

Mai 2023 · Dr. Sven Herpig, Christina Rupp,
Rebecca Beigel & Frederic Dutke

Deutschlands staatliche Cybersicherheits- architektur

10. Auflage

Unterstützt durch die Data Science Unit:
Anna Semenova & Pegah Maham



Think Tank für die Gesellschaft im technologischen Wandel



Inhalt

1. Hintergrund und Methodik	11
2. Visualisierung der Cybersicherheitsarchitektur	16
3. Abkürzungsverzeichnis und Akteurskategorisierung	17
4. Erläuterung – Akteure auf UN-Ebene	39
Policy-Überblick	40
Ausbildungs- und Forschungsinstitut der Vereinten Nationen (UNITAR)	40
Büro der Vereinten Nationen für Abrüstungsfragen (UNODA)	41
Büro der Vereinten Nationen für Drogen- und Verbrechenbekämpfung (UNODC)	41
Entwicklungsprogramm der Vereinten Nationen (UNDP)	42
Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE)	43
Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen (UNDESA)	44
Internationale Fernmeldeunion (ITU)	45
Internet Governance Forum (IGF)	46
Konferenz der Vereinten Nationen für Handel und Entwicklung (UNCTAD)	47
Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG)	47
Wirtschafts- und Sozialrat der Vereinten Nationen (ECOSOC)	48
UN-Generalversammlung (UNGA)	49
UN-Institut für Abrüstungsforschung (UNIDIR)	50
UN-Institut für interregionale Kriminalitäts- und Justizforschung (UNICRI)	51
UN-Sicherheitsrat (UNSC)	52
United Nations Digital and Technology Network (DTN)	52
United Nations Group on the Information Society (UNGIS)	53
United Nations Information Security Special Interest Group (UNISSIG)	53
United Nations International Computing Centre (UNICC)	54
United Nations Office of Counter-Terrorism (UNOCT)	54
United Nations Office of Information and Communications Technology (UN OICT)	55
5. Erläuterung – Weitere internationale Akteure	56
Policy-Überblick	57
Europarat (CoE)	57
Forum of Incident Response and Security Teams (FIRST)	58
Internationale Elektrotechnische Kommission (IEC)	59



Internationale Kriminalpolizeiliche Organisation (Interpol)	59
Internationale Organisation für Normung (ISO)	60
Internet Corporation for Assigned Names and Numbers (ICANN)	61
Internet Engineering Task Force (IETF)	61
ISO and IEC Joint Technical Committee (JTC 1)	62
Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)	62
Trusted Introducer (TI)	63
6. Erläuterung – Akteure auf EU-Ebene	64
Policy-Überblick	65
Agentur der Europäischen Union für Cybersicherheit (ENISA)	66
Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL)	68
Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)	68
CEN/CENELEC Cyber Security Coordination Group (CSCG)	69
Computer Emergency Response Team der Europäischen Kommission (CERT-EU)	70
Computer Security Incident Response Teams Netzwerk (CSIRTs Netzwerk)	71
Cyber Crisis Liaison Organisation Network (CyCLONe)	71
Cyber and Information Domain Coordination Centre (CIDCC)	72
Direktion Krisenbewältigung und Planung (CMPD)	73
ENISA-Beratungsgruppe (ENISA AG)	73
EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell)	74
EU Cyber Capacity Building Network (EU CyberNet)	74
Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)	75
Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA)	75
Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG)	76
Europäische Kommission (EK)	76
Europäische Kooperation für Akkreditierung (EA)	78
Europäische Verteidigungsagentur (EVA)	78
Europäische Zentralbank (EZB)	79
Europäischer Auswärtiger Dienst (EAD)	80
Europäische:r Datenschutzbeauftragte:r (EDSB)	81
Europäischer Rat (ER)	81
Europäisches Amt für Betrugsbekämpfung (OLAF)	82
Europäisches Institut für Telekommunikationsnormen (ETSI)	82
Europäisches Komitee für elektrotechnische Normung (CENELEC)	83
Europäisches Komitee für Normung (CEN)	83
Europäisches Polizeiamt (Europol)	84



Europäisches Sicherheits- und Verteidigungskolleg (ESVK)	84
Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC)	85
Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität (EC3)	86
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)	87
European Cybercrime Training and Education Group (ECTEG)	87
European Cyber Security Organisation (ECSO)	88
European Government CERTs group (EGC group)	88
European Judicial Network (EJN)	89
European Judicial Cybercrime Network (EJCN)	89
European Judicial Training Network (EJTN)	89
European Multidisciplinary Platform Against Criminal Threats (EMPACT)	90
European Union Cybercrime Task Force (EUCTF)	90
Gemeinsame Forschungsstelle (GD JRC)	91
Generaldirektion Forschung und Innovation (GD RTD)	91
Generaldirektion Informatik (GD DIGIT)	91
Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD CONNECT)	92
Generaldirektion Migration und Inneres (GD HOME)	92
Gruppe der Interessenträger für die Cybersicherheitszertifizierung (SCCG)	93
Horizontale Ratsarbeitsgruppe „Fragen des Cyberraums“ (HWPCI)	93
ICT Advisory Committee of the EU Agencies (ICTAC)	94
Institut der Europäischen Union für Sicherheitsstudien (EUISS)	94
Intelligence Directorate des EU-Militärstabs (EUMS INT)	95
Inter-Service Group „Community Capacity in Crisis-Management“ (ISG C3M)	95
Inter-Service Group „Countering Hybrid Threats“ (ISG CHT)	95
Joint Cyber Unit (JCU)	96
Kontaktgruppe zum Schutz Kritischer Infrastrukturen (SKI-Kontaktgruppe)	96
Kooperationsgruppe unter der NIS-Richtlinie (NIS Cooperation Group)	97
MeliCERTes	98
Militärausschuss der Europäischen Union (EUMC)	98
Politisches und Sicherheitspolitisches Komitee (PSK)	98
Rat der Europäischen Union (Council)	99
Reference Incident Classification Taxonomy Task Force (TF-CSIRT)	100
Senior Officials Group Information Systems Security (SOG-IS)	100
Ständige Strukturierte Zusammenarbeit (PESCO)	101
Taxonomy Governance Group (TGG)	101
Zentrum für die Koordination von Notfallmaßnahmen (ERCC)	102
Zentrum für Informationsgewinnung und -analyse (INTCEN)	102



7. Erläuterung – Akteure auf NATO-Ebene	104
Policy-Überblick	105
Allied Command Operations (ACO)	105
Allied Command Transformation (ACT)	106
Cyber Defence Committee (CDC)	106
Emerging Security Challenges Division (ESCD)	107
Joint Intelligence and Security Division (JISD)	107
NATO Communications and Information Agency (NCIA)	108
NATO Communication and Information System Group (NCISG)	108
NATO Computer Incident Response Capability (NCIRC)	109
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)	109
NATO Consultation, Control and Command Board (C3B)	110
NATO Cyber Defence Management Board (CDMB)	111
NATO Cyber Security Centre (NCSC)	111
NATO Cyberspace Operations Centre (CyOC)	111
NATO-Militärausschuss (MC)	112
NATO School Oberammergau (NS-O)	112
NATO Security Committee (SC)	113
NCI Academy	113
Nordatlantikrat (NAC)	114
8. Erläuterung – Akteure auf Bundesebene	115
Policy-Überblick	116
Agentur für Innovation in der Cybersicherheit (Cyberagentur)	117
Auswärtiges Amt (AA)	118
Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit (BfDI)	119
Bundeskanzleramt (BKAm)	120
Bundesnachrichtendienst (BND)	120
Bundesministerium der Justiz (BMJ)	121
Bundesministerium der Verteidigung (BMVg)	121
Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)	122
Bundesweite IT-Systemhaus GmbH (BWI)	123
Cyber Innovation Hub (CIHBw)	123
Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (BAIUDBw)	124
Bundesakademie für Sicherheitspolitik (BAKS)	124
Bundesamt für den Militärischen Abschirmdienst (BAMAD)	124
Cyber-Reserve	125
Organisationsbereich Cyber- und Informationsraum (CIR)	126
Kommando Cyber- und Informationsraum (KdoCIR)	126



Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw)	127
Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)	128
Universitäten der Bundeswehr (UniBw)	128
Forschungsinstitut Cyber Defence (CODE)	128
Bundesministerium des Innern und für Heimat (BMI)	129
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	130
Gemeinsames Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern (GeKoB)	130
Gemeinsames Melde- und Lagezentrum von Bund und Ländern (GMLZ)	131
Bundesamt für Sicherheit in der Informationstechnik (BSI)	132
Allianz für Cybersicherheit (ACS)	134
Bundes Security Operations Center (BSOC)	135
Computer Emergency Response Team der Bundesverwaltung (CERT-Bund)	136
Cyber-Sicherheitsnetzwerk (CSN)	136
Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt	137
Nationaler Pakt Cybersicherheit (NPCS)	137
Nationales IT-Lagezentrum (LZ)	138
Nationales IT-Krisenreaktionszentrum (IT-KRZ)	138
Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS)	138
Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)	139
Bundesamt für Verfassungsschutz (BfV)	140
Bundeskriminalamt (BKA)	140
Bundespolizei (BPol)	142
Bündnis für Cybersicherheit	142
Initiative Wirtschaftsschutz	143
IT-Rat	143
Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	144
Bundesministerium für Bildung und Forschung (BMBF)	145
Bundesministerium für Digitales und Verkehr (BMDV)	145
Bundesamt für Seeschifffahrt und Hydrographie (BSH)	146
Bundesministerium für Finanzen (BMF)	146
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	146
Informationstechnikzentrum Bund (ITZBund)	147
Zollkriminalamt (ZKA)	148
Bundesministerium für Gesundheit (BMG)	148
Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)	149



Bundesministerium für Wirtschaft und Klimaschutz (BMWK)	149
Beirat für Standardisierung in der Informations- und Kommunikationstechnologie (BSIKT)	150
Bundeskartellamt (BKartA)	150
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)	151
Initiative IT-Sicherheit in der Wirtschaft	151
Transferstelle IT-Sicherheit im Mittelstand (TISiM)	151
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)	152
Bundesverband der Verbraucherzentralen und Verbraucherverbände (vzbv)	152
Cyber Security Cluster Bonn e.V.	153
Deutsche Bundesbank (D BBk)	153
Deutsche Akkreditierungsstelle (DAkKS)	154
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)	154
Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE)	155
Deutsches Institut für Normung (DIN)	155
Deutschland sicher im Netz e.V. (DsiN)	156
DIN/DKE Gemeinschaftsgremium „Cybersecurity“	156
Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän.“	156
Föderale IT-Kooperation (FITKO)	157
gematik	157
German Competence Centre against Cyber Crime (G4C)	158
Innenministerkonferenz (IMK)	158
IT-Planungsrat (IT-PLR)	159
IT Security made in Germany (ITSMIG)	159
Kompetenz- und Forschungszentren für IT-Sicherheitsforschung (CISPA, ATHENE, KASTEL)	160
Nationaler CERT-Verbund	160
Nationaler Cyber-Sicherheitsrat (NCSR)	160
Nationales Cyber-Abwehrzentrum (CYBER-AZ)	161
Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen (UP KRITIS)	162
Stiftung Wissenschaft und Politik (SWP)	162
Verwaltungs-CERT-Verbund (VCV)	162
9. Erläuterung – Akteure auf Landesebene	164
Policy-Überblick	165
9.1 Baden-Württemberg (BW)	167
Überblick	168
Cybersicherheitsagentur Baden-Württemberg (CSBW)	170



IT-Rat Baden-Württemberg	171
Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg (SITiF BW)	171
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	171
9.2 Bayern (BY)	172
Überblick	173
Cyberabwehr Bayern	175
Cyber-Allianz-Zentrum (CAZ)	175
Kompetenzzentrum Cybercrime	175
Landesamt für Sicherheit in der Informationstechnik Bayern (LSI)	176
Zentralstelle Cybercrime Bayern (ZCB)	176
Zentrum Digitalisierung.Bayern (ZD.B)	176
9.3 Berlin (BE)	178
Überblick	179
Cyber Defense Center der Landesverwaltung Berlin (CDC-Lv)	180
Digitalagentur Berlin (DAB)	181
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	181
9.4 Brandenburg (BB)	182
Überblick	183
Ausschuss der Ressort Information Officer (RIO-Ausschuss)	184
Cyber-Competence-Center (CCC)	184
IT-Rat Brandenburg	185
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus	185
9.5 Bremen (HB)	186
Überblick	187
9.6 Hamburg (HH)	189
Überblick	190
9.7 Hessen (HE)	192
Überblick	193
Hessisches Cyberabwehrausbildungszentrum Land/Kommunen (HECAAZ L/K)	194
Hessen Cyber Competence Center (Hessen3C)	194
Kommunales Dienstleistungszentrum Cybersicherheit (KDLZ-CS)	195
Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT)	195
9.8 Mecklenburg-Vorpommern (MV)	197
Überblick	198
Netzverweis.de	199



Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	200
Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV)	200
9.9 Niedersachsen (NI)	201
Überblick	202
Cybersicherheitsbündnis	203
Digitalagentur Niedersachsen	204
9.10 Nordrhein-Westfalen (NW)	205
Überblick	206
Cybercrime-Kompetenzzentrum	208
Cyberwehr (Cyberwehr [NW])	208
Interministerieller Ausschuss Cybersicherheit (IMA Cybersicherheit)	208
Kompetenzzentrum für Cybersicherheit in der Wirtschaft (DIGITAL.SICHER.NRW)	209
Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen	209
Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)	210
9.11 Rheinland-Pfalz (RP)	211
Überblick	212
Landeszentralstelle Cybercrime (LZC)	214
9.12 Saarland (SL)	215
Überblick	216
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken	217
Netzwerkstelle Digitalisierung (DiNet)	218
Initiative für Cybersicherheit (CYBR360)	218
9.13 Sachsen (SN)	219
Überblick	220
Arbeitsgruppe Informationssicherheit (AG IS)	221
Cyber Crime Competence Center Sachsen (SN4C)	222
Zentralstelle Cybercrime Sachsen (ZCS)	222
9.14 Sachsen-Anhalt (ST)	223
Überblick	224
Cybercrime Competence Center (4C)	225
9.15 Schleswig-Holstein (SH)	226
Überblick	227
IT-Verbund Schleswig-Holstein (ITVSH)	228
9.16 Thüringen (TH)	229
Überblick	230
9.17 Bundesländerübergreifende Akteure	232
CERT Nord	232
Dataport	232
Sicherheitskooperation Cybercrime	232



10. Erläuterung – Akteure auf Kommunalebene	233
Policy-Überblick	234
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (Vitako)	234
IT-SiBe-Forum	234
Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt)	235
Kommunale Spitzenverbände (KSV)	235
Kommunalgremium des IT-Planungsrates	236



1. Hintergrund und Methodik

Die ersten Grundsteine der deutschen Cybersicherheitsarchitektur wurden bereits Ende der 1980er-Jahre mit der Einrichtung einer sich mit IKT-Sicherheit befassenden Arbeitsgruppe und der nachfolgenden Gründung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Jahre 1991 gelegt.

Seitdem hat sich einiges getan: Cybersicherheit ist für die deutsche Außen- und Innen- sowie auch die Sicherheits- und Verteidigungspolitik ein elementarer Bestandteil geworden, was sowohl zu der Entstehung vieler neuer (inter)nationaler Akteure als auch dem Wachstum von untereinander bestehenden Verbindungen geführt hat. In den öffentlichen Fokus geriet die deutsche Cybersicherheitspolitik insbesondere im Jahr 2011¹ durch die Veröffentlichung der ersten Cybersicherheitsstrategie für Deutschland, die in den Jahren 2016² und 2021³ aktualisiert wurde.

Keine der drei bisherigen Cybersicherheitsstrategien beinhaltet dabei eine grafische oder anderweitige Übersicht über die immer komplexer werdende Architektur deutscher Behörden mit Aufgaben und Kompetenzen sowie ihren relevanten internationalen Schnittstellen und Verbindungen im Cyberraum. Erstmals wurde 2020 durch das Bundesministerium des Innern, für Bau und Heimat (BMI) im Rahmen des Nationalen Pakts Cybersicherheit (NPCS) eine Auflistung von Akteuren und Initiativen im Bereich der Cybersicherheit aus Staat, Zivilgesellschaft, Wissenschaft und Wirtschaft als Online-Kompendium⁴ vorgelegt, seither jedoch nicht erneut aktualisiert.

Für eine effektive und effiziente deutsche Aufstellung im Cyberraum bleibt, gerade auch vor dem Hintergrund begrenzter Ressourcen⁵, eine strukturierte politische Herangehensweise unverzichtbar. Im Rahmen unserer Arbeit zu Cybersicherheitspolitik⁶ an der Stiftung Neue Verantwortung möchten wir hierzu einen Beitrag leisten und stellen in dieser seit 2017 bestehenden und kontinuierlich überarbeiteten sowie aktualisierten Publikation daher

- eine **Visualisierung** der staatlichen Cybersicherheitsarchitektur inklusive ihrer internationalen Schnittstellen in statischem (Kapitel 2) sowie zu Beginn jedes Ebenenkapitels und in interaktivem Format unter www.stiftung-nv.de/cybersicherheitsarchitektur,

1 [Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2011.](#)

2 [Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.](#)

3 [Bundesministerium des Innern, für Bau und Heimat, Cybersicherheitsstrategie für Deutschland 2021.](#)

4 [Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland.](#)

5 [Julia Schuetze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.](#)

6 [Stiftung Neue Verantwortung, Internationale Cybersicherheitspolitik.](#)



- ein **Abkürzungsverzeichnis** aller in der Visualisierung verwendeten Akteursabkürzungen und eine **Akteurskategorisierung** (Kapitel 3),
- einen **tabellarischen Policy-Überblick**⁷ für jede Ebene zu Beginn des jeweiligen Kapitels sowie
- ein nach Ebenen sortiertes alphabetisches **Akteursverzeichnis** (Kapitel 4–10) mit Erläuterungen zu Akteur und dessen jeweiligen ebeneninternen sowie auch übergreifenden Verbindungen vor.

Die Cybersicherheitsarchitektur eines Landes beinhaltet alle Akteure – Behörden, Plattformen, Organisationen usw. – die gemäß der nationalen Definition von Cybersicherheit ein Teil des (inter)nationalen Ökosystems sind.

In der vorliegenden Veröffentlichung führen wir nur den staatlichen Teil der Cybersicherheitsarchitektur auf, das bedeutet alle staatlichen und die direkt damit verbundenen Akteure⁸.

Die identifizierten Verknüpfungen in der Visualisierung repräsentieren dabei unterschiedliche Beziehungsaspekte und rangieren von der Entsendung von Mitarbeiter:innen in die verknüpfte Organisation über eine Mitgliedschaft im Beirat sowie finanziellen Zuwendungen bis hin zur Fach- und Rechtsaufsicht.

⁷ Unter Policies werden hierbei beispielsweise auf Bundes-, Länder-, Kommunal- und EU-Ebene relevante Gesetzgebung und Strategien oder auf internationaler Ebene anderweitig relevante wichtige Dokumente wie beispielsweise Konventionen oder Abschlussberichte verstanden. In Einzelfällen können weitere Formen von Policy-Outputs als sinnvolle Aufnahme bewertet werden. Das angegebene Jahr bezieht sich in Fällen mehrerer Optionen auf das Inkrafttreten oder die letzte Änderung.

⁸ Diese Publikation hat dabei den Anspruch, jeweilige Ebenen für den Bereich der Cybersicherheitspolitik so umfassend und vollständig wie möglich und als sinnvoll erachtet darzustellen. Zur Aufnahme eines Akteurs innerhalb der internationalen Ebenen (EU, NATO, UN und Weitere) ist die Identifikation einer Verbindung mit Akteuren innerhalb der deutschen Ebenen (Bundes-, Länder- und Kommunalebene) idealerweise vorhanden, stellt aber kein Ausschlusskriterium dar.



Neben Anpassungen und Aktualisierungen auf allen Ebenen wurden in dieser Auflage folgende **Akteure** auf bereits bestehenden Ebenen neu hinzugefügt:

Abkürzung	Name	Ebene
CYBR360	Initiative für Cybersicherheit	Landesebene
DiNet	Netzwerkstelle Digitalisierung	Landesebene
ZDigBw	Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum	Bundesebene
ZDMV	Zentrum für Digitalisierung Mecklenburg-Vorpommern	Landesebene

Folgende **Policies** wurden auf bestehenden Ebenen hinzugefügt:

Name	Ebene
Agenda Cybersicherheitsforschung des Bundesministeriums für Bildung und Forschung. Maßnahmen im Zuge der Zeitenwende	Bundesebene
Bremische Cybersicherheitsstrategie	Landesebene
Directive on measures for a high common level of cybersecurity across the Union („NIS 2“, Directive (EU) 2022/2555)	EU-Ebene
Directive on the resilience of critical entities (Directive (EU) 2022/2557)	EU-Ebene
Gesetz über die Digitalisierung im Freistaat Bayern (BayDiG)	Landesebene
Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMVG)	Landesebene
Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence (JOIN 2022/49)	EU-Ebene
Regulation of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Regulation (EU) 2022/2554)	EU-Ebene

Weitere rein legislative und judikative Akteure auf allen Ebenen sowie Akteure aus Privatwirtschaft, Wissenschaft und Zivilgesellschaft wurden bisher nicht berücksichtigt.



Basis dieser Veröffentlichung bilden fast ausschließlich öffentlich verfügbare Informationen. Wir freuen uns daher über jeden Hinweis. Änderungs- und Ergänzungsvorschläge nimmt [Frederic Dutke](#) gerne entgegen. Korrekturen an der aktuellen Version werden auf der entsprechenden Webseite in einer Art „Bug Tracker“ zeitnah veröffentlicht.

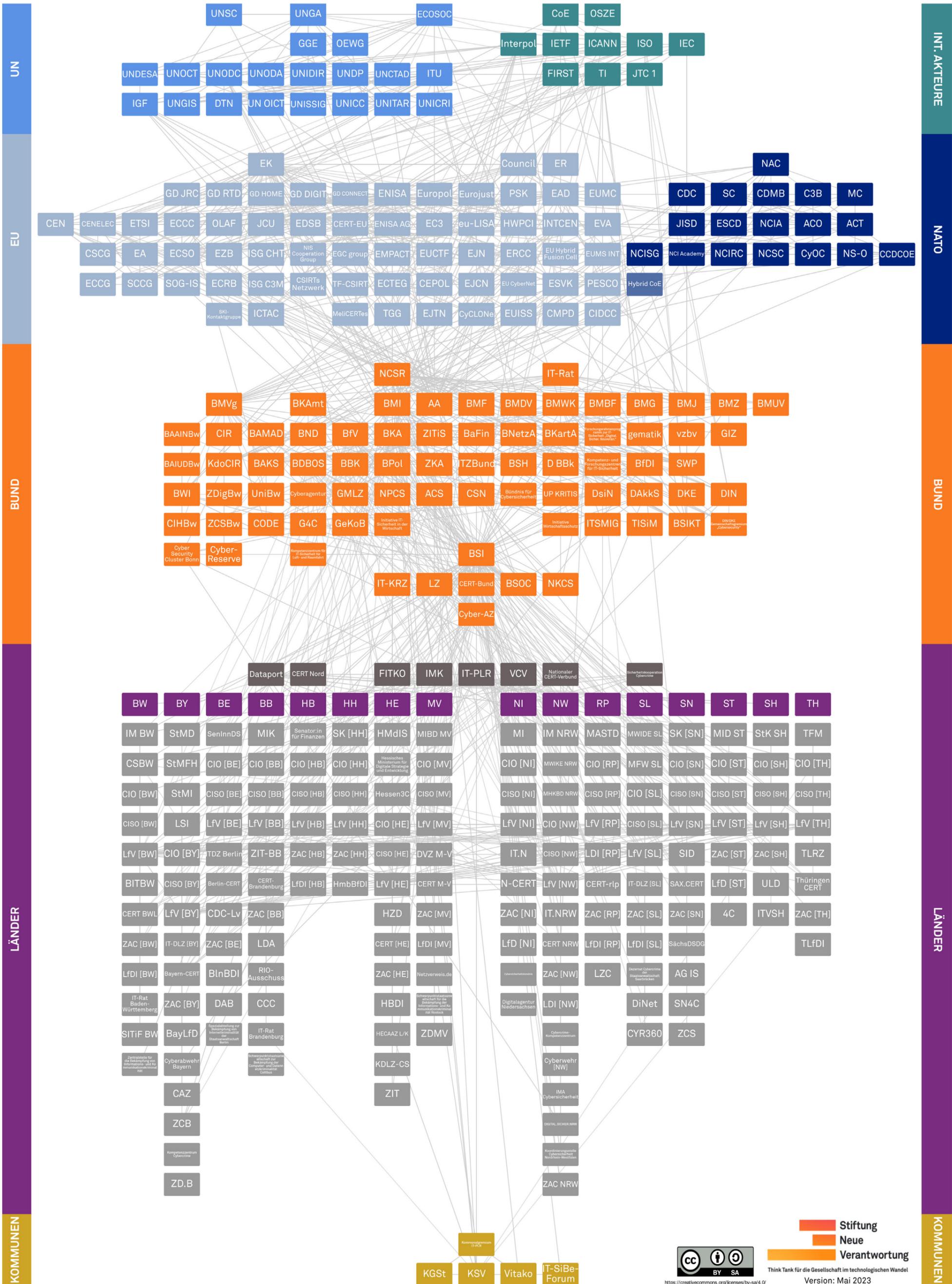
Das Dokument wird auch künftig periodisch aktualisiert, um den neuesten Entwicklungsstand abzubilden und zusätzliche Erweiterungen vorzunehmen. Die nächste Aktualisierung der Cybersicherheitsarchitektur erscheint im September/Okttober 2023.



