.2025.

Menhard, Esther/Meister, Andre (2025): Bundesregierung verfehlt Ziele der IT-

Konsolidierung, in: netzpolitik.org vom 18.08.2025, https://netzpolitik.org/2025/bundesrechnungshof-bundesregierung-verfehlt-ziele-der-it-konsolidierung/, zuletzt aufgerufen am 10.10.2025.

Ministère des Armées (o.D.): Le Commandement de la cyberdéfense (COMCYBER), Web Dossier, https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber, zuletzt aufgerufen am 10.10.2025.

Ministère des Armées/COMCYBER (2019): Éléments publics de doctrine militaire de lutte informatique offensive, Januar 2019, https://www.defense.gouv.fr/sites/default/files/comcyber/doctrine%20militaire%20de%20lutte%20informatique%20offensive.pdf, zuletzt aufgerufen am 10.10.2025.

Ministry of National Defence of the Republic of Lithuania (2025): Overview of the Cybersecurity Status in Lithuania: Key Information 2024, 25.07.2025, https://kam.lt/wp-content/uploads/2025/07/Overview-of-the-Cybersecurity-status_LT_2024.pdf, zuletzt aufgerufen am 10.10.2025.

Mumford, Andrew/Carlucci, Pascal (2023): Hybrid warfare: The continuation of ambiguity by other means, in: European Journal of International Security 8(2), S. 192–206.

Nakasone, Paul M. (2019): A Cyber Force for Persistent Operations, in: Joint Force Quarterly 92, S. 10–14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf, zuletzt aufgerufen am 10.10.2025.

National Cyber Force (UK) (2023): The National Cyber Force: Responsible Cyber Power in Practice, White Paper vom 04.04.2023, https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf, zuletzt aufgerufen am 10.10.2025.

National Cyber Security Centre (Irland) (o.D.): Quick Guide: Ransomware. How to #BreakTheChain, https://www.ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Ransomware.pdf, zuletzt aufgerufen am 10.10.2025.

National Cyber Security Centrum (Niederlande) (2022): Incident Response Plan – Ransomware, 2022, https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/augustus/2/incident-response-plan-ransomware/Opmaak%2BIncident%2Bresponse%2Bplan_WEB2.pdf, zuletzt aufgerufen am 10.10.2025.

National Institute of Standards and Technology (NIST) (2024a): FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML KEM), 13.08.2024, https://csrc.nist.gov/pubs/fips/203/final, zuletzt aufgerufen am 10.10.2025.

National Institute of Standards and Technology (NIST) (2024b): FIPS 204: Module-Lattice-Based Digital Signature Standard (ML DSA), 13.08.2024, https://csrc.nist.gov/pubs/fips/204/final, zuletzt aufgerufen am 10.10.2025.

National Institute of Standards and Technology (NIST) (2024c): FIPS 205: Stateless Hash Based Digital Signature Standard (SLH DSA), 13.08.2024, https://csrc.nist.gov/pubs/fips/205/final, zuletzt aufgerufen am 10.10.2025.

National Institute of Standards and Technology (NIST) (2024d): NIST Releases First 3 Finalized Post Quantum Encryption Standards, Pressemitteilung vom 13.08.2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, zuletzt aufgerufen am 10.10.2025.

NATO (2014): Wales Summit Declaration, Pressemitteilung (2014) 120 vom 05.09.2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm, zuletzt aufgerufen am 10.10.2025.

NATO (2016a): Warsaw Summit Communiqué, 09.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, zuletzt

aufgerufen am 10.10.2025.
NATO (2016b): Cyber Defence Pledge, Pressemitteilung (2016) 124 vom 08.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2018): Brussels Summit Declaration (11.–12.07.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2021): NATO releases first ever strategy for Artificial Intelligence, 22.10.2021, https://www.nato.int/cps/en/natohq/news_187934.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2022): NATO 2022 Strategic Concept, 29.06.2022, https://www.nato.int/cps/en/natohq/topics_210907.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2023): Vilnius Summit Communiqué (11.–12.07.2023), https://www.nato.int/cps/en/natohq/official_texts_217320.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2024a): Cyber defence (Themenseite), 30.07.2024, https://www.nato.int/cps/en/natohq/topics_78170.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2024b): Washington Summit Declaration (Einrichtung des NATO Integrated Cyber Defence Centre), 15.07.2024, https://www.nato.int/cps/en/natohq/official_texts_227678.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2024c): Allies agree new NATO Integrated Cyber Defence Centre, News vom 10.07.2024, https://www.nato.int/cps/en/natohq/news_227647.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2024d): Summary of NATO's revised Artificial Intelligence (AI) strategy, 10.07.2024, https://www.nato.int/cps/en/natohq/official_texts_227237.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2024e): NATO releases revised AI strategy, 10.07.2024, https://www.nato.int/cps/fr/natohq/news_227234.htm, zuletzt aufgerufen am 10.10.2025.
NATO (2025): Defence Innovation Accelerator for the North Atlantic (DIANA), 26.06.2025, https://www.nato.int/cps/en/natohq/topics_216199.htm, zuletzt aufgerufen am 10.10.2025.
NATO Allied Maritime Command (2024): NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure, 28.05.2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui, zuletzt aufgerufen am 10.10.2025.
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2025): Locked Shields 2025: Showcased Nations' Commitment to Defending Cyberspace, 09.05.2025, https://ccdcoe.org/news/2025/locked-shields-2025-showcased-nations-commitment-to-defending-cyberspace, zuletzt aufgerufen am 10.10.2025.
NATO Strategic Communications Centre of Excellence (StratCom COE) (o.D. a): 2007 cyber attacks on Estonia (Timeline), https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf, zuletzt aufgerufen am 10.10.2025.
NATO Strategic Communications Centre of Excellence (StratCom COE) (o.D. b): About the NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5, zuletzt aufgerufen am 10.10.2025.
NATO Strategic Communications Centre of Excellence (StratCom COE) (o.D. c): About Strategic Communications, https://stratcomcoe.org/about_us/about-

strategic-communications/1, zuletzt aufgerufen am 10.10.2025.
Ottis, Rain (2008): Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, in: CCDCOE Januar 2008, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, zuletzt aufgerufen am 10.10.2025.
Parly, Florence (2019): Stratégie cyber des Armées (Rede vom 18.01.2019), Ministère des Armées, https://www.defense.gouv.fr/sites/default/files/ministere-armees/Discours%20de%20Florence%20Parly%20-%20Strat%C3%A9gie%20cyber%20des%20Arm%C3%A9es%20-%2018%20janvier%202019.pdf, zuletzt aufgerufen am 10.10.2025.
Payne, Julia (2022): Oil shipments in European oil hub delayed after cyber-attacks, in: Reuters vom 04.02.2022, https://www.reuters.com/world/europe/oil-shipments-european-oil-hub-delayed-after-cyber-attacks-2022-02-04/, zuletzt aufgerufen am 10.10.2025.
Pearson, James (2022): Shell re-routes oil supplies after cyberattack on German logistics firm, in: Reuters vom 01.02.2022, https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/, zuletzt aufgerufen am 10.10.2025.
Pfannenstiel, Melia/Cox, Dan (2024): NATO's Cyber Era (1999–2024): Implications for Multidomain Operations, in: Military Review – Online Exclusive, Oktober 2024, S. 1–10.
Reynolds, Ian/Atalan, Yasir (2024): Calibrating NATO's Vision of AI Enabled Decision Support, CSIS, 08.07.2024, https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support, zuletzt aufgerufen am 10.10.2025.
Schaubert, Medina (2018): Der „Fall Lisa": Entwicklungen in Berlin Hellersdorf Marzahn, in: Bundeszentrale für politische Bildung vom 09.10.2018, https://www.bpb.de/themen/migration-integration/russlanddeutsche/271945/der-fall-lisa, zuletzt aufgerufen am 10.10.2025.
Schmitt, Michael N. (Hg.) (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press: Cambridge.
Schmoldt, Janine (2024): Von der Defensive zur Cyberoffensive? Aktive Cyberabwehr, Hackbacks und der Diskurs der Akteure in der deutschen Cybersicherheitspolitik, in: Zeitschrift für Außen- und Sicherheitspolitik 17(2), S. 165–182.
Schulze, Matthias (2020): German Military Cyber Operations are in a Legal Gray Zone, in: Lawfare Blog (online) vom 08.04.2020, https://www.lawfaremedia.org/article/german-military-cyber-operations-are-legal-gray-zone, zuletzt aufgerufen am 10.10.2025.
Schulze, Matthias/Herpig, Sven (2018): Germany Develops Offensive Cyber Capabilities Without a Coherent Strategy of What to Do With Them, in: Defense One vom 03.12.2018, https://www.defenseone.com/ideas/2018/12/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them/153227, zuletzt aufgerufen am 10.10.2025.
Senatsverwaltung für Justiz Berlin (2020): Vorstellung des vorläufigen forensischen Abschlussberichts zur Emotet Infektion am Kammergericht, 27.01.2020, https://www.berlin.de/sen/justv/presse/pressemitteilungen/2020/pressemitteilung.887323.php, zuletzt aufgerufen am 10.10.2025.
Smirnova, Julia (2025): Strategien und Erscheinungsformen russischer Desinformation, in: APuZ 39/2025, S. 49–55, https://www.bpb.de/system/files/dokument_pdf/APuZ_2025-39_online_PropagandaUndDesinformation.pdf, zuletzt aufgerufen am 10.10.2025.
Stevens, Tim/Cormac, Rory/D Lonergan, Erica/Lomas, Dan/Hüsch, Pia/Devanny, Joe (2023): Evaluating the National Cyber Force's „Responsible Cyber Power in