Versionshistorie

Auflage	Datum	Co-Autor	Co-Autor:in	Veröffentlichung & Anmerkungen
1. Auflage	07/2018	Sven Herpig	Tabea Breternitz	Link
2. Auflage	04/2019	Sven Herpig	Clara Bredenbrock	Link
3. Auflage	11/2019	Sven Herpig	Kira Messing	Link
4. Auflage	03/2020	Sven Herpig	Rebecca Beigel	Link
5. Auflage	10/2020	Sven Herpig	Rebecca Beigel	Link
6. Auflage	04/2021	Sven Herpig	Christina Rupp	Deutsch / English
7. Auflage	10/2021	Sven Herpig	Christina Rupp	Deutsch / English <i>Unterstützt durch die Data Science Unit: Anna Semenova & Pegah Maham</i>
8. Auflage	04/2022	Sven Herpig	Christina Rupp	Deutsch <i>Unterstützt durch die Data Science Unit: Anna Semenova & Pegah Maham</i>
9. Auflage	09/2022	Sven Herpig	Christina Rupp	Deutsch / English <i>Unterstützt durch die Data Science Unit: Anna Semenova & Pegah Maham</i>
10. Auflage	05/2023	Sven Herpig	Christina Rupp Rebecca Beigel Frederic Dutke	Vorliegende Version

STAATLICHE CYBERSICHERHEITSARCHITEKTUR



Stiftung
Neue
Verantwortung



Think Tank für die Gesellschaft im technologischen Wandel
Version: Mai 2023

<https://creativecommons.org/licenses/by-sa/4.0/>



3. Abkürzungsverzeichnis und Akteurskategorisierung

Zur Nachvollziehbarkeit enthält diese Liste alle innerhalb unserer Visualisierung verwendeten Abkürzungen und Bezeichnungen. In Fällen, in denen es für einen Akteur deutsche und englische offizielle Abkürzungen gibt, werden in dieser Publikation bewusst die deutschen Pendanten verwendet. Erläuterungen für alle hier genannten Akteure finden sich auf den jeweiligen Ebenen in alphabetischer Reihenfolge. Auf der Bundesebene sind aufgeführte Akteure im Geschäftsbereich eines Ministeriums diesen ebenso in alphabetischer Sortierung untergeordnet. Kursiv gedruckte Institutionen befinden sich entweder in der Planung oder im Aufbau.

Im Rahmen der Akteurskategorisierung wurden sämtliche Akteure nach ihren Zuständigkeiten, Aufgabenfeldern und Funktionen inhaltlich und thematisch eingeordnet. Sofern zutreffend, können Akteure auch mehreren Kategorien zugeordnet sein. Basis für die Kategorisierung eines Akteurs stellt die in dieser Publikation angeführte entsprechende Erläuterung dar.

Zusätzlich zu der Beschreibung der Akteure und Erklärung ihrer Verbindungen, ermöglicht die Kategorisierung einen vertieften und transparenten Ein- und Überblick in die deutsche Cybersicherheitsarchitektur. Darüber hinaus können beispielsweise gemeinsame Handlungsfelder unterschiedlichster Akteure identifiziert und diese dadurch entsprechenden Clustern zugeordnet werden.

Neben dieser tabellarischen Übersicht sind die den Akteuren zugeschriebene(n) Kategorie(n) auch bei den jeweiligen Akteureinträgen am linken Rand durch entsprechende Symbole abgebildet. Die Kategorisierung wurde auch in die interaktive Visualisierung durch Anzeige der einem Akteur zugeordnete(n) Kategorie(n) integriert.



Akteuren konnte eine oder mehrere dieser sechs Kategorien zugeordnet werden:



Aus- und Weiterbildung

Akteure, die Aus- und Weiterbildungsangebote, -formate oder -plattformen für verschiedene Zielgruppen organisieren bzw. zur Verfügung stellen. Dieser Wissensaustausch und -transfer kann u.a. Trainings, Kurse oder Fortbildungen in den Bereichen Cybersicherheit oder -verteidigung umfassen.



Forschung und Forschungsförderung

Akteure, die aktiv in die Forschung von IT- und cybersicherheitsrelevanten Themen involviert sind, beispielsweise als Forschungsinstitut, oder diese von außen durch entsprechende Förderung, u.a. durch die Finanzierung von Kompetenzzentren oder die Etablierung bzw. das Management von inhaltlich relevanten Forschungsprogrammen, unterstützen.



Informationsaustausch- und Kooperationsplattform

Akteure, die sich dem Teilen von Informationen, und/oder der Vernetzung, und/oder der Verbesserung von Beziehungen sowie der Zusammenarbeit zur Stärkung von IT- und Cybersicherheit verschrieben haben. Entsprechende Foren und Netzwerke können mit thematischen Schwerpunkten, aber auch themenübergreifend mit unterschiedlichen Institutionalisierungsgraden etabliert sein.



Normung und Zertifizierung

Akteure, die an der Entwicklung und Vereinbarung von Normen, Standards und Zertifizierungen für auf IKT-basierten Anwendungen, Systemen und Netzwerken arbeiten, die IT- und cybersicherheitsrelevante Vorgaben beinhalten.



Operative IT- und Cybersicherheit

Akteure, die operativ Maßnahmen umsetzen, die zu mehr IT- und Cybersicherheit führen sollen, u.a. Prävention und Detektion von sowie Reaktion auf Vorfälle(n), Bekämpfung von Cyberkriminalität oder auch das Verhängen von Bußgeldern für die Missachtung von Richtlinien.



Policy und Strategie

Akteure, denen die inhaltliche Politikgestaltung sowie die Festlegung von Policy-Zielen im Bereich der IT- und Cybersicherheit obliegt und zudem häufig die Verantwortung für die Erarbeitung relevanter Gesetzgebung, Richtlinien und/oder Strategien tragen. Die Entscheidungen und Outputs dieser Akteure stellen oftmals die Weichen für viele andere Akteure innerhalb der Cybersicherheitsarchitektur. Darüber hinaus fallen hierunter Akteure, die Inputs in politische Prozesse, wie zum Beispiel Beratung, liefern.



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
4C	Cybercrime Competence Center	Operative IT- und Cybersicherheit
A		
AA	Auswärtiges Amt	Policy und Strategie
ACO	Allied Command Operations	Operative IT- und Cybersicherheit
ACS	Allianz für Cyber-Sicherheit	Informationsaustausch- und Kooperationsplattform
ACT	Allied Command Transformation	Aus- und Weiterbildung Operative IT- und Cybersicherheit
AG IS	Arbeitsgruppe Informationssicherheit	Policy und Strategie
B		
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr	Operative IT- und Cybersicherheit
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht	Operative IT- und Cybersicherheit
BAIUSBw	Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr	Operative IT- und Cybersicherheit
BAKS	Bundesakademie für Sicherheitspolitik	Aus- und Weiterbildung
BAMAD	Bundesamt für den Militärischen Abschirmdienst	Operative IT- und Cybersicherheit
Bayern-CERT	Computer Emergency Response Team Bayern	Operative IT- und Cybersicherheit
BayLfD	Bayerische:r Landesbeauftragte:r für den Datenschutz	Operative IT- und Cybersicherheit
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Operative IT- und Cybersicherheit
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
Berlin-CERT	Computer Emergency Response Team Berlin	Operative IT- und Cybersicherheit
BfDI	Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit	Operative IT- und Cybersicherheit
BFV	Bundesamt für Verfassungsschutz	Operative IT- und Cybersicherheit
BITBW	Landesoberbehörde IT Baden-Württemberg	Operative IT- und Cybersicherheit
BKA	Bundeskriminalamt	Operative IT- und Cybersicherheit
BKAmt	Bundeskanzleramt	Policy und Strategie
BKartA	Bundeskartellamt	Policy und Strategie
BlnBDI	Berliner Beauftragte:r für Datenschutz und Informationsfreiheit	Operative IT- und Cybersicherheit
BMBF	Bundesministerium für Bildung und Forschung	Policy und Strategie
BMDV	Bundesministerium für Digitales und Verkehr	Policy und Strategie
BMF	Bundesministerium für Finanzen	Policy und Strategie
BMG	Bundesministerium für Gesundheit	Policy und Strategie
BMI	Bundesministerium des Innern und für Heimat	Policy und Strategie
BMJ	Bundesministerium der Justiz	Policy und Strategie
BMUV	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz	Policy und Strategie
BMVg	Bundesministerium der Verteidigung	Policy und Strategie
BMWK	Bundesministerium für Wirtschaft und Klimaschutz	Policy und Strategie
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung	Policy und Strategie



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
BND	Bundesnachrichtendienst	Operative IT- und Cybersicherheit
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen	Operative IT- und Cybersicherheit
BPol	Bundespolizei	Operative IT- und Cybersicherheit
BSH	Bundesamt für Seeschifffahrt und Hydrographie	Operative IT- und Cybersicherheit
BSI	Bundesamt für Sicherheit in der Informationstechnik	Forschung und Forschungsförderung Informationsaustausch- und Kooperationsplattform Normung und Zertifizierung Operative IT- und Cybersicherheit
BSIKT	Beirat für Standardisierung in der Informations- und Kommunikationstechnologie	Normung und Zertifizierung
BSOC	Bundes Security Operations Center	Operative IT- und Cybersicherheit
Bündnis für Cybersicherheit	Bündnis für Cybersicherheit	Informationsaustausch- und Kooperationsplattform
BWI	Bundesweite IT-Systemhaus GmbH	Operative IT- und Cybersicherheit
C		
C3B	NATO Consultation, Control and Command Board	Policy und Strategie
CAZ	Cyber-Allianz-Zentrum	Operative IT- und Cybersicherheit
CCC	Cyber-Competence-Center	Operative IT- und Cybersicherheit
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	Forschung und Forschungsförderung Aus- und Weiterbildung
CDC	Cyber Defence Committee	Policy und Strategie
CDC-Lv	Cyber Defense Center der Landesverwaltung Berlin	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
CDMB	NATO Cyber Defence Management Board	Policy und Strategie
CEN	Europäisches Komitee für Normung	Normung und Zertifizierung
CENELEC	Europäisches Komitee für elektrotechnische Normung	Normung und Zertifizierung
CEPOL	Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung	Aus- und Weiterbildung
CERT [HE]	Computer Emergency Response Team Hessen	Operative IT- und Cybersicherheit
CERT BWL	Computer Emergency Response Team Baden-Württemberg	Operative IT- und Cybersicherheit
CERT M-V	Computer Emergency Response Team Mecklenburg-Vorpommern	Operative IT- und Cybersicherheit
CERT Nord	CERT Nord	Operative IT- und Cybersicherheit
CERT NRW	Computer Emergency Response Team Nordrhein-Westfalen	Operative IT- und Cybersicherheit
CERT-Brandenburg	Computer Emergency Response Team Brandenburg	Operative IT- und Cybersicherheit
CERT-Bund	Computer Emergency Response Team der Bundesverwaltung	Operative IT- und Cybersicherheit
CERT-EU	Computer Emergency Response Team der Europäischen Kommission	Operative IT- und Cybersicherheit
CERT-rlp	Computer Emergency Response Team Rheinland-Pfalz	Operative IT- und Cybersicherheit
CIDCC	Cyber and Information Domain Coordination Centre	Operative IT- und Cybersicherheit
CIHBw	Cyber Innovation Hub	Forschung und Forschungsförderung
CIO [Bundesland]	Landesbeauftragte:r für Informationstechnologie	Policy und Strategie
CIR	Organisationsbereich Cyber- und Informationsraum	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
CISO [Bundesland]	Informationssicherheits-beauftragte:r	Operative IT- und Cybersicherheit
CMPD	Direktion Krisenbewältigung und Planung	Policy und Strategie
CODE	Forschungsinstitut Cyber Defence	Forschung und Forschungsförderung
CoE	Europarat	Policy und Strategie
Council	Rat der Europäischen Union	Policy und Strategie
CSBW	Cybersicherheitsagentur Baden-Württemberg	Operative IT- und Cybersicherheit
CSCG	CEN/CENELEC Cyber Security Coordination Group	Normung und Zertifizierung
CSIRTs Netzwerk	Computer Security Incident Response Teams Netzwerk	Operative IT- und Cybersicherheit Informationsaustausch- und Kooperationsplattform
CSN	Cyber-Sicherheitsnetzwerk	Informationsaustausch- und Kooperationsplattform
Cyber Security Cluster Bonn	Cyber Security Cluster Bonn e.V.	Informationsaustausch- und Kooperationsplattform
Cyberabwehr Bayern	Cyberabwehr Bayern	Informationsaustausch- und Kooperationsplattform Operative IT- und Cybersicherheit
Cyberagentur	Agentur für Innovation in der Cybersicherheit	Forschung und Forschungsförderung
Cybercrime-Kompetenzzentrum	Cybercrime-Kompetenzzentrum	Operative IT- und Cybersicherheit
Cyber-Reserve	Cyber-Reserve	Operative IT- und Cybersicherheit
Cybersicherheitsbündnis	Cybersicherheitsbündnis	Informationsaustausch- und Kooperationsplattform
Cyberwehr [NW]	Cyberwehr	Operative IT- und Cybersicherheit
CyCLONe	Cyber Crisis Liaison Organisation Network	Informationsaustausch- und Kooperationsplattform Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
CyOC	NATO Cyberspace Operations Centre	Operative IT- und Cybersicherheit
CYR360	Initiative für Cybersicherheit	Informationsaustausch- und Kooperationsplattform Operative IT- und Cybersicherheit Aus- und Weiterbildung
D		
D BBk*	Deutsche Bundesbank	Operative IT- und Cybersicherheit
DAB	Digitalagentur Berlin	Informationsaustausch- und Kooperationsplattform
DAkKS	Deutsche Akkreditierungsstelle	Normung und Zertifizierung
Dataport	Dataport	Operative IT- und Cybersicherheit
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken	Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken	Operative IT- und Cybersicherheit
DIGITAL.SICHER.NRW	Kompetenzzentrum für Cybersicherheit in der Wirtschaft	Informationsaustausch- und Kooperationsplattform
Digitalagentur Niedersachsen	Digitalagentur Niedersachsen	Informationsaustausch- und Kooperationsplattform
DIN	Deutsches Institut für Normung	Normung und Zertifizierung
DIN/DKE Gemeinschaftsgremium „Cybersecurity“	DIN/DKE Gemeinschaftsgremium „Cybersecurity“	Normung und Zertifizierung
DiNet	Netzwerkstelle Digitalisierung	Informationsaustausch- und Kooperationsplattform
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE	Normung und Zertifizierung
DsiN	Deutschland sicher im Netz e.V.	Informationsaustausch- und Kooperationsplattform
DTN	United Nations Digital and Technology Network	Informationsaustausch- und Kooperationsplattform
DVZ M-V	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern	Operative IT- und Cybersicherheit

* Aufgrund der gleichlautenden Abkürzung mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), wird die offizielle Abkürzung der Deutschen Bundesbank (BBk) bei Verwendung im Rahmen dieser Publikation und Visualisierung leicht ergänzt um „D BBk“.



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
E		
EA	Europäische Kooperation für Akkreditierung	Normung und Zertifizierung
EAD	Europäischer Auswärtiger Dienst	Policy und Strategie
EC3	Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität	Operative IT- und Cybersicherheit
ECCC	Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit	Forschung und Forschungsförderung Informationsaustausch- und Kooperationsplattform
ECCG	Europäische Gruppe für die Cybersicherheitszertifizierung	Normung und Zertifizierung
ECOSOC	Wirtschafts- und Sozialrat der Vereinten Nationen	Policy und Strategie
ECRB	Euro Cyber Resilience Board for pan-European Financial Infrastructures	Informationsaustausch- und Kooperationsplattform
ECSO	European Cyber Security Organisation	Informationsaustausch- und Kooperationsplattform
ECTEG	European Cybercrime Training and Education Group	Aus- und Weiterbildung
EDSB	Europäische:r Datenschutzbeauftragte:r	Operative IT- und Cybersicherheit
EGC group	European Government CERTs group	Informationsaustausch- und Kooperationsplattform
EJCN	European Judicial Cybercrime Network	Informationsaustausch- und Kooperationsplattform
EJN	European Judicial Network	Aus- und Weiterbildung Informationsaustausch- und Kooperationsplattform
EJTN	European Judicial Training Network	Aus- und Weiterbildung
EK	Europäische Kommission	Policy und Strategie



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
EMPACT	European Multidisciplinary Platform Against Criminal Threats	Informationsaustausch- und Kooperationsplattform Operative IT- und Cybersicherheit
ENISA	Agentur der Europäischen Union für Cybersicherheit	Informationsaustausch- und Kooperationsplattform Normung und Zertifizierung Policy und Strategie
ENISA AG	ENISA-Beratungsgruppe	Informationsaustausch- und Kooperationsplattform
ER	Europäischer Rat	Policy und Strategie
ERCC	Zentrum für die Koordination von Notfallmaßnahmen	Operative IT- und Cybersicherheit
ESCD	Emerging Security Challenges Division	Policy und Strategie
ESVK	Europäisches Sicherheits- und Verteidigungskolleg	Aus- und Weiterbildung
ETSI	Europäisches Institut für Telekommunikationsnormen	Normung und Zertifizierung
EU CyberNet	EU Cyber Capacity Building Network	Aus- und Weiterbildung Informationsaustausch- und Kooperationsplattform
EU Hybrid Fusion Cell	EU-Analyseeinheit für hybride Bedrohungen	Informationsaustausch- und Kooperationsplattform
EUCTF	European Union Cybercrime Task Force	Informationsaustausch- und Kooperationsplattform
EUISS	Institut der Europäischen Union für Sicherheitsstudien	Forschung und Forschungsförderung Policy und Strategie
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht	Operative IT- und Cybersicherheit
EUMC	Militärausschuss der Europäischen Union	Policy und Strategie



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
EUMS INT	Intelligence Directorate des EU-Militärstabs	Operative IT- und Cybersicherheit
Eurojust	Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen	Operative IT- und Cybersicherheit
Europol	Europäisches Polizeiamt	Operative IT- und Cybersicherheit
EVA	Europäische Verteidigungsagentur	Forschung und Forschungsförderung Policy und Strategie
EZB	Europäische Zentralbank	Operative IT- und Cybersicherheit
F		
FIRST	Forum of Incident Response and Security Teams	Informationsaustausch- und Kooperationsplattform
FITKO	Föderale IT-Kooperation	Informationsaustausch- und Kooperationsplattform Policy und Strategie
Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän.“	Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän.“	Forschung und Forschungsförderung
G		
G4C	German Competence Centre against Cyber Crime	Informationsaustausch- und Kooperationsplattform
GD CONNECT	Generaldirektion Kommunikationsnetze, Inhalte und Technologien	Policy und Strategie
GD DIGIT	Generaldirektion Informatik	Policy und Strategie
GD HOME	Generaldirektion Migration und Inneres	Policy und Strategie
GD JRC	Gemeinsame Forschungsstelle	Forschung und Forschungsförderung Policy und Strategie
GD RTD	Generaldirektion Forschung und Innovation	Policy und Strategie



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
GeKoB	Gemeinsames Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern	Informationsaustausch- und Kooperationsplattform
gematik	gematik	Operative IT- und Cybersicherheit
GGE	Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security	Policy und Strategie
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit	Aus- und Weiterbildung
GMLZ	Gemeinsames Melde- und Lagezentrum von Bund und Ländern	Operative IT- und Cybersicherheit
H		
HBDI	Hessische:r Beauftragte:r für Datenschutz und Informationsfreiheit	Operative IT- und Cybersicherheit
HECAAZ L/K	Hessisches Cyberabwehrbildungszentrum Land/Kommunen	Aus- und Weiterbildung
Hessen3C	Hessen Cyber Competence Center	Operative IT- und Cybersicherheit
Hessisches Ministerium für Digitale Strategie und Entwicklung	Hessisches Ministerium für Digitale Strategie und Entwicklung	Policy und Strategie
HmbBfDI	Hamburgische:r Beauftragte:r für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg	Operative IT- und Cybersicherheit
HMdIS	Hessisches Ministerium des Innern und für Sport	Policy und Strategie
HWPCI	Horizontale Ratsarbeitsgruppe „Fragen des Cyberraums“	Policy und Strategie
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats	Forschung und Forschungsförderung Informationsaustausch- und Kooperationsplattform
HZD	Hessische Zentrale für Datenverarbeitung	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
I		
ICANN	Internet Corporation for Assigned Names and Numbers	Normung und Zertifizierung
ICTAC	ICT Advisory Committee of the EU Agencies	Informationsaustausch- und Kooperationsplattform
IEC	Internationale Elektrotechnische Kommission	Normung und Zertifizierung
IETF	Internet Engineering Task Force	Normung und Zertifizierung
IGF	Internet Governance Forum	Policy und Strategie Informationsaustausch- und Kooperationsplattform
IM BW	Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg	Policy und Strategie
IM NRW	Ministerium des Innern des Landes Nordrhein-Westfalen	Policy und Strategie
IMA Cybersicherheit	Interministerieller Ausschuss Cybersicherheit	Policy und Strategie
IMK	Innenministerkonferenz	Policy und Strategie
Initiative IT-Sicherheit in der Wirtschaft	Initiative IT-Sicherheit in der Wirtschaft	Informationsaustausch- und Kooperationsplattform
Initiative Wirtschaftsschutz	Initiative Wirtschaftsschutz	Informationsaustausch- und Kooperationsplattform
INTCEN	Zentrum für Informationsgewinnung und -analyse	Operative IT- und Cybersicherheit
Interpol	Internationale Kriminalpolizeiliche Organisation	Operative IT- und Cybersicherheit
ISG C3M	Inter-Service Group „Community Capacity in Crisis-Management“	Informationsaustausch- und Kooperationsplattform
ISG CHT	Inter-Service Group „Countering Hybrid Threats“	Informationsaustausch- und Kooperationsplattform
ISO	Internationale Organisation für Normung	Normung und Zertifizierung
IT.N	IT.Niedersachsen	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
IT.NRW	Landesbetrieb Information und Technik Nordrhein-Westfalen	Operative IT- und Cybersicherheit
IT-DLZ [BY]	IT-Dienstleistungszentrum des Freistaats Bayern	Operative IT- und Cybersicherheit
IT-DLZ [SL]	Landesamt für IT-Dienstleistungen	Operative IT- und Cybersicherheit
ITDZ Berlin	IT-Dienstleistungszentrum Berlin	Operative IT- und Cybersicherheit
IT-KRZ	Nationales IT-Krisenreaktionszentrum	Operative IT- und Cybersicherheit
IT-PLR	IT-Planungsrat	Policy und Strategie
IT-Rat	IT-Rat	Policy und Strategie
IT-Rat Baden-Württemberg	IT-Rat Baden-Württemberg	Policy und Strategie
IT-Rat Brandenburg	IT-Rat Brandenburg	Policy und Strategie
IT-SiBe-Forum	IT-SiBe-Forum	Informationsaustausch- und Kooperationsplattform
ITSMIG	IT Security made in Germany	Informationsaustausch- und Kooperationsplattform
ITU	Internationale Fernmeldeunion	Policy und Strategie Normung und Zertifizierung
ITVSH	IT-Verbund Schleswig-Holstein	Informationsaustausch- und Kooperationsplattform
ITZBund	Informationstechnikzentrum Bund	Operative IT- und Cybersicherheit
J		
JCU	Joint Cyber Unit	Informationsaustausch- und Kooperationsplattform Operative IT- und Cybersicherheit
JISD	Joint Intelligence and Security Division	Operative IT- und Cybersicherheit
JTC 1	ISO and IEC Joint Technical Committee	Normung und Zertifizierung



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
K		
KDLZ-CS	Kommunales Dienstleistungszentrum Cybersicherheit	Operative IT- und Cybersicherheit
KdoCIR	Kommando Cyber- und Informationsraum	Operative IT- und Cybersicherheit
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsmanagement	Informationsaustausch- und Kooperationsplattform
Kommunalgremium IT-PLR	Kommunalgremium des IT-Planungsrates	Policy und Strategie
Kompetenz- und Forschungszentren für IT-Sicherheit	Kompetenz- und Forschungszentren für IT-Sicherheitsforschung	Forschung und Forschungsförderung
Kompetenzzentrum Cybercrime	Kompetenzzentrum Cybercrime	Operative IT- und Cybersicherheit
Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt	Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt	Operative IT- und Cybersicherheit
Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen	Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen	Informationsaustausch- und Kooperationsplattform
KSV	Kommunale Spitzenverbände	Policy und Strategie
L		
LDA	Landesbeauftragte:r für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg	Operative IT- und Cybersicherheit
LDI [NW]	Landesbeauftragte:r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen	Operative IT- und Cybersicherheit
LDI [RP]	Landesbetrieb Daten und Information	Operative IT- und Cybersicherheit
LfD [Bundesland]	Landesbeauftragte:r für den Datenschutz	Operative IT- und Cybersicherheit
LfDI [Bundesland]	Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit	Operative IT- und Cybersicherheit
LfV [Bundesland]	Landesbehörde für Verfassungsschutz	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
LSI	Landesamt für Sicherheit in der Informationstechnik Bayern	Operative IT- und Cybersicherheit
LZ	Nationales IT-Lagezentrum	Operative IT- und Cybersicherheit
LZC	Landeszentralstelle Cybercrime	Operative IT- und Cybersicherheit
M		
MASTD	Ministerium für Arbeit, Soziales, Transformation und Digitalisierung	Policy und Strategie
MC	NATO-Militärausschuss	Policy und Strategie
MeliCERTes	MeliCERTes	Informationsaustausch- und Kooperationsplattform
MFW SL	Ministerium der Finanzen und für Wissenschaft	Policy und Strategie
MHKBD NRW	Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen	Policy und Strategie
MI	Niedersächsisches Ministerium für Inneres und Sport	Policy und Strategie
MIBD MV	Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern	Policy und Strategie
MID ST	Ministerium für Infrastruktur und Digitales Sachsen-Anhalt	Policy und Strategie
MIK	Ministerium des Innern und für Kommunales Brandenburg	Policy und Strategie
MWIDE SL	Ministerium für Wirtschaft, Innovation, Digitales und Energie	Policy und Strategie
MWIKE NRW	Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen	Policy und Strategie
N		
NAC	Nordatlantikrat	Policy und Strategie



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
Nationaler CERT-Verbund	Nationaler CERT-Verbund	Informationsaustausch- und Kooperationsplattform
Cyber-AZ	Nationales Cyber-Abwehrzentrum	Informationsaustausch- und Kooperationsplattform
N-CERT	Computer Emergency Response Team Niedersachsen	Operative IT- und Cybersicherheit
NCI Academy	NCI Academy	Aus- und Weiterbildung
NCIA	NATO Communications and Information Agency	Operative IT- und Cybersicherheit
NCIRC	NATO Computer Incident Response Capability	Operative IT- und Cybersicherheit
NCISG	NATO Communication and Information Systems Group	Operative IT- und Cybersicherheit
NCSC	NATO Cyber Security Centre	Operative IT- und Cybersicherheit
NCSR	Nationaler Cyber-Sicherheitsrat	Policy und Strategie
Netzverweis.de	Netzverweis.de	Operative IT- und Cybersicherheit
NIS Cooperation Group	Kooperationsgruppe unter der NIS-Richtlinie	Informationsaustausch- und Kooperationsplattform
NKCS	Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung	Forschung und Forschungsförderung
NPCS	Nationaler Pakt Cybersicherheit	Informationsaustausch- und Kooperationsplattform
NS-O	NATO School Oberammergau	Aus- und Weiterbildung
O		
OEWG	Open-ended Working Group on security of and in the use of information and communications technologies	Policy und Strategie
OLAF	Europäisches Amt für Betrugsbekämpfung	Operative IT- und Cybersicherheit
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa	Policy und Strategie



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
P		
PESCO	Ständige Strukturierte Zusammenarbeit	Informationsaustausch- und Kooperationsplattform
PSK	Politisches und Sicherheitspolitisches Komitee	Policy und Strategie
R		
RIO-Ausschuss	Ausschuss der Ressort Information Officer	Operative IT- und Cybersicherheit
S		
SächsDSDG	Sächsische:r Datenschutzbeauftragte:r	Operative IT- und Cybersicherheit
SAX.CERT	Computer Emergency Response Team Sachsen	Operative IT- und Cybersicherheit
SC	NATO Security Committee	Policy und Strategie
SCCG	Gruppe der Interessenträger für die Cybersicherheits-zertifizierung	Normung und Zertifizierung
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	Operative IT- und Cybersicherheit
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetz-kriminalität Cottbus	Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetz-kriminalität Cottbus	Operative IT- und Cybersicherheit
Senator:in für Finanzen	Der:die Senator:in für Finanzen	Policy und Strategie
SenInnDS	Senatsverwaltung für Inneres, Digitalisierung und Sport Berlin	Policy und Strategie
Sicherheitskooperation Cybercrime	Sicherheitskooperation Cybercrime	Informationsaustausch- und Kooperationsplattform
SID	Staatsbetrieb Sächsische Informatik Dienste	Operative IT- und Cybersicherheit
SITiF BW	Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
SK [HH]	Senatskanzlei Hamburg	Policy und Strategie
SK [SN]	Sächsische Staatskanzlei	Policy und Strategie
SKI-Kontaktgruppe	Kontaktgruppe zum Schutz Kritischer Infrastrukturen	Informationsaustausch- und Kooperationsplattform
SN4C	Cyber Crime Competence Center Sachsen	Operative IT- und Cybersicherheit
SOG-IS	Senior Officials Group Information Systems Security	Normung und Zertifizierung
Spezialabteilung zu Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	Operative IT- und Cybersicherheit
StK SH	Staatskanzlei Schleswig-Holstein	Policy und Strategie
StMD	Bayerisches Staatsministerium für Digitalisierung	Policy und Strategie
StMFH	Bayerisches Staatsministerium der Finanzen und für Heimat	Policy und Strategie
StMI	Bayerisches Staatsministerium des Innern, für Sport und Integration	Policy und Strategie
SWP	Stiftung Wissenschaft und Politik	Forschung und Forschungsförderung Policy und Strategie
T		
TF-CSIRT	Reference Incident Classification Taxonomy Task Force	Informationsaustausch- und Kooperationsplattform
TFM	Thüringisches Finanzministerium	Policy und Strategie
TGG	Taxonomy Governance Group	Informationsaustausch- und Kooperationsplattform
Thüringen CERT	Computer Emergency Response Team Thüringen	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
TI	Trusted Introducer	Informationsaustausch- und Kooperationsplattform
TISiM	Transferstelle IT-Sicherheit im Mittelstand	Informationsaustausch- und Kooperationsplattform
TLfDI	Thüringische:r Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit	Operative IT- und Cybersicherheit
TLRZ	Thüringer Landesrechenzentrum	Operative IT- und Cybersicherheit
U		
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Operative IT- und Cybersicherheit
UN OICT	United Nations Office of Information and Communications Technology	Operative IT- und Cybersicherheit
UNCTAD	Konferenz der Vereinten Nationen für Handel und Entwicklung	Policy und Strategie
UNDESA	Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen	Policy und Strategie
UNDP	Entwicklungsprogramm der Vereinten Nationen	Policy und Strategie
UNGA	UN-Generalversammlung	Policy und Strategie
UNGIS	United Nations Group on the Information Society	Informationsaustausch- und Kooperationsplattform
UniBw	Universitäten der Bundeswehr	Aus- und Weiterbildung Forschung und Forschungsförderung
UNICC	United Nations International Computing Centre	Operative IT- und Cybersicherheit
UNICRI	UN-Institut für interregionale Kriminalitäts- und Justizforschung	Policy und Strategie Forschung und Forschungsförderung



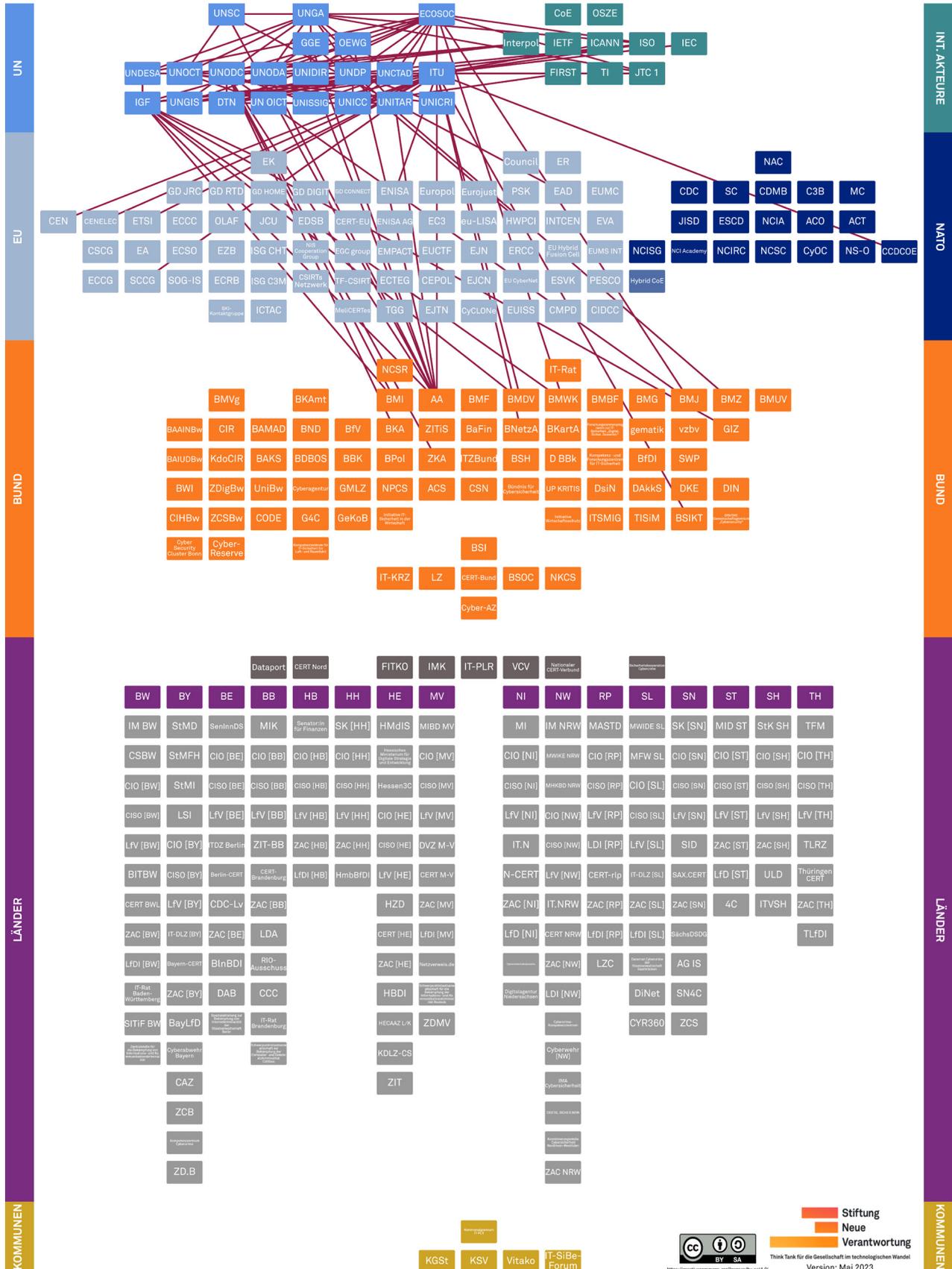
Abkürzungen/Bezeichnungen	Name	Akteurskategorie
UNIDIR	UN-Institut für Abrüstungsforschung	Policy und Strategie Forschung und Forschungsförderung
UNISSIG	United Nations Information Security Special Interest Group	Informationsaustausch- und Kooperationsplattform
UNITAR	Ausbildungs- und Forschungsinstitut der Vereinten Nationen	Aus- und Weiterbildung Forschung und Forschungsförderung
UNOCT	United Nations Office of Counter-Terrorism	Policy und Strategie
UNODA	Büro der Vereinten Nationen für Abrüstungsfragen	Policy und Strategie
UNODC	Büro der Vereinten Nationen für Drogen- und Verbrechenbekämpfung	Policy und Strategie
UNSC	UN-Sicherheitsrat	Policy und Strategie
UP KRITIS	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen	Informationsaustausch- und Kooperationsplattform
V		
VCV	Verwaltungs-CERT-Verbund	Informationsaustausch- und Kooperationsplattform
Vitako	Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister	Informationsaustausch- und Kooperationsplattform
vzbv	Bundesverband der Verbraucherzentralen und Verbraucherverbände	Policy und Strategie
Z		
ZAC [Bundesland]	Zentrale Ansprechstelle Cybercrime für die Wirtschaft	Operative IT- und Cybersicherheit
ZAC NRW	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen	Operative IT- und Cybersicherheit
ZCB	Zentralstelle Cybercrime Bayern	Operative IT- und Cybersicherheit



Abkürzungen/Bezeichnungen	Name	Akteurskategorie
ZCS	Zentralstelle Cybercrime Sachsen	Operative IT- und Cybersicherheit
ZCSBw	Zentrum für Cyber-Sicherheit der Bundeswehr	Operative IT- und Cybersicherheit
ZD.B	Zentrum Digitalisierung.Bayern	Forschung und Forschungsförderung Informationsaustausch- und Kooperationsplattform
ZDigBw	Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum	Operative IT- und Cybersicherheit Normung und Zertifizierung
ZDMV	Zentrum für Digitalisierung Mecklenburg-Vorpommern	Operative IT- und Cybersicherheit
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	Operative IT- und Cybersicherheit
ZIT	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität	Operative IT- und Cybersicherheit
ZIT-BB	Brandenburgischer IT-Dienstleister	Operative IT- und Cybersicherheit
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich	Operative IT- und Cybersicherheit
ZKA	Zollkriminalamt	Operative IT- und Cybersicherheit



4. Erläuterung – Akteure auf UN-Ebene





Policy-Überblick

Jahr	Name
2021	Final Substantive Report: Open-ended working group on developments in the field of information and telecommunications in the context of international security (A/AC.290/2021/CRP.2)
2021	Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135)
2015	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)
2013	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)
2010	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)



Ausbildungs- und Forschungsinstitut der Vereinten Nationen (UNITAR)

Als Ausbildungs- und Forschungseinrichtung der UN hat sich UNITAR der Bereitstellung von Schulungsmöglichkeiten verschrieben, um globale und nationale Entscheidungsfindungsprozesse und Maßnahmen im Sinne der Gestaltung einer besseren Zukunft sowie der Implementierung der Agenda 2030 zu verbessern. UNITAR's Angebote richten sich sowohl an Institutionen und Personen aus dem öffentlichen sowie dem Privatsektor. UNITAR bietet auch für den Bereich der Cybersicherheit Trainings- und Bildungsangebote an. Diese befassen sich inhaltlich unter anderem mit Kriegsführung im Cyberraum und humanitärem Völkerrecht, Cyberoperationen und Menschenrechten oder digitaler Diplomatie. Gemeinsam mit anderen Organisationen schreibt und richtet UNITAR ein „Cyber Policy and United Nations Negotiations Fellowship“ für Frauen aus der ganzen Welt aus.

UNITAR ist im UN-System eine gemeinsame Forschungs- und Ausbildungseinrichtung der UNGA und des ECOSOC. UNITAR nimmt Leistungen des UNICC in Anspruch und hat den vom UNOCT koordinierten UN Global Counter-Terrorism Coordination Compact unterzeichnet. Deutschland ist im Kuratorium von UNITAR durch den: die Botschafter:in Deutschlands (AA) bei den UN in Genf vertreten⁹.

⁹ [GIP Digital Watch, United Nations Institute for Training and Research.](#)
[United Nations Institute for Training and Research, Cyber Policy and United Nations Negotiations Fellowship.](#)
[United Nations Institute for Training and Research, The Board of Trustees.](#)
[United Nations Institute for Training and Research, The Institute.](#)



Büro der Vereinten Nationen für Abrüstungsfragen (UNODA)

Das Büro der Vereinten Nationen für Abrüstungsfragen unterstützt globale als auch regionale Maßnahmen und Bemühungen, die zu Fortschritten in der kontrollierten Entwaffnung, insbesondere von Massenvernichtungswaffen, beitragen. Diese schließen beispielsweise die Bereitstellung objektiver Informationen, vertrauensbildende Initiativen in militärischen Angelegenheiten oder die Auseinandersetzung mit den humanitären Auswirkungen von neuen Waffentechnologien ein. Im Bereich der Cybersicherheit bietet UNODA unter anderem einen kostenlosen Online-Kurs zu Cyberdiplomatie an und hat einen Kommentar zu freiwilligen Normen für verantwortliches Staatenverhalten in der Nutzung von IKT veröffentlicht. Gemeinsam mit dem Cybersecurity Tech Accord hat UNODA einen Wettbewerb (Apps 4 Digital Peace) ausgerufen, um die Entwicklung von Anwendungen zu fördern, die in der Lage sein sollen, die Stabilität im Cyberraum zu erhöhen und Konfliktpotenziale sowie böswillige Nutzungsverhalten zu verringern.

UNODA ist Teil des UN-Sekretariats und unterstützt unter anderem die Arbeit der UNGA und des DISEC bei Themen mit Abrüstungsbezug inhaltlich und organisatorisch. UNODA hat das Sekretariat der GGE's gestellt und auch organisatorische Unterstützung für die OEWG geleistet. Es unterstützt UNIDIR finanziell und hat den vom UNOCT koordinierten UN Global Counter-Terrorism Coordination Compact unterzeichnet. UNODA arbeitet mit Interpol zusammen. Das AA unterstützt ausgewählte UNODA-Projekte und Trust Funds finanziell¹⁰.



Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC)

Das UNODC hat es sich zur Aufgabe gemacht, Bedrohungen auf der Basis von transnational organisierter Kriminalität, Korruption, Terrorismus sowie Drogenhandel und -nutzung durch praktische Unterstützung und die Förderung grenzüberschreitenden Handelns weltweit zu bekämpfen. Im Kontext der Verbrechensbekämpfung hat sich das UNODC auch dem Kampf gegen Cyberkriminalität verschrieben. Hierzu möchte es unter anderem Beiträge zu Bewusstseins- und Kapazitätsaufbau, dem Aufbau nationaler Strukturen und Strafrechtssysteme sowie der internationalen Zusammenarbeit leisten. In der Umsetzung und Operationalisierung seiner Vorhaben wird UNODC's Engagement durch das „Global Programme on Cybercrime“ unterstützt. In der Vergangenheit stellten UN-Mitgliedsstaaten in Zentralamerika, Nord- und Ostafrika, Nahost sowie Südostasien und der Pazifik geografische Schwerpunkte des Programms dar. Die in den letzten Jahren im jährlichen Rhythmus zusammenkom-

¹⁰ [Auswärtiges Amt, Jahresabrüstungsbericht 2020.](#)
[Cybersecurity Tech Accord, Cybersecurity Tech Accord announces new contest in partnership with the UN Office of Disarmament Affairs.](#)
[United Nations Office for Disarmament Affairs, About Us.](#)
[United Nations Office for Disarmament Affairs, Cyberdiplomacy.](#)
[United Nations Office for Disarmament Affairs, Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.](#)



mende „Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime“ (IEG) ist mit der Erarbeitung einer umfassenden Studie zu Cyberkriminalität beauftragt. Deren Ausführungen sollen unter anderem dazu beitragen, die Stärkung bestehender oder Etablierung neuer nationaler, internationaler oder sonstiger Reaktionsmöglichkeiten zu prüfen. Neben der IEG agiert UNODC zudem als Sekretariat des UN-Ad-hoc-Komitees zur Ausarbeitung einer internationalen Konvention zur Bekämpfung der kriminellen Nutzung von IKT. UNODC stellt darüber hinaus ein online zugängliches „Cybercrime Repository“ zur Verfügung, welches Datenbanken zu relevanten Rechtsfällen, Gesetzgebung sowie Lessons Learned enthält.

UNODC ist Teil des UN-Sekretariats und die CCPCJ des ECOSOC ist sein Lenkungsgremium. Mit der ITU besteht eine Kooperationsvereinbarung im Bereich Cyberkriminalität und UNODC ist zudem Partner von ITU's GCI. UNODC ist an dem DTN, der UNGIS sowie der UNISSIG beteiligt und hat den vom UNOCT koordinierten UN Global Counter-Terrorism Coordination Compact unterzeichnet. Das Ad-hoc Komitee ist ein Unterorgan der UNGA. UNODC arbeitet mit Interpol zusammen. An Treffen der IEG haben von deutscher Seite bisher Vertreter:innen des AA, BKA, BMI, BMJ, sowie des ZKA in unterschiedlicher Zusammenstellung teilgenommen. Das BMJ hat für Deutschland einen Entwurf der „Comprehensive Study on Cybercrime“ kommentiert. Deutschland zählt zu den größten Beitragsstaaten zu UNODC's Budget, welcher – mindestens in Teilen – aus dem Haushalt des AA finanziert wird¹¹.



Entwicklungsprogramm der Vereinten Nationen (UNDP)

Das UNDP arbeitet in 170 Ländern zu nachhaltiger Entwicklung, demokratischer Regierungsführung und Friedenskonsolidierung sowie der Resilienz gegenüber dem Klima und Katastrophen. UNDP fördert Länder beispielsweise bei dem Aufbau von institutionellen Fähigkeiten sowie der Entwicklung politischer Richtlinien mit dem

¹¹ [Bundesministerium der Finanzen, Bundeshaushaltsplan 2021 Einzelplan 05: Auswärtiges Amt. Commission on Crime Prevention and Criminal Justice \(Resolution 26/4\), Strengthening international cooperation to combat cybercrime.](#)
[Federal Ministry of Justice and Consumer Protection, German Comments on the Comprehensive Study on Cybercrime.](#)
[United Nations General Assembly, Subsidiary organs of the General Assembly.](#)
[United Nations Office on Drugs and Crime, About UNODC.](#)
[United Nations Office on Drugs and Crime, Ad hoc committee established by General Assembly resolution 74/247.](#)
[United Nations Office on Drugs and Crime, Cybercrime.](#)
[United Nations Office on Drugs and Crime, Cybercrime Repository.](#)
[United Nations Office on Drugs and Crime, Expert Group to Conduct a Comprehensive Study on Cybercrime Vienna \(6–8 April 2021\): List of Participants.](#)
[United Nations Office on Drugs and Crime, Expert Group to Conduct a Comprehensive Study on Cybercrime Vienna \(27–29 March 2019\): List of Participants.](#)
[United Nations Office on Drugs and Crime, Expert Group to Conduct a Comprehensive Study on Cybercrime Vienna \(25–28 February 2013\): List of Participants.](#)
[United Nations Office on Drugs and Crime, Global Programme on Cybercrime.](#)
[United Nations Office on Drugs and Crime, List of pledges, 1 January–31 December 2018.](#)
[United Nations Office on Drugs and Crime, Open-ended Intergovernmental Expert Group Meeting on Cybercrime.](#)



übergeordneten Ziel, zur Verringerung von Armut und Ungleichheit beizutragen. Auf Anfrage bietet UNDP Entwicklungsländern auch Unterstützung im Bereich der Cybersicherheit an. Diese beinhaltet Schulungen und weitere Leistungen in den Bereichen Risikobewertung und -minderung, Resilienz sowie von Richtlinien, Standards und Zertifizierung. Darüber hinaus kann UNDP bei dem Aufbau von lokalen Kapazitäten, Fähigkeiten und Verfahren helfen, die bei der Reaktion auf Cybervorfälle notwendig werden. Gemeinsam mit FIRST richtet UNDP eine jährliche „Cybersecurity for Developing Nations“-Konferenz aus.