Practice“, Kommentar, in: The Royal United Services Institute for Defence and Security Studies (RUSI) vom 14.04.2023, https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice, zuletzt aufgerufen am 10.10.2025.

Swedish Psychological Defence Agency (MPF) (2024/2025): About us, https://mpf.se/psychological-defence-agency/about-us, zuletzt aufgerufen am 10.10.2025.

T-Systems (2019): Forensics Report – Emotet/Trickbot Infektion Kammergericht Berlin (freigegebene Fassung), 23.12.2019, https://www.berlin.de/sen/justv/presse/pressemitteilungen/2020/pm-11-2020-t-systems-forensik_bericht_public_v1.pdf, zuletzt aufgerufen am 10.10.2025.

UK Ministry of Defence, Cyber & Specialist Operations Command (2023): Supporting NATO’s Cyber Posture: Insight from Strategic Command shared at CyberSec Summit 2023, 05.10.2023, https://www.gov.uk/government/news/supporting-natos-cyber-posture, zuletzt aufgerufen am 10.10.2025.

U.S. Cyber Command (2018): Achieve and Maintain Cyberspace Superiority – Command Vision for USCYBERCOM, 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, zuletzt aufgerufen am 10.10.2025.

U.S. Cyber Command (2024): Media Release: USCYBERCOM Executes International Coordinated Cyber Security Activity 2024, 15.11.2024, https://www.cybercom.mil/Media/News/Article/3966564/media-release-uscybercom-executes-international-coordinated-cyber-security-acti, zuletzt aufgerufen am 10.10.2025.

U.S. Cyber Command (o.D.): Mission and Vision, https://www.cybercom.mil/About/Mission-and-Vision/, zuletzt aufgerufen am 10.10.2025.

U.S. Department of Defense (2018): Summary: Department of Defense Cyber Strategy, 19.09.2018, https://dodcio.defense.gov/Portals/0/Documents/Library/Cyber-Strategy2018.pdf, zuletzt aufgerufen am 10.10.2025.

Verfassungsschutz Baden-Württemberg (2021): „GHOSTWRITER“: Phishing Kampagne gegen deutsche Politiker, 24.06.2021, https://www.verfassungsschutz-bw.de/,Lde/_GHOSTWRITER_+Phishing-Kampagne+gegen+deutsche+Politiker, zuletzt aufgerufen am 10.10.2025.

Voelsen, Daniel (Hg.) (2024): Maritime kritische Infrastrukturen: Strategische Bedeutung und geeignete Schutzmaßnahmen (SWP-Studie 2024/S 03), in: Stiftung Wissenschaft und Politik vom 06.02.2024, https://www.swp-berlin.org/10.18449/2024S03, zuletzt aufgerufen am 10.10.2025.