UNDP berichtet über den ECOSOC an die UNGA. Ein:e UNDP-Vertreter:in gehört dem UNICRI-Kuratorium an. UNDP ist an dem DTN, der UNGIS sowie der UNISSIG beteiligt und hat den vom UNOCT koordinierten UN Global Counter-Terrorism Coordination Compact unterzeichnet. Es zählt zudem zu den Nutzer:innen der Common Secure Threat Intelligences des UNICC. UNDP ist bei FIRST involviert und von Seiten der ISO als mit ihr kooperierende Organisation gelistet. Deutschland ist Mitglied im UNDP Executive Board und größter Beitragszahler zum UNDP-Budget, welcher aus dem Haushalt des BMZ stammt¹².



Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE)

Die GGE's sind temporär zusammenkommende Arbeitsgruppen von ausgewählten nationalen Regierungsexpert:innen, die unter anderem die Art und Weise der Anwendbarkeit des Völkerrechts auf die Nutzung von IKT, Normen für verantwortungsvolles Staatsverhalten im Cyberraum, vertrauensbildende Maßnahmen sowie Kapazitätsaufbau diskutieren. Im Laufe der Jahre ist die Mitgliedschaft, die sich paritätisch aus den UN-Regionalgruppen zusammensetzt, von 15 auf 25 Mitglieder angewachsen. Seit 2004 haben insgesamt sechs Gruppen von Regierungsexpert:innen getagt, wovon sich vier auf einen Abschlussbericht einigen konnten. In ihrem Bericht aus 2013 bestätigte die Gruppe die Anwendbarkeit des Völkerrechts auf den Cyberraum und der folgende Bericht aus 2015 stellte einen Katalog von elf freiwilligen und nicht-verbindlichen Verhaltensnormen auf, die das Verhalten von Staaten leiten sollen. Diese beinhalten unter anderem den Respekt für Menschenrechte und Privatsphäre, die Meldung von Schwachstellen, den Verzicht auf Operationen auf kritische Infrastrukturen sowie CERTs und den Missbrauch von IKT. Derzeit liegt kein Entwurf für die Einsetzung einer neuen GGE vor.

¹² [Auswärtiges Amt, ABC der Vereinten Nationen.](#)
[Bundesministerium der Finanzen, Bundeshaushaltsplan 2021 Einzelplan 23: Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung.](#)
[Paul Raines, UNDP Cybersecurity Assistance for Developing Nations.](#)
[United Nations Development Programme, About us.](#)
[United Nations Development Programme, Members of the Executive Board.](#)
[United Nations Development Programme, Top Contributors.](#)
[United Nations Development Programme, UNDP and FIRST to host third annual Cybersecurity for Developing Nations Conference.](#)



Die Einrichtung der GGE's wurde durch das **UNGA DISEC** beauftragt. Die Gruppen wurden inhaltlich durch **UNODA** unterstützt, welches auch das Sekretariat gestellt hat. Mitarbeiter:innen von **UNIDIR** haben die GGE in der Vergangenheit gebrieft. Die letzte GGE hat im Rahmen der **HWPCI** auch eine regionale Konsultation mit EU-Mitgliedsstaaten geführt. Deutschland war Teil aller bisher sechs GGE's und wurde durch Vertreter:innen des **AA** repräsentiert. Ein Vertreter des AA hatte den Vorsitz der Gruppe in 2016/2017 inne¹³.



Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen (UNDESA)

Die zum UN-Sekretariat gehörende Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten arbeitet in den Bereichen Analyse, Kapazitätsaufbau sowie der Normensetzung mit dem Ziel, UN-Mitgliedstaaten bei der Zielerreichung in wirtschaftlichen, sozialen und ökologischen Angelegenheiten zu unterstützen. UNDESA verfügt auch über eine Abteilung für „Public Institutions and Digital Government“ (DPIDG), der wiederum eine „Digital Government Branch“ (DGB) unterstellt ist. Der Leiter UN DESA's betrachtet politische und rechtliche Rahmenbedingungen für Datenschutz und Cybersicherheit als eines von 10 identifizierten Schlüsselementen zur nachhaltigen und widerstandsfähigen Erholung von der COVID-19-Pandemie. Alle zwei Jahre gibt UNDESA eine Studie und Rangliste zum Stand des E-Government aller UN-Mitgliedstaaten heraus. Hierbei stellt unter anderem das Vorhandensein von Gesetzen zur digitalen und Cybersicherheit einen Indikator dar.

UNDESA ist Teil des UN-Sekretariats unterstützt unter anderem Befassungen von **UNGA-** sowie **ECOSOC-Gremien**. Eine der DGB untergeordnete Einheit stellt das Sekretariat des **IGFs**. UNDESA arbeitet mit der **ITU** im Bereich der Cybersicherheit zusammen und unterstützt die Erstellung des **GCI**. Sie ist in beobachtender Funktion mit dem von **UNOCT** koordinierten **UN Global Counter-Terrorism Coordination Compact** assoziiert¹⁴.

13 [Matthias Kettemann & Alexandra Paulus, Ein Update für das Internet, Reform der globalen digitalen Zusammenarbeit 2021.](#)

[United Nations General Assembly \(A/70/174\), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.](#)

[United Nations Office for Disarmament Affairs, Advance Copy: Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.](#)

[United Nations Office for Disarmament Affairs, Factsheet: Developments in the Field of Information and Telecommunications in the Context of International Security.](#)

[United Nations Office for Disarmament Affairs, Group of Governmental Experts.](#)

[United Nations Office for Disarmament Affairs, Joint Contribution: The future of discussions on ICTs and cyberspace at the UN.](#)

[United Nations Office for Disarmament Affairs, Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. \(Webseite entfernt\)](#)

[United Nations Office for Disarmament Affairs, The UN GGEs on ICTs and International Security. \(Webseite entfernt\)](#)

14 [Division for Public Institutions and Digital Government, Digital Government.](#)

[Division for Public Institutions and Digital Government, Organisational Chart.](#)

[Elliott Harris, Ten Key Elements for Accelerating Digital Transformation for Sustainable and Resilient Recovery from COVID-19.](#)

[GIP Digital Watch, United Nations Department of Economic and Social Affairs.](#)

[United Nations Department of Economic and Social Affairs, UN E-Government Surveys.](#)



Internationale Fernmeldeunion (ITU)

Die ITU ist als UN-Sonderorganisation für Informations- und Kommunikationstechnologien zuständig. Sie entwickelt unter anderem technische Standards für den IKT-Sektor, auf denen das globale Telekommunikationssystem und der Großteil aller Internetverbindungen basiert, und vermittelt deren globale Annahme. Sie ist zudem bestrebt, Hürden, die dem Zugang zu und der Nutzung von IKT entgegenstehen, beispielsweise durch technologischen Wissenstransfer, weltweit abzubauen. Neben Staaten arbeitet die ITU hierzu auch mit Akteuren aus der Privatwirtschaft zusammen. Cybersicherheit stellt dabei eine thematische Priorität der ITU dar. Die ITU hat eine Handreichung zur Entwicklung einer nationalen Cybersicherheitsstrategie herausgegeben und betreibt zudem ein entsprechendes Repository von bereits verabschiedeten Strategien. Darüber hinaus unterstützt die ITU UN-Mitgliedstaaten bei der Einrichtung von Computer Incident Response Teams. Jährlich organisiert die ITU regionale sowie eine globale Cybersicherheitsübung („CyberDrill“), durch die Kapazitäten, Reaktionsfähigkeiten und regionale Kooperation gefördert werden sollen. Regelmäßig gibt die ITU einen Global Cybersecurity Index (GCI) heraus, der Länder-Engagement im Bereich der Cybersicherheit anhand von rechtlichen, technischen und organisatorischen Indikatoren sowie Kapazitätsentwicklung und Kooperation misst.

ITU ist eine autonome UN-Sonderorganisation, deren Arbeit durch den ECOSOC und den UNSCEB koordiniert wird. UNCTAD und das CCDCOE waren als Partner an der Entwicklung der Handreichung beteiligt. Als ITU's Partner im Kontext des GCI werden unter anderem UNDESA, UNODC und ECSO aufgeführt. Mit dem UNODC besteht zudem eine Kooperationsvereinbarung für den Bereich der Cyberkriminalität und mit UNDESA arbeitet ITU auch in weiteren Fragen der Cybersicherheit zusammen. Eine weitere Kooperationsvereinbarung besteht zwischen ITU und UNICRI, um den Austausch zu Best Practices zu Cybersicherheit, Missbrauch von Technologien und Cyberkriminalität zu verstärken. Das UNCCT des UNOCT beteiligt sich an CyberDrill. Die ITU ist an dem DTN, der UNGIS sowie der UNISSIG beteiligt. Die ITU kann sich an Treffen der MAG des IGF beteiligen und greift auf Leistungen, inklusive der Common Secure Threat Intelligence, von UNICC zurück. Ein:e ITU-Vertreter:in ist im Governmental Advisory Committee der ICANN repräsentiert. Die ITU gehört zu den Partnern von FIRST. Die ITU kooperiert mit der IEC und der ISO, mit der sie zudem gemeinsam als World Standards Cooperation (WSC) zusammenarbeitet. Die ITU ist Partnerorganisation des JTC 1 und zählt zu den Liaisons des JTC 1/SC 27. Gemeinsam mit der EK arbeitet die ITU an der Harmonisierung der IKT-Politik innerhalb der AKP-Staaten zusammen. Mit der ENISA tauscht sich die ITU unter anderem zu Best Practices aus und greift auf ihr Fachwissen im europäischen Kontext zurück. ETSI's TC Cyber kooperiert mit der ITU und CEN/CENELEC's CEN/CLC/JTC 13 prüft u.a. die Übernahme von



*ITU-Standards. Die ITU ist Mitglied im **SCCG**. Von deutscher Seite führt die ITU das **BMDV** und die **BNetzA** als beteiligte mitgliedstaatliche Einrichtungen auf. Der **BSIKT** befasst sich u. a. auch mit Entwicklungen innerhalb der ITU.¹⁵*



Internet Governance Forum (IGF)

Das jährlich stattfindende Internet Governance Forum versteht sich als Diskussions- und Austauschplattform für verschiedenste Stakeholder aus Regierung, Wirtschaft oder Zivilgesellschaft, um die Entwicklung und Nutzung des Internets sektoren- und interessensübergreifend zu besprechen. Hierdurch soll zu einem Informationsaustausch und gemeinsamen Verständnis zwischen den Akteuren, der Identifikation von aufkommenden Problemen sowie der Verfügbarkeit des Internets in Entwicklungsländern beigetragen werden. Das inhaltliche Programm und der Zeitplan des IGF werden durch eine Multistakeholder Advisory Group (MAG) bestimmt, die sich aus Vertreter:innen nationaler Regierungen, sowie privatwirtschaftlichen, zivilgesellschaftlichen, wissenschaftlichen und technischen Akteuren aus allen Regionalgruppen der UN zusammensetzt. Im Rahmen des IGF finden auch Veranstaltungen und Workshops zu Cybersicherheit statt. Neben dem globalen IGF gibt es auch Initiativen für regional und national stattfindende IGFs (NRIs).

UNDESA** stellt das Sekretariat des IGF. Das Sekretariat des IGF hat sich mit einer Stellungnahme an den **OEWG**-Beratungen beteiligt. Dem MAG gehört derzeit ein:e Vertreter:in der **GIZ** an. Darüber hinaus können sich Vertreter:innen des **BMWK**, der **EK**, der **ITU** sowie der **UNCTAD** an Treffen der MAG beteiligen. Die Bundesregierung zählt zu den größten Beitragszahlern des IGF Trust Funds, welcher – mindestens in Teilen – aus dem Haushalt des **BMWK** bezahlt wird. Die **EK** ist institutioneller Partner des auf europäischer Ebene stattfindenden **European Dialogue on Internet Gover-

15 [International Telecommunication Union, CyberDrills.](#)
[International Telecommunication Union, European Commission / Union.](#)
[International Telecommunication Union, European Cybersecurity Organization.](#)
[International Telecommunication Union, European Union Agency for Network and Information Security.](#)
[International Telecommunication Union, Germany.](#)
[International Telecommunication Union, Global Cybersecurity Index.](#)
[International Telecommunication Union, Guide to developing a national cybersecurity strategy – Strategic engagement in cybersecurity.](#)
[International Telecommunication Union, National CIRT.](#)
[International Telecommunication Union, National Cybersecurity Strategies Repository.](#)
[International Telecommunication Union, Our Vision.](#)
[International Telecommunication Union, UNDESA.](#)
[International Telecommunication Union, UNICRI.](#)
[International Telecommunication Union, UNODC.](#)



nance (EuroDIG). Im Steering Committee des deutschen IGF (IGF-D) sind unter anderem Vertreter:innen des **AA**, **BMI**, **BMDV** und **BMWK** repräsentiert¹⁶.



Konferenz der Vereinten Nationen für Handel und Entwicklung (UNCTAD)

UNCTAD unterstützt auf nationaler, regionaler sowie globaler Ebene Entwicklungsländer unter anderem durch Analysen und technische Zuwendungen bei der Diversifizierung ihrer Wirtschaft, der Verringerung finanzieller Volatilität sowie dem Zugang zu digitalen Technologien, um diese erfolgreich und nach gerechten Maßstäben in das internationale Handels- und Wirtschaftssystem einzubetten und eine nachhaltige Entwicklung in den jeweiligen Ländern zu fördern. UNCTAD stellt einen „Global Cyberlaw Tracker“ zur Verfügung, in dem verabschiedete und bevorstehende nationale Gesetzgebungsvorhaben im Bereich von Cyberkriminalität, E-Transaktionen, Datenschutz und Privatsphäre sowie Verbraucherschutz aller UNCTAD-Mitgliedsstaaten gesammelt werden.

UNCTAD berichtet an die **UNGA** und den **ECOSOC**. UNCTAD ist an dem **DTN**, der **UNGIS** sowie der **UNISSIG** beteiligt. UNCTAD kann sich an Treffen der **MAG** des **IGF** beteiligen. Sie nimmt Leistungen des **UNICC** in Anspruch. UNCTAD war als Partner an der von der **ITU** herausgegebenen Handreichung zur Entwicklung einer nationalen Cybersicherheitsstrategie beteiligt. UNCTAD zählt zu den Partnerorganisationen des **JTC 1** und ist von Seiten der **ISO** als mit ihr kooperierende Organisation gelistet¹⁷.



Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG)

Ähnlich dem Mandat der GGE, diskutieren in der OEWG als UN-Forum Vertreter:innen der UN-Mitgliedstaaten unter anderem über Völkerrecht, Normen, Kapazitätsaufbau sowie vertrauensbildende Maßnahmen in Bezug auf IKT-Entwicklungen, die Auswirkungen für die internationale Sicherheit entfalten können. An der OEWG

16 [Bundesministerium der Finanzen, Bundeshaushaltsplan 2021 Einzelplan 09: Bundesministerium für Wirtschaft und Energie.](#)
[European Dialogue on Internet Governance, About.](#)
[Internet Governance Forum, About IGF FAQs.](#)
[Internet Governance Forum, About the Internet Governance Forum.](#)
[Internet Governance Forum, Cyber.](#)
[Internet Governance Forum, Donors to the IGF Trust Fund.](#)
[Internet Governance Forum, MAG 2021 Members.](#)
[Internet Governance Forum, National IGF Initiatives.](#)
[Internet Governance Forum, Regional IGF Initiatives.](#)
[Internet Governance Forum Deutschland, Über uns.](#)

17 [GIP Digital Watch, United Nations Conference on Trade and Development.](#)
[United Nations Conference on Trade and Development, About UNCTAD.](#)
[United Nations Conference on Trade and Development, Digital Economy Report 2019.](#)
[United Nations Conference on Trade and Development, E-Commerce and Digital Economy Programme: Year In Review 2020.](#)
[United Nations Conference on Trade and Development, Membership of UNCTAD and of the Trade and Development Board.](#)
[United Nations Conference on Trade and Development, Summary of Adoption of E-Commerce Legislation Worldwide.](#)



können sich alle UN-Mitgliedstaaten beteiligen. Zudem sind weitere Stakeholder, wie Vertreter:innen von NGOs, Wissenschaft oder Unternehmen, eingeladen, sich für die Teilnahme an intersessionalen Treffen zu bewerben. Die erste OEWG hat im März 2021 einen Konsensbericht verabschiedet. Statements und Kommentierungen von Berichtsentwürfen durch einige UN-Mitgliedstaaten sind auf der Webseite der OEWG oder via UN Web TV einsehbar. Im Dezember 2020 wurde die Einrichtung einer neuen OEWG für die Jahre 2021-2025 beschlossen, die ihre Tätigkeit nach Abschluss der ersten OEWG aufgenommen hat.

Die beiden OEWG's wurden durch Resolutionen der UNGA eingesetzt. Das Sekretariat des IGF hat sich mit einer Stellungnahme an den OEWG-Beratungen beteiligt. Teilnahmebewerbungen von weiteren Stakeholdern werden durch UNODA verwaltet. UN-IDIR unterstützt die Arbeit der OEWG. Deutschland hat durch Vertreter:innen des AA an Sitzungen der OEWG teilgenommen¹⁸.



Wirtschafts- und Sozialrat der Vereinten Nationen (ECOSOC)

Als eines der UN-Hauptorgane ist der ECOSOC mit „internationale[n] Angelegenheiten auf den Gebieten der Wirtschaft, des Sozialwesens, der Kultur, der Erziehung, der Gesundheit und auf verwandten Gebieten“ betraut. Dem ECOSOC sind einige Einrichtungen, wie beispielsweise die Wirtschaftskommission für Europa der Vereinten Nationen (UNECE) sowie die Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ), unterstellt, die sich im Rahmen ihres Mandates auch mit Themen mit Cybersicherheitsbezug befassen. Innerhalb der UNECE, einer von fünf regionalen UN-Wirtschaftskommissionen, wurde beispielsweise im Rahmen ihrer Arbeitsgruppe 6, die sich mit regulatorischer Zusammenarbeit und Standardisierungspolitik befasst, eine sektorale Initiative zur Cybersicherheit etabliert. Diese Initiative hat sich zum Ziel gesetzt, zum Abbau von Handelshemmnissen sowie der Wettbewerbsförderung durch erhöhte Konvergenz von nationalen technischen Vorschriften und Etablierung eines gemeinsamen Regulierungsrahmen beizutragen. Demgegenüber ist die CCPCJ ein politisches Entscheidungsgremium im Bereich der Verbrechensprävention und Strafjustiz, die sich, neben einer Forumfunktion für Wissens- und Erfahrungsaustausch unterhalb der Mitgliedstaaten, inhaltlich

¹⁸ [GIP Digital Watch, UN GGE and OEWG.](#)

[Regionalzentrum der Vereinten Nationen, Die Charta der Vereinten Nationen.](#)

[Secretariat of the Internet Governance Forum, Submission to the „Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security“.](#)

[United Nations, The United Nations System.](#)

[United Nations Office of Disarmament Affairs, Open-ended Working Group.](#)

[United Nations General Assembly \(A/AC.290/2021/CRP.2\), Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report.](#)

[United Nations General Assembly \(A/AC.290/2021/INF.1\), Opened-ended Working Group on developments in the field of information and telecommunications in the context of international security, Third substantive session \(8–12 March 2021\): List of Participants.](#)

[United Nations General Assembly \(A/RES/75/240\), Resolution adopted by the General Assembly on 31 December 2020: Developments in the field of information and telecommunications in the context of international security.](#)

die Verbesserung (inter)nationaler Maßnahmen zur Kriminalitätsbekämpfung zum Ziel gesetzt hat. Auf Empfehlung der CCPCJ hat der ECOSOC beispielsweise eine Resolution zur Förderung der technischen Hilfe und des Aufbaus von Kapazitäten zur Stärkung von nationalen Maßnahmen sowie internationaler Zusammenarbeit zur Bekämpfung der Cyberkriminalität verabschiedet. Die CCPCJ bereitet den alle fünf Jahre stattfindenden «United Nations Congress on Crime Prevention and Criminal Justice» (UNCPCJ) vor, der auch Cyberkriminalität diskutiert.

Die Mitglieder des ECOSOC werden von der UNGA gewählt. Der ECOSOC kann dem UNSC Auskünfte erteilen und ihn auf Ersuchen unterstützen. Das UNDP berichtet über den ECOSOC an die UNGA. UNIDIR ist im UN-System eine gemeinsame Forschungs- und Ausbildungseinrichtung der UNGA und des ECOSOC. UNDESA unterstützt unter anderem Befassungen von ECOSOC-Gremien. Die CCPCJ agiert als Lenkungsgremium des UNODC und hat die Errichtung der IEG Cybercrime beschlossen. Die UNCTAD berichtet unter anderem an den ECOSOC. Die UNECE nimmt Leistungen des UNICC in Anspruch und ist an dem DTN sowie der UNGIS beteiligt. Zudem ist die UNECE eine Partnerorganisation des JTC 1 und von Seiten der ISO als mit ihr kooperierende Organisation gelistet. Mit dem JTC 1/SC 27 hat es in der Vergangenheit beispielsweise zu geschlechtsspezifischer Normentwicklung für den Bereich der Cybersicherheit zusammengearbeitet. Deutschland ist Mitglied des ECOSOC (bis 2023) sowie der CCPCJ (ebenso bis 2023). An Sitzungen der CCPCJ haben in der Vergangenheit unter anderem Vertreter:innen des AA und BMJ teilgenommen. Ein:e Vertreter:in der Physikalisch-Technischen Bundesanstalt, die zum Geschäftsbereich des BMWK gehört, hat den Vorsitz der Arbeitsgruppe 6 der UNECE inne¹⁹.



UN-Generalversammlung (UNGA)

Die UN-Generalversammlung ist das „politische Hauptorgan der [UN] mit allumfassender Zuständigkeit“, deren Resolutionen – außer in Haushaltsfragen – keine rechtlich bindende Wirkung entfalten. Im Plenum tagt die UNGA bei einer jährlich im Herbst stattfindenden Sitzungsperiode. Der UNGA unterstehen zudem unter anderem sechs Komitees, die sich beispielsweise mit Abrüstung und internationaler Sicherheit (First Committee, DISEC), wirtschaftlichen und finanziellen Fragen

¹⁹ Physikalisch-Technische Bundesanstalt, 9.3: Personal. (Webseite entfernt)
[United Nations Economic and Social Council \(E/CN.15/2021/INF/2\), Commission on Crime Prevention and Criminal Justice Thirtieth session Vienna \(17–21 May 2021\): List of Participants.](#)
[United Nations Economic and Social Council, Members.](#)
[United Nations Economic and Social Council \(ECE/CTCS/WP.6/2019/9\), Report on the sectoral initiative on cyber security.](#)
[United Nations Economic and Social Council \(E/RES/2019/19\), Resolution adopted by the Economic and Social Council on 23 July 2019.](#)
[United Nations Economic Commission for Europe, Cybersecurity.](#)
[United Nations Economic Commission for Europe, Governance and organizational structure.](#)
[United Nations Office on Drugs and Crime, Commission on Crime Prevention and Criminal Justice.](#)
[United Nations Office on Drugs and Crime, Members of the Commission on Crime Prevention and Criminal Justice as of 1 January 2021.](#)



(Second Committee, ECOFIN) oder sozialen, humanitären und kulturellen Themen (Third Committee, SOCHUM) auseinandersetzen. Im Rahmen der UNGA wurde sich in der UN erstmals Ende der 1990er-Jahre mit dem Thema Cybersicherheit befasst, welche die Einberufung der ersten GGE zur Folge hatte. Zudem legt der UN-Generalsekretär der UNGA seitdem einen jährlichen Bericht zu „Developments in the field of information and telecommunications in the context of international security“ vor.

Die UNGA wählt unter anderem die nicht-ständigen Mitglieder des UNSC sowie die Mitglieder des ECOSOC. Sie kann gegenüber dem UNSC Empfehlungen aussprechen und ihn auf möglicherweise die internationale Sicherheit gefährdende Situationen aufmerksam machen. Es bestimmt alle zwei Jahre die Prioritätensetzung des UNOCT. UNODA unterstützt die Arbeit der UNGA und des DISEC bei Themen mit Abrüstungsbezug inhaltlich und organisatorisch. Die UNCTAD berichtet an die UNGA. Die GGE und OEWG finden bzw. haben im Rahmen des DISEC stattgefunden. Das Ad-hoc Komitee zur Ausarbeitung einer internationalen Konvention zur Bekämpfung der kriminellen Nutzung von IKT, für das das UNODC als Sekretariat fungiert, ist ein Unterorgan der UNGA. UNIDIR als auch UNITAR sind im UN-System gemeinsame Forschungs- und Ausbildungseinrichtungen der UNGA und des ECOSOC. UNODA unterstützt unter anderem die Arbeit der UNGA und des DISEC bei Themen mit Abrüstungsbezug inhaltlich und organisatorisch und auch UNDESA kann Befassungen von UNGA-Gremien unterstützen²⁰.



UN-Institut für Abrüstungsforschung (UNIDIR)

Das unabhängige UN-Institut für Abrüstungsforschung befasst sich innerhalb der UN mit der Erforschung von Abrüstung und weiteren relevanten Fragestellungen im Kontext internationaler Sicherheitspolitik. Hierzu möchte es mit UN-Mitgliedstaaten in einen Dialog treten, Vertreter:innen unterschiedlicher Sektoren zusammenbringen, sowie Ideen einbringen und praktische Maßnahmen vorantreiben. Zudem steht es auch als beratender Akteur für UN-Mitgliedstaaten, UN-Einrichtungen als auch weiteren Partnern zur Verfügung. Der Bereich der Cybersicherheit wird von UNIDIR's Security and Technology Programme (SecTec) abgedeckt, in welchem Cyberstabilität eines der vier Fokusthemen darstellt. Das SecTec hat mit dem Cyber Policy Portal eine online verfügbare Ressource für Einblicke in die Cybersicherheitslandschaft aller UN-Mitgliedstaaten sowie einzelner Regionalorganisationen geschaffen und veranstaltet zudem regelmäßige Workshops sowie eine jährliche Cyber Stability Konferenz.

²⁰ [Auswärtiges Amt, ABC der Vereinten Nationen.](#)
[Regionalzentrum der Vereinten Nationen, Die Charta der Vereinten Nationen.](#)
[United Nations, First Committee Approves 15 Draft Resolutions, Decisions on Disarmament Measures, Including 2 Following Different Paths towards Keeping Cyberspace Safe.](#)
[United Nations, The United Nations System.](#)
[United Nations General Assembly, Functions and powers of the General Assembly.](#)
[United Nations General Assembly \(A/74/120\), Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General.](#)
[United Nations Office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security.](#)



UNIDIR ist im UN-System eine gemeinsame Forschungs- und Ausbildungseinrichtung der UNGA und des ECOSOC. UNIDIR hat die beiden Vorsitzenden der GGE und OEWG bei der Erfüllung ihrer Aufgaben unterstützt. Es hat den von dem UNOCT koordinierten UN Global Counter-Terrorism Coordination Compact unterzeichnet. Finanziell wird UNIDIR unter anderem durch Beiträge aus Deutschland, der EU und UNODA unterstützt. In der Vergangenheit hat das JTC 1/SC 27 u.a. mit auch mit UNIDIR zu geschlechtsspezifischer Normentwicklung für den Bereich der Cybersicherheit zusammengearbeitet. Das AA hat eine gemeinsame Veranstaltung mit Cyberbezug gemeinsam mit UNIDIR ausgerichtet sowie entsprechende thematische UNIDIR-Konferenzen finanziell unterstützt²¹.



UN-Institut für interregionale Kriminalitäts- und Justizforschung (UNICRI)

UNICRI sieht seine Aufgabe in der Unterstützung von UN-Mitgliedstaaten und der internationalen Gemeinschaft bei der Bekämpfung von kriminellen Bedrohungen, welche den Frieden und Stabilität, die Einhaltung der Menschenrechte sowie eine nachhaltige Entwicklung gefährden. Mit der Ambition der Förderung von nationaler Eigenverantwortung und institutionellen Fähigkeiten, möchte UNICRI hierzu als Anlaufstelle unter anderem konkret zur Förderung von gerechten Strafrechtssystemen sowie der Einhaltung internationaler Instrumente und Standards beitragen. Unter UNICRI's Prioritäten fallen auch Cybersicherheit sowie der Missbrauch von Technologien. Schwerpunktbereiche UNICRI's stellen hier unter anderem organisierte Kriminalität, Diskriminierung und Rassismus im Cyberraum sowie Cybersicherheit in Robotik, autonomen Systemen und kritischen Infrastrukturen dar. UNICRI verfügt über eine Emerging Crimes Unit, die in diesem Kontext unter anderem an einem Projekt der Weltbank zur Bereitstellung von Tools und Kapazitätsaufbau zur Bekämpfung von Cyberkriminalität für aufstrebende Volkswirtschaften beteiligt ist.

UNICRI ist im UN-System eine Forschungs- und Ausbildungseinrichtung des ECOSOC. UNICRI wird durch ein Kuratorium geleitet, dem von Amts wegen unter anderem auch ein:e Vertreter:in des UNDP angehört. Zwischen der ITU und UNICRI besteht eine Kooperationsvereinbarung mit dem Ziel den Austausch zu Best Practices zu Cybersicherheit, Missbrauch von Technologien und Cyberkriminalität zu verstärken. Gemeinsam mit dem UNCCT des UNOCT hat UNICRI einen Bericht zur böswilligen Nutzung von künstlicher Intelligenz für terroristische Zwecke herausgebracht²².

- 21 [GIP Digital Watch, United Nations Institute for Disarmament Research, United Nations Institute for Disarmament Research, Capturing Technology: Rethinking Arms Control. The Impact of Artificial Intelligence on Cyber Operations.](#)
[United Nations Institute for Disarmament Research, Our Funding.](#)
[United Nations Institute for Disarmament Research, UNIDIR Cyber Policy Portal.](#)
[United Nations Institute for Disarmament Research, The UN, Cyberspace and International Peace and Security.](#)
- 22 [United Nations Interregional Crime and Justice Research Institute, About UNICRI.](#)
[United Nations Interregional Crime and Justice Research Institute, Current and Past Activities.](#)
[United Nations Interregional Crime and Justice Research Institute, Cybersecurity and Technology Misuse.](#)
[United Nations Interregional Crime and Justice Research Institute, Governing Body.](#)



UN-Sicherheitsrat (UNSC)

Innerhalb der UN kommt dem UN-Sicherheitsrat gemäß UN-Charta die Hauptverantwortung für die Aufrechterhaltung internationalen Friedens und Sicherheit zu (Art. 24). Er setzt sich aus fünf ständigen (China, Frankreich, Russland, Vereinigtes Königreich und Vereinigte Staaten) sowie zehn nicht-ständigen Mitgliedern zusammen, die jeweils für eine Dauer von zwei Jahren nach einem geographischen Schlüssel gewählt werden. Auch Cybersicherheit ist mittlerweile Thema von formalen und informalen (sog. „Arria“-Meetings) Befassungen und Debatten des Sicherheitsrates. In der Vergangenheit wurden in diesem Rahmen beispielsweise Cyberoperationen gegen kritische Infrastrukturen, Konfliktprävention, Cyberstabilität und Kapazitätsaufbau diskutiert. Die Arbeit des UNSC wird durch eine Vielzahl von Untergremien und Komitees wie dem United Nations Security Council Counter-Terrorism Committee (CTC) unterstützt, welches wiederum durch das Counter-Terrorism Committee Executive Directorate (CTED) assistiert wird. CTC und CTED widmen sich unter anderem auch der Bekämpfung der Nutzung von IKT zu terroristischen Zwecken.

Deutschland ist regelmäßig als nicht-ständiges Mitglied im UNSC vertreten, zuletzt zwischen 2019 und 2020. Die nicht-ständigen Mitglieder des UNSC werden durch die UNGA gewählt. Der ECOSOC kann dem UNSC Auskünfte erteilen und ihn auf Ersuchen unterstützen. In der Vergangenheit haben sich unter anderem Vertreter:innen der Ständigen Vertretung Deutschlands bei den Vereinten Nationen New York (AA) sowie die dem EAD unterstellte Delegation der Europäischen Union an Debatten zu Cybersicherheit beteiligt. Gemeinsam mit dem UNOCT (und Interpol) hat das CTED ein Compendium bewährter Praktiken zum Schutz Kritischer Infrastrukturen veröffentlicht²³.



United Nations Digital and Technology Network (DTN)

Als interner UN-Mechanismus hat sich das DTN die Förderung der Zusammenarbeit bei Themen mit Digital- oder Technologiebezug sowie einer koordinierten und kollektiven Digitalisierung innerhalb des UN-Systems zur Aufgabe gemacht. Das DTN soll unter anderem Räume für den Austausch von Lessons Learned, aktuellen Prioritäten, Kooperationen bei gemeinsamen Projekten und Evaluierung sowie den Aufbau von Untergruppen zu bestimmten Themen und Technologien ermöglichen. Zu den thematischen Interessen des DTN, in denen es Fortschritte anstrebt, gehören unter anderem auch Informations- und Cybersicherheit. An den Treffen des DTN, die zweimal im Jahr stattfinden, nehmen in der Regel die Chief Information Officers (CIO) der im Koordinierungsgremium der Leiter:innen der UN-Organisationen

²³ [Delegation of the European Union to the United Nations – New York, EU Statement – United Nations Security Council: Arria-formula meeting on Cyber-attacks against critical infrastructure. Permanent Mission of the Federal Republic of Germany to the United Nations, Remarks by Ambassador Jürgen Schulz during the Security Council VTC Arria on Cybersecurity, May 22, 2020.](#)
[Security Council Report, Cybersecurity.](#)
[United Nations Security Council Counter-Terrorism Committee. Counter-Terrorism Committee Executive Directorate, Counter-terrorism in cyberspace: Factsheet.](#)
[United Nations Security Council Counter-Terrorism Committee. Counter-Terrorism Committee Executive Directorate and United Nations Office of Counter-Terrorism, The protection of critical infrastructure against terrorist attacks: Compendium of good practices.](#)



(UNSCEB) vertretenen UN-Organisationen teil, die als Repräsentant:in ihrer Organisation agieren. Das DTN wird durch eine informelle externe Expert:innengruppe unterstützt, die Ratschläge und Empfehlungen abgeben kann. Institutionelle Vorläufer des DTN waren das ICT Network (ICTN) sowie das Information Systems Coordination Committee (ISCC).

*Der:die Leiter:in des **UN OICT** übernimmt die Funktion des:der Co-Vorsitzenden des DTN. Das DTN berichtet an das High-level Committee on Management (HLCM) des UNSCEB. Das DTN kann Empfehlungen der an ihn berichtenden **UNISSIG** annehmen, verändern oder ablehnen. Am DTN sind unter anderem **ITU**, **UNCTAD**, **UNDP**, **UNECE (ECOSOC)** und **UNODC** beteiligt²⁴.*



United Nations Group on the Information Society (UNGIS)

Als ressortübergreifender Zusammenschluss von 31 UN-Organisationen möchte die UNGIS die Umsetzung der Ergebnisdokumente der zwei World Summits on the Information Society in Genf (2003) und Tunis (2005) durch Nutzung von Synergien und Implementierung koordinierter Maßnahmen unterstützen. In beiden Abschlussdokumenten wird unter anderem auch auf die Notwendigkeit einer „global culture of cybersecurity“, die Bekämpfung und Verfolgung von Cyberkriminalität Bezug genommen. UNGIS-Mitglieder sind die im UNSCEB vertretenen UN-Organisationen. Hierdurch soll im Rahmen der Arbeit der UNGIS sichergestellt werden, dass Themen mit IKT-Bezug einen wichtigen Platz auf der UN-Agenda behalten und IKT auch im Entwicklungskontext in das Mandat der UNSCEB-Mitglieder aufgenommen werden. Jährlich kommt die UNGIS zu einem hochrangigen Treffen zusammen. Weitere Events und Treffen finden zudem auf Arbeitsebene statt.

*An der UNGIS sind unter anderem **ITU**, **UNCTAD**, **UNDP**, **UNECE (ECOSOC)** und **UNODC** beteiligt²⁵.*



United Nations Information Security Special Interest Group (UNISSIG)

Als interner UN-Mechanismus hat sich die UNISSIG die Kooperation im Bereich der Informationssicherheit zum Ziel gesetzt und ist bestrebt, zur Verbesserung der Informationssicherheit innerhalb aller Mitgliedsorganisationen beizutragen. Konkret sollen im Rahmen der UNISSIG Risiken durch kontinuierliche und kollektive Bewertungen der aktuellen Gefährdungslage minimiert und ein koordiniertes Informationssicherheitsmanagement für das UN-System geschaffen werden. An den Treffen der UNISSIG, die jährlich stattfinden, nehmen in der Regel die Chief Information Security Officers (CISO) der im UNSCEB vertretenen UN-Organisationen teil.

²⁴ [UN Systems Chief Executives Board for Coordination, Digital and Technology Network.](#)

[UN Systems Chief Executives Board for Coordination, Digital & Technology Network \(DTN\): Terms of Reference.](#)

[UN Systems Chief Executives Board for Coordination, 30th Meeting of the CEB ICT Network.](#)

²⁵ [GIP Digital Watch, United Nations Group on the Information Society.](#)

[United Nations Digital Library, Declaration of Principles. Building the information society: A global challenge in the new millennium.](#)

[United Nations Digital Library, Tunis Agenda for the Information Society.](#)

[United Nations Group on the Information Society, About UNGIS.](#)

[United Nations Group on the Information Society, Members.](#)



Die UNISSIG wurde durch das **DTN** eingesetzt und berichtet an das Netzwerk. An der UNISSIG sind unter anderem **ITU**, **UNCTAD**, **UNDP** und **UNODC** beteiligt²⁶.



United Nations International Computing Centre (UNICC)

UNICC stellt anderen UN-Organisationen als spezialisierte UN-Einheit unter anderem Netzwerkinfrastruktur, zentrale digitale Dienstleistungen und Unterstützung bei Informationssicherheit zur Verfügung. Für den Bereich der Informationssicherheit schließt dies beispielsweise Schwachstellenmanagement, Penetrationstests, Phishing-Simulationen sowie den Betrieb eines Threat Intelligence Netzwerks und Security Operation Centers ein. Das UNICC betreibt zudem die „Common Secure Threat Intelligence“ als Teil ihres Common Secure Information Security Hub, durch die durch UNICC Informationen zu Cyberbedrohungen und entsprechenden Vorfällen, beispielsweise automatisiert über eine Malware Information Sharing Platform, geteilt werden können. Die teilnehmenden Institutionen kommen zu einem jährlichen Treffen zusammen.

Zu UNICC's Kunden und Partnern zählt unter anderem die **ITU**, **UNCTAD**, **UNECE (ECOSOC)**, **UNITAR** und **UN OICT**. Zu den Nutzern der Common Secure Threat Intelligence zählen unter anderem die **ITU**, **UNCTAD** und **UNDP**. UNICC ist bei **FIRST** involviert²⁷.



United Nations Office of Counter-Terrorism (UNOCT)

Zu den Aufgaben des UNOCT zählt unter anderem die Verbesserung der Koordination und Sicherstellung der Kohärenz zwischen den unterzeichnenden Institutionen des UN Global Counter-Terrorism Coordination Compact sowie die Verstärkung der UN-Unterstützung bei nationalen Kapazitätsaufbau im Bereich der Terrorismusbekämpfung. Beim UNOCT ist zudem das UN Counter Terrorism Center (UNCCT) angesiedelt, bei dem Cybersicherheit eines der Programme und Projekte darstellt. Hier möchte das UNCCT die Fähigkeiten von UN-Mitgliedstaaten und privaten Organisationen bei der Eindämmung der missbräuchlichen IKT-Nutzung durch terroristische Akteure stärken, die Bedrohung von Cyberoperationen von diesen auf Kritische Infrastrukturen mindern, sowie auf den sozialen Medien zur menschenrechtskonformen Sammlung digitaler Beweise beitragen.

*UNOCT ist Teil des UN-Sekretariats und seine Prioritäten werden alle zwei Jahre durch die **UNGA** im Rahmen der Überprüfung der UN Global Counter-Terrorism Strategy be-*

²⁶ [UN Systems Chief Executives Board for Coordination, HLCCM ICT Network UN Information Security Special Interest Group \(UNISSIG\): Terms of Reference.](#)

[UN Systems Chief Executives Board for Coordination, Information Security Special Interest Group.](#)

²⁷ [GIP Digital Watch, UN International Computing Centre.](#)

[United Nations International Computing Centre, Clients and Partner Organizations.](#)

[United Nations International Computing Centre, UNICC Facilitates UN Inter-Agency Collaboration with a Reputation for Cyber Excellence.](#)

[United Nations International Computing Centre, What We Do.](#)



stimmt. UNOCT arbeitet unter anderem mit dem CTC als Untergremium des UNSC zusammen. Das UNCCT beteiligt sich an ITU's Cybersicherheitsübung CyberDrill. In der Vergangenheit hat das UNCCT zudem einen Hackathon zur Bekämpfung digitalen Terrorismuses mit dem UN OICT organisiert. Gemeinsam mit dem UNICRI hat das UNCCT einen Bericht zur böswilligen Nutzung von künstlicher Intelligenz für terroristische Zwecke herausgebracht. Zu den unterzeichnenden Organisationen des UN Global Counter-Terrorism Coordination Compact zählen unter anderem UNDP, UNICRI, UNIDIR, UNITAR, UNODA, UNODC und UN OICT. UNDESA ist als Beobachter mit dem Compact assoziiert. UNOCT arbeitet mit Interpol zusammen. Die EU und Deutschland sind unter den führenden 10 Beitragszahlern von UNOCT. Deutschland ist Mitglied des Advisory Board des UNCCT²⁸.



United Nations Office of Information and Communications Technology (UN OICT)

Im Bereich der Cybersicherheit hat sich das UN OICT als zentrale Anlaufstelle für Partner innerhalb der UN zur Aufgabe gemacht, Cyberbedrohungen für die UN zu erkennen, diese zu verhindern und bei Auftreten zu ihrer Schadensbehebung beizutragen. Es hat hierzu beispielsweise ein Informationsrisikomanagement und Richtlinien für das UN-Sekretariat inklusive eines Aktionsplans erstellt. Im UN OICT ist das Digital Blue Helmets Programm (DBH) verortet, welches als Plattform zu schnellem Informationsaustausch, Cyberverteidigung, Erhöhung von Widerstandsfähigkeiten sowie einem koordinierten Einsatz von Schutzmaßnahmen im Falle eines Cybersicherheitsvorfalls beitragen soll. Es setzt sich aus spezialisierten Cybersicherheits-expert:innen zusammen und unterhält unter anderem ein Global Cybersecurity Monitoring Centre in New York sowie regionale Cybersecurity Monitoring Centres. Auf lange Sicht möchte das DBH unter anderem zur Minderung der Auswirkungen von Zero Day-Schwachstellen, der Förderung digitaler IDs sowie dem weiteren Ausbau der Abwehrkapazitäten der UN gegenüber externen Bedrohungen beitragen

Der:die Leiter:in des UN OICT übernimmt die Funktion des:der Co-Vorsitzenden des DTN. In der Vergangenheit hat das UN OICT mit dem UNCCT des UNOCT einen Hackathon zur Bekämpfung digitalen Terrorismuses organisiert. Es zählt zu den Kunden und Partnern des UNICC²⁹.

28 [AIT Austrian Institute of Technology, United Nations Counter-Terrorism Centre führte Cybersecurity Innovation Challenge am AIT.](#)

[United Nations Interregional Crime and Justice Research Institute, Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes.](#)

[United Nations Office of Counter-Terrorism, About us.](#)

[United Nations Office of Counter-Terrorism, Advisory Board.](#)

[United Nations Office of Counter-Terrorism, Funding and donors.](#)

[United Nations Office of Counter-Terrorism, UN Global Counter-Terrorism Coordination Compact Entities.](#)

[United Nations Office of Counter-Terrorism, UN Counter-Terrorism Centre, Cybersecurity.](#)

[United Nations Office of Counter-Terrorism, UN Counter-Terrorism Centre, UNCCT-ITU Cyber Drill 2020 – Terrorist Threat Simulation Cyber Exercise.](#)

29 [Office of Information and Communications Technology, About OICT.](#)

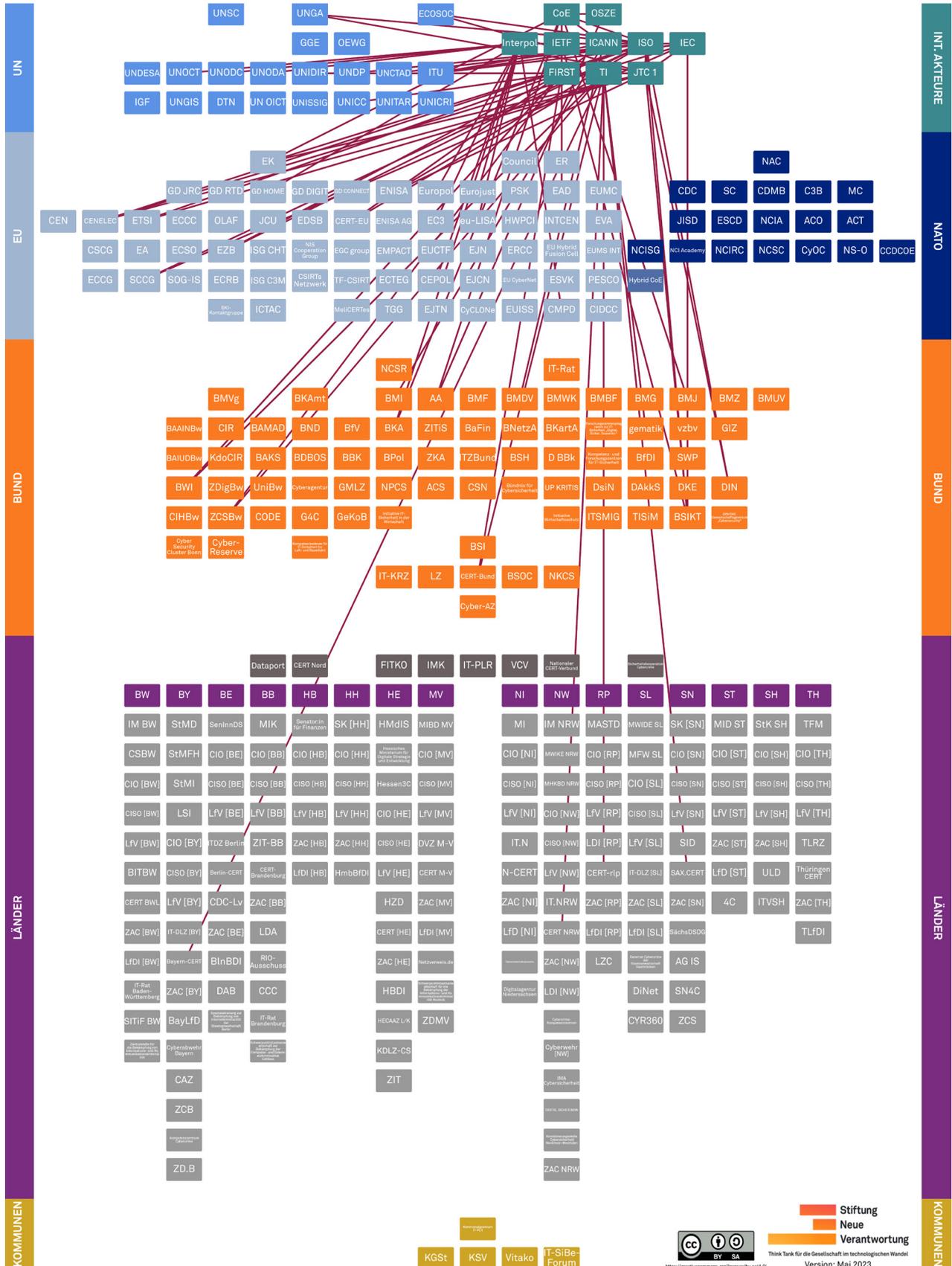
[Office of Information and Communications Technology, Coordination.](#)

[Office of Information and Communications Technology, Cybersecurity.](#)

[Office of Information and Communications Technology, Digital Blue Helmets.](#)



5. Erläuterung – Weitere internationale Akteure





Policy-Überblick

* seit Mai 2022 offen für Unterzeichnungen von Staaten, noch nicht in Kraft getreten.

Jahr	Akteur	Name
2022*	CoE	<u>Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence</u>
2016	OSZE	<u>OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies</u>
2013	OSZE	<u>Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies</u>
2006	CoE	<u>Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art</u>
2004	CoE	<u>Übereinkommen über Computerkriminalität („Budapest-Konvention“)</u>



Europarat (CoE)

Im Rahmen der zwischenstaatlichen Organisation des Europarates wurde u.a. ein Übereinkommen über Computerkriminalität, die sogenannte Budapest-Konvention, getroffen. Die Umsetzung des Übereinkommens sowie die Prüfung möglicher Abänderungen und die Zusammenarbeit der Vertragsparteien wird durch ein Cybercrime Convention Committee (T-CY) unterstützt. In der CoE-Organisationsstruktur verantwortet das Information Society and Action against Crime Directorate neben weiteren Schwerpunkten das Thema Cyberkriminalität. Zur Umsetzung der Budapest-Konvention gibt der CoE zudem verschiedene Berichte und Leitfäden, wie beispielsweise zur Zusammenarbeit zwischen Strafverfolgungsbehörden und Internet Service Providern, heraus. In Bukarest hat das CoE ein Cybercrime Programme Office (C-PROC) eingerichtet, welches Projekte zum Kapazitätsaufbau im Bereich der Ermittlung, Verfolgung und Verurteilung von Cyberkriminalität auf Basis der Vorgaben der Budapest-Konvention organisiert. Der CoE stellt auch ein Informationsportal, die sogenannte Octopus Community, in dem thematische Ressourcen, wie beispielsweise Länderprofile, zur Verfügung gestellt werden. Alle ein bis zwei Jahre organisiert der Europarat mit der Octopus Conference eine Konferenz, die sich mit der Bekämpfung von Cyberkriminalität befasst. Gemeinsam mit der EU hat der CoE das GLACY+-Projekt initiiert, welches in bestimmten Fokusländern u.a. deren Fähigkeiten zur Anwendung der Vorschriften der Budapest-Konvention sowie die internationale Zusammenarbeit stärken soll.

Deutschland ist Mitglied des CoE und hat die Budapest-Konvention ratifiziert. Der:die deutsche Außenminister:in bzw. der:die Leiter:in der Ständigen Vertretung Deutschlands beim Europarat (AA) vertritt Deutschland im CoE-Ministerkomitee. Das AA



kommt auch für im Rahmen der Budapest-Konvention ersuchter Rechtshilfe oder Auslieferungen durch andere Vertragsparteien die Funktion als Ansprechpartner zu. Dem **BKA** kommt die in der Budapest-Konvention vorgesehene Rolle als 24/7-verfügbare Kontaktstelle zu. Von deutscher Seite nehmen Vertreter:innen des **BMJ** an Treffen des T-CY teil. Der **EAD** entsendet eine Delegation zum CoE und Vertreter:innen der **EK** können auf Einladung an CoE-Treffen von Ministerkomitee bis Arbeitsgruppen teilnehmen. Auch der Europarat unterhält Verbindungsbüros zur EU, der **OSZE** und den Vereinten Nationen. Ein:e CoE-Vertreter:in ist im Governmental Advisory Committee des **ICANN** repräsentiert. Die **ISO** führt den CoE als mit ihr kooperierende Organisation auf³⁰.



Forum of Incident Response and Security Teams (FIRST)

Als Forum und Austauschplattform möchte FIRST auf vertrauensvoller Basis das Teilen von Informationen, beispielsweise zu Schwachstellen und Sicherheitslücken, sowie die Zusammenarbeit zwischen Mitglieder-CERTs stärken, um dadurch das Internet sicherer zu machen und etwaige Schäden nach Vorfällen minimieren zu können.

Aus Deutschland beteiligen sich u.a. **CERT-Bund**, das CERT der **BWI** sowie das CERT der **Bw (ZCSBw)** an FIRST. Von internationaler Seite sind zudem noch das **CERT-EU**, das CERT der **EZB** sowie **UNICC** und **UNDP** involviert. Zu den FIRST-Partnern gehören u.a. die **ITU** sowie die **ICANN**. Unter den FIRST-Liaisons befinden sich u.a. auch Vertreter:innen der **ITU** und der **ENISA**³¹.

- 30 [Europarat, 25th Plenary Meeting of the T-CY 15 November 2021: Meeting report.](#)
[Europarat, Action against Cybercrime.](#)
[Europarat, Co-operation between the Council of Europe and the European Union.](#)
[Europarat, Cybercrime Convention Committee.](#)
[Europarat, Cybercrime Programme Office \(C-PROC\).](#)
[Europarat, Global Action on Cybercrime Extended \(GLACY\)+.](#)
[Europarat, Information Society and Action against Crime Directorate.](#)
[Europarat, Law enforcement – Internet service provider Cooperation.](#)
[Europarat, List of Competent Authorities Set Up in Accordance with Articles 24, 27 and 35 of the Budapest Convention on Cybercrime.](#)
[Europarat, List of external offices.](#)
[Europarat, Octopus Community.](#)
[Europarat, Octopus Conferences.](#)
[Europarat, Reports.](#)
[Europarat, Reservations and Declarations for Treaty No.185 – Convention on Cybercrime \(ETS No. 185\).](#)
[Europarat, T-CY Workplan for the period January 2022 – December 2023.](#)
[Europarat, The Budapest Convention and its Protocols.](#)
- 31 [Forum of Incident Response and Security Teams, About FIRST.](#)
[Forum of Incident Response and Security Teams, FIRST Liaison Members.](#)
[Forum of Incident Response and Security Teams, FIRST Teams.](#)
[Forum of Incident Response and Security Teams, FIRST Vision and Mission Statement.](#)
[Forum of Incident Response and Security Teams, Partners.](#)



Internationale Elektrotechnische Kommission (IEC)

Als Normungsorganisation arbeitet die IEC an der internationalen Standardisierung in den Bereichen elektrischer und elektronischer Technologien. Im Bereich der Cybersicherheit orientiert sich die IEC an einem ganzheitlichen Ansatz, der sich aus den Komponenten Menschen, Prozesse und Technologien zusammensetzt, um Cyberresilienz aufzubauen. Die entsprechenden Vorschriften können dabei entweder technologieunabhängig und flexibel, sog. horizontale Standards, oder spezifisch für bestimmte technische Anwendungsbereiche, sog. vertikale Standards, erarbeitet werden. Als horizontale Standards im Bereich der Cybersicherheit ist beispielsweise die Normenreihe IEC 62443 zu nennen, die sich mit der Cybersicherheit von industriellen Automatisierungs- und Steuerungssystemen befasst.

IEC, ISO und die ITU arbeiten gemeinsam als World Standards Cooperation (WSC) zusammen. Gemeinsam mit dem ISO hat die IEC das JTC 1 etabliert. Auf europäischer Ebene kooperiert zudem mit der CENELEC. Deutsches Mitglied in der IEC ist die DKE. Die IEC wiederum ist Mitglied der SCCG. Der BSIKT befasst sich u.a. auch mit Entwicklungen innerhalb der IEC³².



Internationale Kriminalpolizeiliche Organisation (Interpol)

Interpol unterstützt seine Mitgliedsstaaten bei der Durchführung sowie Koordinierung grenzüberschreitender Ermittlungen und Operationen zur Bekämpfung von Cyberkriminalität oder übernimmt partiell auch die Leitung von letzteren in der Form von sogenannten *Cyber Surges*. Zu diesen Zwecken sind bei Interpol ein Cyber Fusion Centre (CFC) angesiedelt und mit dem Cybercrime Knowledge Exchange Workspace (CKE) sowie dem Cybercrime Collaborative Platform – Operation (CCP-Operation) bestehen zwei relevante Kommunikations- und Kollaborationsplattformen. Im CFC werden Informationen von Strafverfolgungsbehörden sowie dem Privatsektor zusammengetragen und analysiert, die darauf aufbauend als Berichte an etwaig bedrohte Staaten weitergegeben werden. Gegenüber der CCP-Operation werden innerhalb des als Netzwerk angedachten CKE lediglich nicht-polizeiliche fachliche Informationen, beispielsweise zu Trends oder Prävention, zwischen autorisierten Mitgliedern, die sich neben Vertreter:innen von Strafverfolgungsbehörden auch aus Regierungen, internationalen Organisationen sowie weiteren Fachexpert:innen zusammensetzen können, ausgetauscht. Die CCP-Operation ermöglicht darüber hinaus die aktive Koordinierung von weltweiten Maßnahmen im Bereich der Strafver-

³² [Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung.](#)
[Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Frankfurt Agreement stärkt Zusammenarbeit zwischen IEC und CENELEC.](#)
[Internationale Elektrotechnische Kommission, Cyber security \[1\].](#)
[Internationale Elektrotechnische Kommission, Cyber security \[2\].](#)
[Internationale Elektrotechnische Kommission, National Committees.](#)
[Internationale Elektrotechnische Kommission, Frequently asked questions.](#)



folgung zur Bekämpfung von Cyberkriminalität durch Informationsaustausch und Ressourcenpooling zwischen operativen Ansprechpartnern. Interpol beteiligt sich am entsprechenden Kapazitätsaufbau in seinen Mitgliedsländern und stellt mit der Digital Security Challenge auch ein Übungsformat für Cyberermittler:innen zur Verfügung. Interpol hat zudem einen Leitfaden zur Erstellung bzw. Überarbeitung einer nationalen Cyberkriminalitätsstrategie herausgegeben.

*Für Deutschland übernimmt das **BKA** die Funktionen als Nationales Zentralbüro. Auf EU-Ebene kooperiert Interpol u.a. mit **Europol**, **Eurojust**, **CEPOL**, **eu-LISA**, dem **CMPD** und **GD HOME**. Jährlich richten Europol (durch das **EC3**) und Interpol eine gemeinsame Konferenz zur Cyberkriminalität aus. Darüber hinaus bestehen auf UN-Ebene u.a. Kooperationen mit **UNODC**, **UNODA** und **UNOCT**. Interpol-Vertreter:innen sind im Governmental Advisory Committee der **ICANN** repräsentiert und Interpol ist von Seiten der **ISO** als mit ihr kooperierende Organisation gelistet³³.*



Internationale Organisation für Normung (ISO)

Mit themenübergreifendem Mandat erarbeitet die ISO als Normungsorganisation internationale Standards für verschiedenste Bereiche (außer Elektrik, Elektronik und Telekommunikation). Zu ISO-Standards, die sich mit IT- und Cybersicherheit befassen, gehören beispielsweise die mit dem IEC abgestimmte „27000-Familie“ oder der ISO/SAE 21434-Standard, welcher technische Anforderungen für die Cybersicherheit von elektrischen oder elektronischen Systemen innerhalb von Automobilfahrzeugen adressiert.

*Deutsches Mitglied der ISO ist das **DIN**. Die ISO kooperiert mit der **IEC** und der **ITU**, gemeinsam arbeiten diese zudem als World Standards Cooperation (WSC) zusammen. Gemeinsam mit dem IEC hat das ISO das **JTC 1** etabliert. **ETSI**'s TC CYBER kooperiert mit der ISO und **CENELEC**'s CEN/CLC/JTC 13 prüft u.a. die Übernahme von ISO-Standards. Die ISO ist Mitglied der **SCCG**. Darüber hinaus sind bei der ISO als mit*

³³ [Bundeskriminalamt, Interpol \(IKPO\).](#)

[Internationale Kriminalpolizeiliche Organisation, Cooperation with United Nations entities.](#)

[Internationale Kriminalpolizeiliche Organisation, Cyber capabilities development.](#)

[Internationale Kriminalpolizeiliche Organisation, Cybercrime.](#)

[Internationale Kriminalpolizeiliche Organisation, Cybercrime Collaboration Services.](#)

[Internationale Kriminalpolizeiliche Organisation, Cybercrime threat response.](#)

[Internationale Kriminalpolizeiliche Organisation, Cybercrime operations.](#)

[Internationale Kriminalpolizeiliche Organisation, Germany.](#)

[Internationale Kriminalpolizeiliche Organisation, Innovation to beat cybercrime acceleration the theme of 2021.](#)

[Europol-INTERPOL Cybercrime Conference.](#)

[Internationale Kriminalpolizeiliche Organisation, INTERPOL and the European Union.](#)

[Internationale Kriminalpolizeiliche Organisation, National Cybercrime Strategy Guidebook.](#)



ihr kooperierende Organisationen u.a. die **EK**, die **EZB**, die **ENISA**, der **CoE**, das **ETSI**, die **IETF**, die **ICANN**, **Interpol**, **UNCTAD**, **UNDP** sowie die **UNECE (ECOSOC)** gelistet³⁴.



Internet Corporation for Assigned Names and Numbers (ICANN)

Die ICANN setzt sich für die Sicherheit, Stabilität und Interoperabilität des globalen Internets sowie seine Erweiterung und Entwicklung ein. Hierzu arbeitet sie zu Unique Identifiers und koordiniert das dem Internet zugrunde liegende Domain Name System (DNS). ICANN spricht sich für die vollständige Einführung von Domain Name System Security Extensions (DNSSEC) für alle Domännennamen durch alle Mitglieder des „Domain Name-Ökosystems“ aus, um das Sicherheitsniveau zu erhöhen und die Kommunikation zwischen Endnutzer:innen und Domäne zu schützen. Innerhalb der ICANN-Organisationsstruktur befasst sich das Security and Stability Advisory Committee (SSAC) mit der Sicherheit und Integrität des DNS und berät anhand seiner Analysen und Einschätzungen das ICANN-Direktorium sowie die ICANN-Community. ICANN stellt zudem verschiedene Publikationen zur Verfügung, die sich aus technischer oder politischer Perspektive mit relevanten Themen innerhalb des ICANN-Aufgabenportfolios befassen.

Vetreter:innen des **BMDV** und **BMI** sind für Deutschland Mitglieder des ICANN Governmental Advisory Committee (GAC). Im GAC sind zudem u.a. der **CoE**, **Interpol** sowie die **ITU** durch Vertreter:innen repräsentiert. Ein:e Vertreter:in des **IETF** ist als Liaison am ICANN-Direktorium beteiligt. ICANN gehört zu den Partnern von **FIRST** und ist von Seiten der **ISO** als mit ihr kooperierende Organisation gelistet³⁵.



Internet Engineering Task Force (IETF)

Die IETF hat sich der Entwicklung von freiwilligen technischen Internetstandards zur Verbesserung von dessen Funktionsweise und Sicherheit verschrieben. Innerhalb der IETF-Security Area und in Zusammenarbeit mit weiteren Areas umfasst dies beispielsweise die Sicherstellung hoher Sicherheitsniveaus von IETF-Protokollen. Im Rahmen der Security Area wird in verschiedenen Arbeitsgruppen auch zur Au-

34 [Institut der Wirtschaftsprüfer in Deutschland, CYBERRISK.](#)
[Internationale Organisation für Normung, Cybersecurity in cars.](#)
[Internationale Organisation für Normung, Members.](#)
[Internationale Organisation für Normung, Organizations in cooperation with ISO.](#)
[Internationale Organisation für Normung, Structure and Governance.](#)
[Internationale Organisation für Normung, What we do.](#)
[World Standards Cooperation, Who we are.](#)

35 [Internet Corporation for Assigned Names and Numbers, Board of Directors.](#)
[Internet Corporation for Assigned Names and Numbers, GAC Membership.](#)
[Internet Corporation for Assigned Names and Numbers, Government Engagement Publications.](#)
[Internet Corporation for Assigned Names and Numbers, ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet.](#)
[Internet Corporation for Assigned Names and Numbers, OCTO Publications.](#)
[Internet Corporation for Assigned Names and Numbers, Security and Stability Advisory Committee \(SSAC\).](#)
[Internet Corporation for Assigned Names and Numbers, What Does ICANN Do?.](#)



thentifizierung und Autorisierung gearbeitet. Für politische Entscheidungsträger:innen bietet das IETF auch im Kontext des IETF Policy Programs Schulungen zur Funktionsweise des Internets an.

Ein:e Vertreter:in des IETF ist als Liaison im ICANN-Direktorium beteiligt. Von Seiten der ISO ist die IETF als mit ihr kooperierende Organisation aufgeführt. Der BSIKT befasst sich u.a. auch mit Entwicklungen innerhalb der IETF³⁶.



ISO and IEC Joint Technical Committee (JTC 1)

Das JTC 1 ist thematisch mit der Diskussion und Erarbeitung von Standards im Bereich von Informationstechnologien betraut. Innerhalb des JTC 1 befasst sich das Untergremium 27 (JTC 1/SC 27) mit Informations- und Cybersicherheit sowie dem Schutz der Privatsphäre. Dieses verantwortet beispielsweise die (Weiter-)Entwicklung der horizontalen Standardreihe ISO/IEC 27000.

JTC 1 ist ein gemeinsames technisches Gremium der ISO und der IEC. Für Deutschland beteiligt sich das DIN an dem JTC 1. Das DIN stellt zudem das Sekretariat des ISO/IEC JTC 1/SC 27. Der BSIKT befasst sich u.a. auch mit Entwicklungen innerhalb des JTC 1. Die EK, ENISA, ETSI und die ITU, UNCTAD sowie die UNECE (ECOSOC) sind Partnerorganisation des JTC 1. Das JTC 1/SC 27 unterhält u.a. Liaisons mit dem ETSI sowie der ITU. CENELEC's CEN/CLC/JTC 13 prüft u.a. die Übernahme von Standards, die im JTC 1 entstanden sind. In der Vergangenheit hat das JTC 1/SC 27 auch mit den UN-Organisationen UNECE und UNIDIR zu geschlechtsspezifischer Normentwicklung für den Bereich der Cybersicherheit zusammengearbeitet³⁷.



Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)

Im Bereich der Cyber- und IT-Sicherheit besteht der primäre Fokus der OSZE in der Förderung der Vertrauensbildung zwischen ihren Mitgliedsstaaten zur Prävention und Eindämmung möglicher Konflikte. Die OSZE-Mitgliedsstaaten haben in der Vergangenheit zwei entsprechende Pakete von vertrauensbildenden Maßnahmen (VBM) verabschiedet. Diese beinhalten u.a. einen „zwischenstaatliche[n] Konsultationsmechanismus für mögliche Zwischenfälle“ sowie die Schaffung weiterer inhaltlicher Austauschplattformen. Zu diesen vereinbarten VBM stellt die OSZE auch

³⁶ [Internet Engineering Task Force, Security & privacy.](#)
[Internet Engineering Task Force, Security Area \(sec\).](#)
[Internet Engineering Task Force, Mission and principles.](#)
[Internet Engineering Task Force, Groups.](#)
[Internet Engineering Task Force, Internet standards.](#)
[Internet Society, IETF Policymakers Program.](#)

³⁷ [Internationale Elektrotechnische Kommission, ISO/IEC JTC 1/SC 27.](#)
[Internationale Organisation für Normung, ISO/IEC JTC 1 Participation.](#)
[Internationale Organisation für Normung, Keeping Cybersafe.](#)
[JTC 1, JTC 1/SC 27 celebrates 30 years.](#)
[JTC 1, Partners.](#)



einen E-Learning-Kurs zur Verfügung. Neben dem VBM-Schwerpunkt möchte die OSZE auch allgemein zur „angemessenen und rechtzeitigen Reaktion staatlicher Behörden“ auf Bedrohungen aus dem Cyberraum wie beispielsweise Cyberkriminalität oder der Nutzung des Internets durch nicht-staatliche Akteure, u.a. zu terroristischen Zwecken, hinwirken. Innerhalb der OSZE-Organisationsstruktur verantwortet das Transnational Threats Department IT- und Cybersicherheit, welches auch weitere thematische Aktivitäten wie beispielsweise Übungen zur Reaktion auf Kritische Infrastrukturen abzielende Cyberoperationen oder Workshops organisiert. Jährlich richtet die OSZE eine Cyber/ICT Security Conference aus.

Deutschland ist Mitglied der OSZE und ist vor Ort durch die Vertretung der Bundesrepublik bei der OSZE (AA) repräsentiert. Der CoE unterhält ein Verbindungsbüro zur OSZE³⁸.



Trusted Introducer (TI)

Trusted Introducer möchte als Informationsaustauschplattform zu einer verbesserten Kooperation, Austausch zu Bedrohungssituationen und im Bedarfsfall zu beschleunigten Reaktionsfähigkeiten zwischen CERTs weltweit beitragen. Es stellt hierfür eine entsprechende Infrastruktur zur Verfügung. CERTs können bei TI als gelistete, akkreditierte oder zertifizierte Teams beteiligt sein.

Von deutscher Seite sind das CERT der Bundeswehr (ZCSBw), das CERT der gematik, das Bayern-CERT, das CERT NRW, das CERT-rlp sowie das SAX.CERT als teilnehmende Teams gelistet. Das CERT-Bund ist bei Trusted Introducer akkreditiert und das CERT der BWI zertifiziert. Das CERT-EU ist Zertifizierungskandidat³⁹.

- 38 [Organisation für Sicherheit und Zusammenarbeit in Europa, Cyber/ICT Security. Organisation für Sicherheit und Zusammenarbeit in Europa, Multilateral engagement key to open and secure cyberspace.](#)
[Organisation für Sicherheit und Zusammenarbeit in Europa, New e-learning course on OSCE cyber/ICT security Confidence-Building Measures now available.](#)
[Organisation für Sicherheit und Zusammenarbeit in Europa, Transnational Threats Department: Cyber/ICT Security. Ständige Vertretung der Bundesrepublik Deutschland bei der OSZE, Ständige Vertretung.](#)
- 39 [Trusted Introducer, Processes.](#)
[Trusted Introducer, Services for Security and Incident Response Teams.](#)
[Trusted Introducer, Team Database.](#)



Policy-Überblick

Jahr	Name
2022	Directive on the resilience of critical entities and repealing Council Directive 2008/114/EC (Directive 2022/2557)
2022	Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 („NIS 2 Directive“, Directive 2022/2555)
2022	Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 („Dora“, Regulation 2022/2554)
2022	Joint Communication: EU Policy on Cyber Defence (JOIN 2022/49)
2022	Council conclusions on the development of the European Union's cyber posture
2021	International Strategy of the EU Agency for Cybersecurity
2021	Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (Regulation 2021/887)
2020	Communication from the Commission: Shaping Europe's Digital Future („Digital Strategy“)
2020	EU Cybersecurity Strategy for the Digital Decade Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2017: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU• 2013: EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace
2019	EU Cybersecurity Act (Regulation 2019/881) Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2013: Regulation 526/2013
2019	EU Law Enforcement Emergency Response Protocol for Major Cross-Border Cyber-Attacks (LE ERP) (Europol-Pressemitteilung)
2019	Regulation on ENISA (The European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification And Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Regulation 2019/881)
2018	EU Cyber Defence Policy Framework Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2014: EU Cyber Defence Policy Framework
2018	Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats (JOIN(2018) 16)
2017	Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises („Blueprint“, 2017/1584)



Jahr	Name
2017	Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities („Cyber Diplomacy Toolbox“) Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities
2016	Directive concerning measures for a high common level of security of network and information systems across the Union („NIS Directive“, Directive 2016/1148)
2016	Joint Communication: Joint Framework on Countering Hybrid Threats. A European Union Response („Playbook“, JOIN(2016) 18)
2013	Directive on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Directive 2013/40/EU)



Agentur der Europäischen Union für Cybersicherheit (ENISA)

ENISA⁴⁰ ist eine EU-Agentur zur Unterstützung der Kommission im Bereich Cybersicherheit. Sie trägt in ihrer Beratungsfunktion zur EU-Cyber Policy bei, unterstützt den Kapazitätsaufbau im Bereich der Cybersicherheit, ist an einem Wissensaustausch mit relevanten Stakeholdern beteiligt und macht auf das Thema der Cybersicherheit aufmerksam. ENISA arbeitet außerdem daran, die Kooperation innerhalb der EU zu verbessern, sorgt für Kohärenz sektoraler Initiativen mit der NIS-Richtlinie und unterstützt den Aufbau von Informationsaustausch- und Analysezentren in kritischen Sektoren. ENISA ist außerdem Knotenpunkt für Information und Wissen in der Cybersicherheitscommunity. Um die Widerstandsfähigkeit der EU gegenüber Cybersicherheitsbedrohungen zu verbessern sowie frühzeitig Lösungen und Strategien für sich aus neuen Technologien ergebenden Herausforderungen zu finden, hat sich die ENISA zudem zum Ziel gesetzt, unterschiedliche Akteure mit dem Ziel der Vorausschau (Foresight) zusammenzubringen. Infolge des Inkrafttretens des Rechtsakts zur Cybersicherheit ist sie beauftragt, „europäische Schemata für die Cybersicherheitszertifizierung“ als Grundlage für die Zertifizierung von Produkten, Prozessen und Dienstleistungen zur Unterstützung des digitalen Binnenmarktes zu entwickeln. ENISA koordiniert Maßnahmen der Mitgliedstaaten bezüglich der Prävention und Abwehr von Cyberoperationen. Jährlich veröffentlicht die ENISA einen Bericht zur Bedrohungslage (ENISA Threat Landscape), der Gefahren aus dem Cyberraum identifiziert und bewertet. Darüber hinaus organisiert die ENISA regelmäßige Cybersicherheitsübungen in unterschiedlichen Formaten, wie die alle zwei Jahre gemeinsam mit EU-Mitgliedstaaten stattfindende Cyber Europe Exercise, die jährliche European Cybersecurity Challenge (ECSC) und die ICTAC Exercise.

40 Die ENISA wurde von „European Network and Information Security Agency“ in „European Union Agency for Cybersecurity“ umbenannt. Die Abkürzung des ursprünglichen Namens blieb dabei erhalten.

GD CONNECT ist die zuständige GD für die ENISA und vertritt gemeinsam mit *GD DIGIT* die EK in ENISA's Management und Executive Board. Die ENISA unterstützt die EK bei der Ausarbeitung eines Zertifizierungssystems für Cybersicherheit, das als Nachfolger des bestehenden Abkommens über die gegenseitige Anerkennung (Mutual Recognition Agreement, MRA) der *SOG-IS* dienen soll. ENISA arbeitet mit relevanten Behörden der Mitgliedstaaten und auf EU-Ebene, insbesondere den nationalen Computer Security Incident Response Teams, dem *CERT-EU*, Europol's *EC3* und *INTCEN* zusammen, um situationsbezogenes Bewusstsein zu schärfen und Policy-Entscheidungen in Bezug auf Gefahrenüberwachung, effektive Kooperation und Reaktionen auf groß angelegte grenzübergreifende Vorfälle zu unterstützen. Sie ist an dem *ICTAC* sowie der *TGG* beteiligt und als teilnehmende Institution der *JCU* vorgesehen. Zwischen *EVA*, *CERT-EU*, *EC3* und der ENISA besteht ein Memorandum of Understanding zur Zusammenarbeit und Austausch im Bereich der Cybersicherheit. ENISA und *eu-LISA* haben Anfang 2021 einen dreijährigen gemeinsamen Kooperationsplan geschlossen, in dessen Rahmen die Zusammenarbeit sowie der Austausch von Wissen und Expertise unter anderem im Bereich der Informationssicherheit verstärkt werden soll. Weitere kooperative Arbeitsbeziehungen bestehen mit der *GD JRC*, der *ECSO*, dem *ESVK* und der *EGC group*. Gemeinsam mit dem *CERT-EU* (und *ECDC*) hat die ENISA die *ICTAC Exercise* auf die Beine gestellt. Die ENISA stellt das Sekretariat des *CSIRTs Netzwerks* und von *CyCLONe*. Das *ECCC* soll die Aufgaben der ENISA ergänzen und mit dieser in der Ausübung seiner Aufgaben zusammenarbeiten. Die *HWPCI* arbeitet mit der ENISA zusammen. ENISA unterstützt die *NIS Cooperation Group* unter anderem durch Identifizierung von bewährten Praktiken in der Umsetzung der NIS-Richtlinie oder bei der Stärkung des vorgesehenen Meldeprozesses für Cybersicherheitsvorfälle innerhalb der EU durch Erarbeitung von Schwellenwerten, Vorlagen und Tools. ENISA ist an *EMPACT* beteiligt und nimmt an Treffen des *ECRB* teil. Die *ENISA AG* berät die ENISA unter anderem bei der Durchführung ihrer Aufgaben und auf Ersuchen kann auch die *SCCG* die ENISA beraten. Sie ist verantwortlich für die Durchführung und Bereitstellung zentraler Aspekte der *MeliCERTes* Anlage und gehört zu den Teilnehmer:innen der *CSCG*. Die *ECCG* kann neben der EK bei ENISA die Entwicklung neuer möglicher Zertifizierungsschemata beantragen. In Besuchsfunktion nimmt die ENISA an der durch das *ACT* organisierten NATO Cyber Coalition Exercise teil. ENISA und die *ITU* tauschen sich unter anderem zu Best Practices aus. Das TC CYBER von *ETSI* kooperiert mit der ENISA. Es besteht eine Kooperationsvereinbarung zwischen *CEN*, *CENELEC* und der ENISA. Die ENISA zählt zudem zu den „Institutional Stakeholder“ des *CEN*. Von Seiten der *ISO* ist die ENISA als mit ihr kooperierende Organisation gelistet. Die ENISA ist eine Partnerorganisation des *JTC 1*. Unter den *FIRST-Liaisons* befindet sich auch eine Vertreterin der ENISA. Auf deutscher Ebene arbeitet ENISA mit



dem *BSI/CERT-Bund* zusammen. Zudem sind Vertreter:innen des BSI im Management Board sowie dem National Liaison Officers Network der ENISA repräsentiert⁴¹.



Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL)

CEPOL ist als EU-Agentur dafür zuständig, Trainings für Strafverfolger:innen zu entwickeln, umzusetzen und zu koordinieren. Sie schafft ein Netzwerk an Trainingsinstituten für Strafverfolger:innen in den Mitgliedsstaaten und unterstützt sie dabei, Trainings zu Prioritäten im Sicherheitsbereich, zu Strafverfolgungsk Kooperation und Informationsaustausch anzubieten. Hierzu wurde unter anderem die CEPOL Cybercrime Academy als Teil des Trainingsportfolios in Budapest geschaffen. Sie ist darauf ausgelegt bis zu 100 Teilnehmer:innen gleichzeitig fortzubilden.

CEPOL Trainings werden in Kooperation mit der *EK*, dem *EC3*, dem *EJTN*, *Eurojust*, der *EUCTF* und der *ECTEG* erarbeitet und durchgeführt. Vertreter:innen von CEPOL sitzen zudem im Beirat des ECTEG. Weiterer Austausch und Arbeitsbeziehungen bestehen mit dem *ESVK* und der *GD HOME*. CEPOL ist zudem Mitglied der Community des *EU CyberNet* und an dem *ICTAC* sowie der *EMPACT* beteiligt. Sie kann als Beobachterin zu Sitzungen des *COSI (Rat der EU)* eingeladen. *Interpol* kooperiert mit CEPOL⁴².



Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)

Im Bereich der inneren Sicherheit hat sich Eurojust zum Ziel gesetzt, einen operativen Beitrag zur Bekämpfung organisierter Kriminalität, Terrorismus, Cyber sowie Schleusungskriminalität zu leisten. Hierzu koordiniert Eurojust Falluntersuchungen, indem es Informationsaustausch fördert, Bezüge zwischen laufenden

41 [Bundesamt für Sicherheit in der Informationstechnik, BSI Magazin 2019/1. Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheit: Nationale und Internationale Zusammenarbeit.](#)
[Europäische Kommission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.](#)
[Europäische Kommission, State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks.](#)
[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.](#)
[European Union Agency for Cybersecurity, About ENISA.](#)
[European Union Agency for Cybersecurity, Cybersecurity exercise boosts preparedness of EU Agencies to respond to cyber incidents.](#)
[European Union Agency for Cybersecurity, Cyber agencies assess future cooperation opportunities.](#)
[European Union Agency for Cybersecurity, ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.](#)
[European Union Agency for Cybersecurity, European Cyber Security Challenge 2020 – Event Date Change.](#)
[European Union Agency for Cybersecurity, EU Agency for Cybersecurity and Joint Research Centre discuss cooperation.](#)
[European Union Agency for Cybersecurity, List of ENISA Management Board Representatives and Alternates.](#)
[European Union Agency for Cybersecurity, List of National Liaison Officers \(NLO\).](#)
[European Union Agency for Cybersecurity, Second Staff Exchange between EU Cybersecurity Organisations.](#)

42 [CEPOL, About us.](#)
[CEPOL, CEPOL Cybercrime Academy Inaugurated.](#)
[Emailaustausch mit CEPOL-Vertreter:innen im August 2019.](#)



Ermittlungen herstellt, strafrechtliche Strategien entwickelt sowie gemeinsames Handeln, beispielsweise durch eine On-Call Koordination für Notfälle, ermöglicht. Hierdurch sollen die Ermittlungsfähigkeiten der Strafverfolgungsbehörden der Mitgliedstaaten im Bereich Cyberkriminalität, das Verständnis für Cyberkriminalität und Ermittlungsoptionen der Strafverfolger:innen und der Justiz gestärkt werden. Regelmäßig veröffentlicht Eurojust Berichte, wie beispielsweise den jährlichen Cybercrime Judicial Monitor, der einen Überblick zu Gesetzgebung und Rechtsprechung auf EU- und nationaler Ebene liefert oder anlassbezogen zu Herausforderungen und Best Practices.

Eurojust arbeitet mit spezialisierten Beratergruppen des EC3, Netzwerken der Chefs:innen der Cyberkriminalitätseinheiten sowie auf Cyberkriminalität spezialisierten Strafverfolger:innen zusammen. Beziehungen zwischen Eurojust und nationalen Behörden sowie Drittstaaten sollen gefördert werden. In der Organisationsstruktur von Eurojust ist Deutschland als EU-Mitgliedstaat mit einem Sitz in dessen wöchentlich tagendem Kollegium vertreten. Dieses wird durch ein Executive Board mit Beteiligung der EK unterstützt. Partnerschaftliche Beziehungen bestehen mit folgenden EU-Institutionen: Europol, EC3, CEPOL, eu-LISA, OLAF und EJTN. Es arbeitet zudem mit der HWPCI zusammen. Eurojust ist an der EMPACT beteiligt. Gemeinsam mit Europol hat Eurojust in der Vergangenheit einen Bericht zu gemeinsamen Herausforderungen in der Bekämpfung von Cyberkriminalität veröffentlicht. Bei Eurojust ist das Sekretariat des EJN angesiedelt und sie ist Mitglied der EUCTF. Eurojust ist zudem im Board des EJCN vertreten und bereitet dessen regelmäßige Treffen vor. Auf der Basis eines MoU kooperiert Eurojust zudem mit dem EJTN. Eurojust kann als Beobachter zu Treffen des COSI (Rat der EU) eingeladen werden. Dem:der EDSB kommt über Eurojust eine Aufsichtsfunktion in Bezug auf die rechtmäßige Verarbeitung personenbezogener Daten zu. Interpol arbeitet mit Eurojust zusammen⁴³.



CEN/CENELEC Cyber Security Coordination Group (CSCG)

Als organisationsübergreifendes Koordinierungsgremium hat sich die CSCG neben der strategischen Analyse von cyberrelevanten Entwicklungen u.a. zum Ziel gesetzt, das Potential von Normen zur Unterstützung von relevanten Vorschriften oder poli-

⁴³ Bundesamt für Sicherheit in der Informationstechnik, *Avalanche-Botnetz: BSI weitete Schutzmaßnahmen aus.* (Webseite entfernt)
[Eurojust, Casework at Eurojust.](#)
[Eurojust, College.](#)
[Eurojust, Cybercrime.](#)
[Eurojust, Cybercrime Judicial Monitor: Issue 6 – May 2021.](#)
[Eurojust, Eurojust Decision.](#)
[Eurojust, EU partners.](#)
[Eurojust, Germany.](#)
[Eurojust, Overview Report. Challenges and best practices from Eurojust's casework in the area of cybercrime.](#)
[Europäische Kommission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.](#)
[Europol and Eurojust, Common challenges in combating cybercrime. As identified by Eurojust and Europol.](#)



tischen Maßnahmen im Bereich der Cybersicherheit zu bewerten sowie Empfehlungen zur europäischen Positionierung in internationalen Normungsorganisationen und -gremien auszusprechen.

*Die CSCG ist ein gemeinsames Koordinierungsgremium von **CEN** und **CENELEC**. Es kann u.a. der **EK** Empfehlungen aussprechen und diese zur Cybersicherheitsstandardisierung beraten. Neben mitgliedsstaatlichen Institutionen gehören zu den Teilnehmer:innen der CSCG u.a. auch Vertreter:innen von **ENISA**, der **EVA** sowie **GD CONNECT**, **GD HOME** und **GD JRC**. Das Sekretariat der CSCG ist beim **DIN** angesiedelt, welches zudem auch für Deutschland an der CSCG beteiligt ist⁴⁴.*



Computer Emergency Response Team der Europäischen Kommission (CERT-EU)

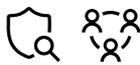
Das CERT-EU ist ein bei der Kommission angegliedertes IT-Notfallteam, das alle Organe, Einrichtungen und Agenturen der EU unterstützt. Seine Aufgaben reichen von der Bewusstseinsstärkung zu Zwecken der Prävention durch Hinweise und Weißbücher, über Aufklärung von Cyberbedrohungen bis hin zur Reaktion auf Vorfälle (incident response) durch Unterstützung und Koordinierung, bspw. durch Auswertung, Validierung und Verifizierung verfügbarer Informationen. Darüber hinaus überwacht das CERT-EU mögliche Schwachstellen und unternimmt Maßnahmen zur Stärkung der technischen Infrastruktur der EU-Institutionen durch „ethical hacking techniques“ und Penetrationstests.

*CERT-EU besteht aus Expert:innen von EU-Institutionen (bspw. der **EK** und Generalsekretariat des **Rates der EU**). Institutionell aufgehängt ist es bei **GD DIGIT**, **GD CONNECT** ist darüber hinaus im Board des CERT-EU vertreten. Das CERT-EU ist als teilnehmende Organisation der **JCU** vorgesehen und bereits Teil des **ICTAC**. Es arbeitet mit anderen CERTs in den Mitgliedsstaaten, dem CERT der **EZB** sowie der **EU Hybrid Fusion Cell** zusammen und ist Mitglied des **CSIRTs Netzwerks**. Über das CERT-EU ist die EU in der **EGC group** vertreten. Zwischen CERT-EU, **EC3**, der **ENISA** und der **EVA** besteht ein Memorandum of Understanding zur Zusammenarbeit und Austausch im Bereich der Cybersicherheit. Zudem haben CERT-EU und die **ENISA** eine strukturierte Zusammenarbeit vereinbart. Weiterer Austausch und Arbeitsbeziehungen bestehen mit dem **ESVK**. Das CERT-EU beteiligt sich an der **TGG**. CERT-EU und die **NCIRC** haben in der Vergangenheit eine technische Vereinbarung zur Zusammenarbeit beschlossen. Bei der Feststellung und Durchführung eines IT-Sicherheitsprogramms zum Schutz der **EK** vor Cybersicherheitsbedrohungen arbeitet CERT-EU unter anderem mit der **GD DIGIT** zusammen. Zudem tauscht das CERT-EU mit der **NCIA** Informationen aus und*

⁴⁴ [CEN/CENELEC/ETSI, CEN/CENELEC/ETSI Cyber Security Coordination Group \(CSCG\) White Paper. Deutsches Institut für Normung, Cyber Security Coordination Group \(CSCG\).](#)



kommt zu regelmäßigen Treffen auf Arbeitsebene zusammen. Das CERT-EU ist Zertifizierungskandidat bei TI und bei FIRST beteiligt⁴⁵.



Computer Security Incident Response Teams Netzwerk (CSIRTs Netzwerk)

Das Netzwerk wurde mit der NIS-Richtlinie eingesetzt und hat das Ziel, zu einer vertrauensvollen operativen Zusammenarbeit der Mitgliedstaaten beizutragen. Es bildet ein Forum, durch das Mitgliedsstaaten kooperieren und so ihre Fähigkeiten zur Handhabung grenzüberschreitender Cybersicherheitsvorfälle verbessern sowie eine koordinierte Reaktion erarbeiten können.

Das CSIRTs Netzwerk ist der *NIS Cooperation Group* unterstellt und setzt sich aus Repräsentanten:innen der ernannten CSIRTs der Mitgliedsstaaten sowie des *CERT-EU* zusammen. Für Deutschland übernimmt diese Funktion das *CERT-Bund*. Die *EK* beteiligt sich am Netzwerk als Beobachter. *ENISA* stellt das Sekretariat, setzt sich aktiv für die Kooperation zwischen den CSIRTs ein und bietet bei Bedarf aktive Unterstützung für die Koordinierung von Vorfällen. *EC3* und *CERT-EU* stellen dem Netzwerk forensische Analysen und weitere technische Informationen bereit.⁴⁶



Cyber Crisis Liaison Organisation Network (CyCLONE)

Als ein operativer Beitrag zu den Empfehlungen der Europäischen Kommission für eine koordinierte Reaktion auf große und grenzüberschreitende Cybersicherheitsvorfälle und -krisen (Blueprint) wurde das Cyber Crisis Liaison Organisation Network (CyCLONE) ins Leben gerufen. Durch verstärkte Kooperationsmechanismen und verbesserten Informationsfluss zwischen Cyber Crises Liaison Organisations (CyCLO) auf der technischen (bspw. CSIRTs) und der politischen Ebene, soll CyCLONE als Forum dazu beitragen, Konsultationen zu nationalen Reaktionsstrategien zu ermöglichen. Zudem sollen koordinierte Folgenabschätzungen zu den erwarteten oder beobachteten Auswirkungen einer Krise, politischen Entscheidungsträgern – sowohl auf nationalem als auch EU-Level – zugänglich gemacht werden. Eine Mitgliedschaft beruht für EU-Mitgliedstaaten auf rein freiwilliger Basis. Im Mai 2021 fand CyCLONE's erste Cybersicherheitsübung CySOPEX statt, in der eine groß angelegte grenzüberschreitende Cyberkrise simuliert und das Cyberkrisenmanagement der

⁴⁵ [CERT-EU, About Us.](#)

[CERT-EU, RFC 2350.](#)

[ENISA, ENISA and CERT-EU sign Agreement to start their Structured Cooperation.](#)

[Europäische Kommission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.](#)

[Europäische Kommission, NATO and CERT-EU discuss cyber threats ahead of EU elections.](#)

[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.](#)

⁴⁶ [CSIRTs Network, CSIRTs Network Members.](#)

[Europäische Kommission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.](#)

[Europäische Kommission, Recommendation on building a Joint Cyber Unit.](#)

[European Union Agency for Cybersecurity, CSIRTs Network.](#)



EU-Mitgliedstaaten getestet wurde. Diese Übung soll unter anderem einen Beitrag zu der Entwicklung der im Blueprint vorgesehenen „standard operating procedures“ (SOP) leisten.

Die Idee für ein solches Netzwerk, welches von der EK unterstützt wird, entstammt einer von Frankreich und Italien geführten Arbeitsgruppe der NIS Cooperation Group und die ENISA fungiert als Sekretariat des Netzwerkes. In der nahen Zukunft sollen vor allem Erkenntnisse aus Cybersicherheitsübungen wie Blue OLEx in die Arbeit des Netzwerkes einfließen. CySOPex wurde mit Unterstützung der ENISA und der EK durchgeführt. Eine Beteiligung des CyCLONe an der JCU ist vorgesehen⁴⁷.



Cyber and Information Domain Coordination Centre (CIDCC)

Auf lange Sicht soll das CIDCC als ständiges multinationales militärisches Element etabliert werden, in dem unter anderem Lagebilder aus dem Cyber- und Informationsraum abgeglichen, bewertet und deren Informationen in die Planung und Führung von Operationen und Missionen der EU eingebracht werden können. Das CIDCC soll bis Ende 2023 erstbefähigt und bis 2026 voll einsatzbereit sein. Bis dahin soll es auch mit den Fähigkeiten ausgestattet sein, Operationen im Cyber- und Informationsraum selbst organisieren und durchführen zu können. Bis zu dem vorgesehenen Umzug des CIDCC's nach Brüssel in 2023, wird es bei dem KdoCIR angesiedelt sein.

Die Initiative zur Errichtung des CIDCC wurde von Deutschland als ein Projekt im Rahmen der Ständigen Strukturierten Zusammenarbeit (PESCO) eingebracht. Neben Deutschland, welches durch sein KdoCIR die Rolle des Koordinators übernimmt, sind die Niederlande, Ungarn und Spanien am Aufbau des CIDCC beteiligt. Im Steuerungsgremium des CIDCC sind neben den teilnehmenden EU-Mitgliedstaaten Repräsentant:innen der EVA, des EU-Militärstabes sowie der ENISA vertreten. In seiner Konzeption des CIDCC hat sich das KdoCIR mit dem EUMS sowie der EVA abgestimmt⁴⁸.

- 47 [Bundesministerium des Innern, BMI und BSI beteiligen sich an Cyberkrisenübung Blue OLEx 2020.](#)
[Europäische Kommission, Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive \(EU\) 2016/1148.](#)
[Europäische Kommission, Joint exercise to test cooperation and cyber resilience at EU level.](#)
[European Union Agency for Cybersecurity, Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network \(CyCLONe\).](#)
[European Union Agency for Cybersecurity, EU Member States test rapid Cyber Crisis Management.](#)
[Vertretung der Europäischen Kommission in Deutschland, EU-Staaten testen ihre Zusammenarbeit im Falle von Cyber-Angriffen.](#)
- 48 [Bundesministerium der Verteidigung, Cyber and Information Domain Coordination Centre \(CIDCC\).](#)
[Bundeswehr, Europäisches Verteidigungsprojekt für Cybersicherheit – Das Cyber and Information Domain Coordination Centre.](#)
[Dorothee Frank, Meilenstein für die europäische Cyberlage.](#)
[PESCO, Cyber and Information Domain Coordination Center \(CIDCC\).](#)



Direktion Krisenbewältigung und Planung (CMPD)

Das Direktorat verantwortet integriertes zivil-militärisches Planen innerhalb des Europäischen Auswärtigen Diensts und trägt dadurch zur Umsetzung der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU bei. Ziel dieses strategischen Planens ist das Entwerfen möglicher Handlungsoptionen für die EU, welche als Grundlage für Entscheidungen des Rates in internationalen Krisensituationen dienen. Die CMPD steuert zweckgebundene Mittel und Unterstützung für den Schutz der IT-Systeme der GSVP sowie den Kapazitätsaufbau im Bereich Cybersicherheit bei.

*Das CMPD ist im **EAD** angesiedelt und ist an der Erstellung von Maßnahmen und Leitlinien für die IT-Sicherheit im GSVP-Kontext beteiligt. **Interpol** arbeitet mit der CMPD zusammen⁴⁹.*



ENISA-Beratungsgruppe (ENISA AG)

Mit dem Cybersecurity Act wurde eine ENISA-Beratungsgruppe eingesetzt, die sich aus anerkannten Expert:innen verschiedener Sektoren als Vertreter:innen der einschlägigen Interessenträger zusammensetzt. Dazu gehören etwa die IT-Branche, kleine und mittelständische Unternehmen, Betreiber „wesentlicher Dienste“, Verbrauchergruppen und ausgewählte zuständige Behörden. Die Amtszeit der Mitglieder beträgt zweieinhalb Jahre.

*Sachverständige der **EK** und der Mitgliedstaaten können an den Sitzungen teilnehmen und an der Arbeit der Beratungsgruppe mitwirken. Vertreter:innen anderer Stellen können von der:dem Exekutivdirektor:in der **ENISA** zur Teilnahme an Sitzungen hinzugerufen werden, besitzen allerdings kein Stimmrecht. Die Beratungsgruppe berät die ENISA bei der Durchführung ihrer Aufgaben sowie der:den Exekutivdirektor:in bei der Ausarbeitung eines Vorschlags für das Jahresarbeitsprogramm der ENISA. Darüber hinaus beschäftigt sie sich mit der Frage, wie die Kommunikation mit den einschlägigen Interessenträgern bezüglich des Jahresarbeitsprogramms sichergestellt werden kann. Neben den 33 ernannten Mitglieder:innen und deren Vertreter:innen sind unter anderem **Europol**, **EC3**, **CEN**, **CENELEC**, **ETSI**, die **eu-LISA** und **CERT-EU** aufgerufen, Repräsentant:innen für die Amtszeit 2023-2025 der ENISA AG zu nominieren⁵⁰.*

49 [European Union External Action Service, The Crisis Management and Planning Directorate \(CMPD\)](#). (Webseite entfernt)

[Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr](#).

50 [ENISA, Advisory Group \(AG\) 2023-2025](#).

[Europäisches Parlament und Rat der Europäischen Union, Verordnung \(EU\) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA \(Agentur der Europäischen Union für Cybersicherheit\) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung \(EU\) Nr. 526/2013 \(Rechtsakt zur Cybersicherheit\)](#).



EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell)

Die EU Hybrid Fusion Cell setzt einen Fokus auf die Analyse externer Aspekte hybrider Bedrohungen und soll eingestufte und offene Informationen, die spezifisch mit Indikatoren und Warnungen hinsichtlich hybrider Bedrohungen zusammenhängen, von verschiedenen Akteuren innerhalb des Europäischen Auswärtigen Diensts, der Kommission und der Mitgliedstaaten, sammeln, analysieren und teilen. Durch diese Analysen soll die Analyseeinheit das Bewusstsein für Sicherheitsrisiken erhöhen sowie die politische Entscheidungsfindung von Entscheidungsträger:innen auf nationaler und EU-Ebene unterstützt werden. Die Analyseeinheit verfügt zudem über ein Netzwerk nationaler Kontaktstellen für die Abwehr hybrider Bedrohungen, welches sich zweimal im Jahr trifft, um unter anderem Best Practices auszutauschen, Resilienz zu stärken sowie Gegeninitiativen zu hybriden Bedrohungen zu formulieren.

*Die EU Hybrid Fusion Cell ist institutionell innerhalb des **INTCEN** im **EAD** angesiedelt. Die Analyseeinheit arbeitet mit dem **EUMS INT** sowie für Informationen, insbesondere zu Cyber-Bedrohungen, auch mit dem **CERT-EU** zusammen. Routinemäßig gehen quartalsweise Berichte der EU Hybrid Fusion Cell an die beiden **Inter-Service Groups CHT** sowie **C3M**. Strukturierte Arbeitsbeziehungen und Informationsaustausch bestehen mit der **NATO Hybrid Analysis Branch** innerhalb der **JISD** sowie dem **NATO CCDCOE**⁵¹.*



EU Cyber Capacity Building Network (EU CyberNet)

Das EU CyberNet dient dazu, die Bemühungen der EU im Bereich des Cyberkapazitätsaufbaus durch Stärkung externer EU-Projekte sowie der Erhöhung der eigenen EU-Kapazität zur Bereitstellung technischer Hilfe im Kontext von Cybersicherheit und Cyberkriminalität zu unterstützen. Neben der Netzwerkfunktion soll EU CyberNet auch die Koordination unter den Akteuren verbessern und kollektives Fachwissen mobilisieren. Bis 2023 soll ein Netzwerk aus mindestens 500 Cybersicherheitsexpert:innen und mindestens 150 Akteuren aufgebaut sein, eine technische Plattform zur Verbindung der Expert:innen und Akteure geschaffen, Schulungen und Unterstützung angeboten und das EU CyberNet zu einem Knowledge Hub für das externe Cyberengagement der EU werden. Letzteres sieht unter anderem auch die Bereitstellung von strategischer, technischer, operativer und politischer Unterstützung, beispielsweise durch Ad-hoc Beratung, für EU-Behörden vor. Regelmäßig organisiert EU CyberNet auch Veranstaltungen zu relevanten Themen des Cyberkapazitätsaufbaus und richtet eine jährliche Konferenz aus.

⁵¹ [Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#)

[Europäische Kommission, FAQ: Joint Framework on countering hybrid threats.](#)

[Europäische Kommission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.](#)

[Europäische Kommission, Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen –eine Antwort der Europäischen Union.](#)

[EU-NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.](#)

[OSW, Towards greater resilience: NATO and the EU on hybrid threats.](#)



Die Etablierung des EU CyberNet wurde in Dokumenten des *Rates der EU* und der *EK* vorgesehen. Das EU CyberNet wird durch die *EK* finanziert und durch die estnische Information System Authority mit Unterstützung des *AA* als Kuratoriumsmitglied implementiert. EU CyberNet hat das *PSK* zur Implementierung der EU-Cybersicherheitsstrategie gebrieft. *CEPOL*, *ESVK*, *EUISS* und *BSI* sind bereits Mitglieder der Community⁵².



Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)

Das ECRB wurde als Austausch- und Diskussionsforum zu strategischen Fragen zwischen privaten und öffentlichen Akteuren im Finanzsektor geschaffen. Innerhalb des ECRB sollen u.a. Best Practices geteilt, das Bewusstsein für Cyberresilienz gestärkt und gemeinsame Initiativen ergriffen werden. Ein Output des ECRB ist die Cyber Information and Intelligence Sharing Initiative (CIISI-EU), die zum Schutz des Finanzsystems und seiner Infrastruktur vor Bedrohungen aus dem Cyberraum beispielsweise durch Prävention, Identifizierung und gegenseitigem Informationsaustausch beitragen soll.

An ECRB-Treffen nehmen u.a. Vertreter:innen der *EK*, *Europol*, der *ENISA* und der *Deutschen Bundesbank* teil. Neben weiteren Akteuren sind die *EZB*, *ENISA* und *Europol* auch in der CIISI-EU involviert. Auf Anfrage kann das ECRB auch gegenüber der *EK*, *EZB* oder weiteren EU-Organisation in beratender Funktion tätig werden. Das Sekretariat des ECRB wird durch die *EZB* gestellt⁵³.



Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA)

eu-LISA verwaltet integrierte IT-Großsysteme, die für die innere Sicherheit in den Schengen-Ländern sorgen. Diese ermöglichen Schengen-Ländern den Austausch von Visadaten und die Ermittlung der Zuständigkeit bei der Überprüfung eines bestimmten Asylantrags. Sie testet außerdem neue Technologien, die helfen sollen, ein moderneres, wirkungsvolles und sicheres Grenzmanagementsystem in der EU aufzubauen. Die Agentur ist zudem für die technische Umsetzung und Entwicklung der Interoperabilität der EU-Informationssysteme zuständig.

52 [EU CyberNet, EU CyberNet.](#)
[EU CyberNet, Informal cybersecurity briefing to the Political and Security Committee.](#)
[EU CyberNet, Project Deliverables.](#)
[EU CyberNet, Team.](#)
[EU CyberNet, Stakeholder Community.](#)
[Rat der EU, EU External Cyber Capacity Building Guidelines.](#)

53 [Europäische Zentralbank, Euro Cyber Resilience Board for pan-European Financial Infrastructures.](#)
[Europäische Zentralbank, Euro Cyber Resilience Board for pan-European Financial Infrastructures \(ECRB\). Cyber Information & Intelligence Sharing Initiative: Terms of Reference.](#)
[Europäische Zentralbank, Third meeting of Euro Cyber Resilience Board for pan-European Financial Infrastructures \(ECRB\).](#)
[Europäische Zentralbank, Mandate of the Euro Cyber Resilience Board for pan-European Financial Infrastructures.](#)



Die Agentur arbeitet mit den Mitgliedstaaten sowie auf EU-Ebene mit dem:der **EDSB**, dem **Rat der EU**, der **EK**, **CEPOL**, **Eurojust**, **Europol** und **GD HOME** zusammen. **Eurojust** und **Europol** sind zudem in **eu-LISA's Management Board** und **Beratergruppen** vertreten. **ENISA** und **eu-LISA** haben Anfang 2021 einen dreijährigen gemeinsamen **Kooperationsplan** geschlossen, in dessen Rahmen die **Zusammenarbeit** sowie der **Austausch von Wissen und Expertise** unter anderem im Bereich der **Informationssicherheit** verstärkt werden soll. **eu-LISA** ist an der **EMPACT** beteiligt. **Kontakte auf Arbeitsebene** wurden zudem mit dem **NATO CCDCOE** aufgenommen. **Interpol** kooperiert mit **eu-LISA**. Das **BMI** ist durch eine:n **Verteter:in** im **Management Board** der **eu-LISA** vertreten⁵⁴.



Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG)

Die Europäische Gruppe für die Cybersicherheitszertifizierung, die sich aus **Vertreter:innen** der **Mitgliedsländer** zusammensetzt, trägt als **Expertengruppe** zur **Entwicklung von Zertifizierungsschemata** durch die **ENISA** bei. Für verschiedene **Produkt- bzw. Servicetypen** werden dabei spezifische Schemata entwickelt, die unter anderem die **Gültigkeitsdauer** von **Sicherheitszertifikaten** beinhalten. Sie unterstützt die **Kommission** dabei, ein **europäisches Arbeitsprogramm** für **Cybersicherheitszertifizierungsschemata** aufzubauen. Das **Arbeitsprogramm** soll beispielsweise der **Industrie** als **strategisches Dokument** dienen, um sich **frühzeitig** auf **zukünftige Zertifizierungsvorgaben** einzustellen.

*Dazu arbeitet die Gruppe mit der **SCCG** zusammen. Um der **schnellen Entwicklungen im Technologiebereich** gerecht zu werden, kann die Gruppe, neben der **EK**, bei **ENISA** die **Entwicklung neuer möglicher Zertifizierungsschemata**, die noch nicht im **Arbeitsprogramm** enthalten sind, **beantragen**⁵⁵.*



Europäische Kommission (EK)

Die Europäische Kommission nimmt eine **strategisch-organisatorische Rolle** in der **EU-Cybersicherheitsarchitektur** ein. Sie ist dafür **zuständig**, **Kapazitäten** und **Ko-**

⁵⁴ [Europäische Union, Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht \(eu-LISA\).](#)

[European Union Agency for Cybersecurity, ENISA and eu-LISA – Cooperation for a More Digitally Resilient Europe. eu-LISA, Consolidated Annual Activity Report 2020.](#)

[eu-LISA, Consolidated Annual Activity Report 2020.](#)

[eu-LISA, Declaration of Interest – Kai Schollendorf.](#)

[eu-LISA, ETIAS.](#)

[eu-LISA, EU Agencies.](#)

[eu-LISA, EU Institutions.](#)

[eu-LISA, Interoperability.](#)

⁵⁵ [Europäische Kommission, The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification.](#)

[Europäisches Parlament und Rat der Europäischen Union, Verordnung \(EU\) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA \(Agentur der Europäischen Union für Cybersicherheit\) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung \(EU\) Nr. 526/2013 \(Rechtsakt zur Cybersicherheit\).](#)

operation in der Cybersicherheit auszubauen, die EU als Akteur in diesem Bereich zu stärken und eine Integration in andere Policy Bereiche der EU voranzutreiben. Sie verfügt über ein eigenes Frühwarnsystem (ARGUS), das ein internes Kommunikationsnetz und ein spezifisches Koordinierungsverfahren umfasst. Im Falle einer schweren, EU-weiten Krise, die den Cyberbereich betrifft, erfolgt die Koordinierung bei der Kommission via ARGUS. Im Digital Europe Programme stellt die EK in verschiedenen Feldern, so unter anderem auch Cybersicherheit, außerdem strategisches Funding bereit, um die digitale Transformation von Gesellschaft und Wirtschaft zu fördern. Digital Europe wird durch andere Programme wie Horizon Europe komplementiert.

*Eine Reihe von Generaldirektionen arbeiten im Bereich Cybersicherheit, darunter **CONNECT**, **DIGIT**, **HOME**, **JRC** und **RTD**. Zudem sind das **CERT-EU** und das **ERCC** (ERCC über GD ECHO) bei der Kommission angegliedert. Der **Rat der EU** kann die EK mit der Verhandlung internationaler Abkommen beauftragen, über dessen Abschluss der Rat basierend auf einem Vorschlag der EK entscheidet. Das **OLAF** ist der EK unterstellt. Das **ECCC** basiert auf einem Vorschlag der EK, welche gemeinsam mit den EU-Mitgliedstaaten auch durch zwei Vertreter:innen im Verwaltungsrat des ECCC repräsentiert ist. Die EK hat den Vorsitz der **SKI-Kontaktgruppe** sowie der **SCCG** (letzteren gemeinsam mit der ENISA) inne. Sie ist zudem im Aufsichtsrat der **EA** vertreten. Die **eu-LISA**, das **EC3**, die **HWPCI**, die **EZB** und das **EUISS** arbeiten mit der EK zusammen. Die EK ist an der Erarbeitung und Durchführung von **CEPOL-Trainings** und **EMPACT** beteiligt. Die **ECCG** unterstützt die EK bei dem Aufbau eines europäischen Arbeitsprogramms für Cybersicherheitszertifizierungsschemata. Auf Anfrage kann der:die **EDSB** für die EK beratend tätig werden. Vertreter:innen der EK nehmen an Treffen des **ECRB** teil, auf Anfrage kann das **ECRB** auch u.a. gegenüber der EK in beratender Funktion tätig werden. Die EK beteiligt sich am **CSIRTs Netzwerk** als Beobachterin und ist Mitglied der **EUCTF**. Die **ENISA** unterstützt die EK bei der Ausarbeitung eines Zertifizierungssystems für Cybersicherheit, das als Nachfolger des bestehenden Abkommens über die gegenseitige Anerkennung (Mutual Recognition Agreement, MRA) der **SOG-IS** dienen soll. Die Etablierung des **EU CyberNet** wurde unter anderem in Dokumenten der EK vorgesehen. Das **EJTN** arbeitet im Bereich Cybersicherheit mit der **EK** zusammen. Die **ECISO** ist Vertragspartnerin der EK. Die **ITU** arbeitet mit der EK im Kontext der Harmonisierung der IKT-Politik innerhalb der AKP-Staaten zusammen. Die EK kann sich an Treffen der **MAG** des **IGF** beteiligen. Vertreter:innen der EK können auf Einladung an **CoE-Treffen** von Ministerkomitee bis Arbeitsgruppen teilnehmen. Die **CSCG** kann der EK Empfehlungen aussprechen und diese zur Cybersicherheitsstandardisierung beraten. **ETSI** und **CENELEC** tauschen sich mit der EK aus. Die **ISO** listet die EK als mit ihr kooperierende Organisation. Die EK gehört zu den Partnerorganisationen des **JTC 1**. In der Vergangenheit hat die EK gemeinsam mit dem **ER** zwei Absichtserklärungen zur verstärkten NATO-EU Kooperation, auch im Bereich der Cybersicherheit und -verteidigung, mit dem NATO-Generalsekretär getroffen. Die EK*



finanziert das OVERCLOCK Projekt, an dem das **BKA** und die **ZITiS** mitwirken. Alle zwei Jahre muss das **BSI** der **EK** bestimmte Informationen übermitteln. Die **EK** zählt zu den Partnern des **GMLZ** sowie den Drittmittelgebern der **SWP**⁵⁶.



Europäische Kooperation für Akkreditierung (EA)

Die Europäische Kooperation für Akkreditierung ist der Zusammenschluss von europäischen Akkreditierungsstellen und ist für die Koordination der Akkreditierung innerhalb der EU, EFTA und beitragswilligen Ländern zuständig. Sie ist eine gemeinnützige Vereinigung und besteht aus 49 national anerkannten Akkreditierungsstellen. Übergeordnet soll die Vereinigung zu einer Harmonisierung von Akkreditierungsverfahren beitragen. Sie ist folglich auch für Akkreditierungen von Produkten der IT-Sicherheit zuständig.

Die **EA** ist von der **EK** offiziell benannt worden, die **EK** sitzt zudem im Aufsichtsrat der **EA**. Die **DAkKS** ist Mitglied in der **EA** und repräsentiert deutsche Interessen. Darüber hinaus ist die **EA** Mitglied der **SCCG**⁵⁷.



Europäische Verteidigungsagentur (EVA)

Die Europäische Verteidigungsagentur unterstützt alle EU-Mitgliedstaaten bei der Entwicklung kooperativer europäischer Verteidigungsprojekte. Ein Ziel der EVA ist der Ausbau der Cyberabwehrfähigkeit. Sie unterstützt Mitgliedstaaten bei der Entwicklung eigener Abwehrfähigkeiten. Cyberverteidigung zählt hierbei dabei zu ihren vier Kernprogrammen. Konkret unterstützt die EVA unter anderem die Erstellung eines Risikomanagementmodells für Cybersicherheit im Kontext der Lieferketten militärischer Fähigkeiten, die Etablierung des Cyber Ranges Federation Projektes sowie den Aufbau spezifischer Fähigkeiten zur Erkennung von APTs als auch Cyber Situational Awareness.

56 [Commission of the European Communities, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Bestimmungen der Kommission zum allgemeinen Frühwarnsystem „ARGUS“.](#)

[Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#)

[European Commission, Operational Vanguard, using Encryption Research for Criminal Lockdown.](#)

[European Commission, The Digital Europe Programme.](#)

Europäische Kommission, Anhang zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen. (Webseite entfernt)

[European Commission, State of the Union: New EU cybersecurity rules ensure more secure hardware and software products.](#)

[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU. EU-NATO, Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.](#)

57 [DAkKS, Europäischer Rechtsrahmen.](#)

[European Accreditation, EA Advisory Board.](#)

[European Accreditation, European co-operation for Accreditation: Who we are.](#)

[European Accreditation, Relations with European Commission.](#)



Die EVA untersteht dem *Rat der EU*, dem es Bericht erstattet und von welchem es seine Leitlinien erhält. Die Rolle des:der Leiter:in der EVA fällt der:dem Hohen Vertreter:in der Union für Außen- und Sicherheitspolitik der EU zu. Das Lenkungs-gremium der EVA kommt auf Ebene der Verteidigungsminister:innen der Mitgliedstaaten zusammen, für Deutschland ist der:die Bundesminister:in der Verteidigung (*BMVg*) Mitglied. Für *PESCO* führt sie gemeinsam mit dem EAD alle Sekretariatsfunktionen. Die EVA ist im Steuerungsgremium des *CIDCC* vertreten und an dem *ICTAC* beteiligt. Mit *ENISA*, dem *EC3* und *CERT-EU* besteht ein Memorandum of Understanding, mit dem Ziel einen Kooperationsrahmen für die Organisationen zu entwickeln. Die EVA ist in unterstützender Funktion als beteiligte Organisation der *JCU* vorgesehen. Es bestehen zudem Arbeitsbeziehungen mit dem *ESVK*, der *ECSO*, dem *Hybrid CoE*, der *HWPCI* und dem *NATO CCDCOE* und *ACT*. Die EVA nimmt an *Locked Shields* teil. Der:die Chief Executive der EVA kommt zu regelmäßigen Treffen mit dem:der *SACT (ACT)* sowie Assistant *SECGEN*'s der NATO zusammen. Das Steering Board der EVA wird zudem regelmäßig durch letztere gebrieft. Die EVA gehört zu den „Institutional Stakeholder“ des *CEN* und den Teilnehmer:innen der *CSCG*⁵⁸.



Europäische Zentralbank (EZB)

Aufgrund ihrer Zuständigkeit als Aufsichtsbehörde für den Euroraum kommt der EZB auch das Monitoring und die Sicherstellung der Operationsfähigkeit von Finanzmarktinfrastruktur und systemrelevanten Zahlungssystemen durch Aufbau einer größtmöglichen Cyberresilienz zu. Hierzu fördert die EZB u.a. den internationalen Austausch von sicherheitsrelevanten Informationen, identifiziert Best Practices und hat ein gemeinsames europäisches Rahmenwerk für „threat intelligence-based ethical red-teaming“ u.a. zur Diagnose von Stärken und Schwächen etabliert (*TIBER-EU*). Darüber hinaus sind die nationalen Zentralbanken im Euro-raum verpflichtet, bedeutende Cybersicherheitsvorfälle der EZB zu melden und die EZB beaufsichtigt zudem, wie diese das Management relevanter Risiken in Bezug auf ihre IT-Systeme handhaben.

58 [Die Europäische Union, Europäische Verteidigungsagentur \(EVA\).](#)
[European Defence Agency, Cooperation between the European Defence Agency and the Euroocean Security and Defence College.](#)
[European Defence Agency, Cyber.](#)
[European Defence Agency, Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States.](#)
[European Defence Agency, EDA participates in „Locked Shields“ cyber defence exercise.](#)
[European Defence Agency, Exchange of letters: NATO Allied Command Transformation.](#)
[European Defence Agency, Four EU cybersecurity organisations enhance cooperation.](#)
[European Defence Agency, Governance.](#)
[European Defence Agency, Liaison between the European Defence Agency and the Cooperative Cyber Defence Centre of Excellence.](#)
[European Defence Agency, Liaison between the European Defence Agency and the European Centre of Excellence for Countering Hybrid Threats.](#)
[European Defence Agency, Priority Setting.](#)
[European External Action Service, Permanent Structured Cooperation – PESCO.](#)
[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.](#)
[EU-NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU](#)



Die EZB beaufsichtigt die nationalen Zentralbanken des Euroraums, darunter auch die **Deutsche Bundesbank**. Sie arbeitet mit anderen EU-Institutionen wie der **EK** und dem dort ansässigen **CERT-EU** sowie nationalen Cybersicherheitsbehörden wie dem **BSI** zusammen. Auch die Deutsche Bundesbank beteiligt sich an **TIBER-EU** und hat ein entsprechendes nationales **TIBER-DE** auf Basis einer gemeinsamen Entscheidung mit dem **BMF** etabliert. Der:die Präsident:in der Deutschen Bundesbank ist Mitglied des EZB-Rates. Das CERT der EZB ist bei **FIRST** involviert⁵⁹.



Europäischer Auswärtiger Dienst (EAD)

Der Europäische Auswärtige Dienst ist leitend im Bereich Konfliktprävention, Cyberdiplomatie und strategischer Kommunikation. Der EAD hat ein eigenes System, um koordiniert auf Krisen und Notfälle zu reagieren: den Crisis Response Mechanism (CRM). Er wird bei sämtlichen Ereignissen ausgelöst, die tatsächlich oder potenziell die Sicherheitsinteressen der EU oder von Mitgliedstaaten betreffen. Die Leitung des EAD obliegt dem:er Hohe Vertreter:in der Europäischen Union für Außen- und Sicherheitspolitik, der:die für die gemeinsame Außen- und Sicherheitspolitik sowie die Gemeinsame Sicherheits- und Verteidigungspolitik der Union zuständig ist. Gleichzeitig ist diese:r auch Vize-Präsident:in der Europäischen Kommission, um eine kohärente EU-Politik, auch im Bereich der Sicherheitspolitik im Cybersicherheitsbereich, zu garantieren.

Der EAD beherbergt **EUMS INT**, **INTCEN** und die dort untergebrachte **EU Hybrid Fusion Cell**. Zudem ist dort das **CMPD** und das **ESVK** angesiedelt. Vertreter:innen des EAD haben den Vorsitz im **PSK** inne. Die **HWPCI**, das **EUISS** und die **ECSO** arbeiten mit dem EAD zusammen. Der EAD hat gemeinsam mit der **EK** den Vorsitz der **ISG CHT** inne und ist an der **ISG C3M** beteiligt. Zusammen mit der **EVA** bildet der EAD das Sekretariat der **PESCO**. Eine Beteiligung des EAD an der **JCU** ist vorgesehen. Der EAD erhält Informationen und Einschätzungen des **STAR (GD HOME)**. Der EAD ist im **COSI (Rat der EU)** vertreten. Regelmäßig tauscht sich der:die Hohe Vertreter:in mit dem:der NATO-Generalsekretär:in aus und nimmt darüber hinaus an Treffen des **NAC** auf Ebene der Verteidigungsminister:innen teil. Für Diskussionen zu Cyberverteidigung/-abwehr ist der EAD bereits zu Treffen mit Vertreter:innen der **ESCD** zusammengekommen. Zudem hat der EAD in der Vergangenheit zusammen mit **ENISA** Berichte veröffentlicht, beispielsweise zu „Foreign Information Manipulation Interference (FIMI) and Cybersecurity – Threat Landscape“. Die dem EAD unterstellte Delegation der EU bei den UN in New York hat sich an Debatten zu Cybersicherheit innerhalb des **UNSC** beteiligt.

59 [Deutsche Bundesbank, TIBER-DE: Threat Intelligence-based Ethical Red Teaming in Germany.](#)
[Europäische Zentralbank, Cyber resilience and financial market infrastructures.](#)
[Europäische Zentralbank, TIBER-EU FRAMEWORK: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.](#)
[Europäische Zentralbank, What is cyber resilience?.](#)
[Europäische Zentralbank, What is TIBER-EU?.](#)



Das **ERCC** koordiniert sich unter anderen mit dem EAD und der EAD entsendet eine Delegation zum **CoE**⁶⁰.



Europäische:r Datenschutzbeauftragte:r (EDSB)

Die:der Europäische Datenschutzbeauftragte:r übernimmt diese Funktion innerhalb der Europäischen Union. Ihm:ihr und der dahinter stehenden Kontrollbehörde obliegt die Überwachung über die Einhaltung datenschutzrechtlicher Prinzipien bei der Verarbeitung personenbezogener Daten durch sämtliche EU-Institutionen. Zur Gewährleistung des Schutzes der Privatsphäre umfasst dies beispielsweise die Durchführung von Untersuchungen oder die Bearbeitung eingereicherter Beschwerden. Darüber hinaus beobachtet und bewertet der:die EDSB etwaige sich durch neue technologische Entwicklungen ergebende Implikationen für den Datenschutz. Der:die EDSB wird für eine Amtszeit von fünf Jahren ernannt und arbeitet zudem mit nationalen Datenschutzbehörden in den EU-Mitgliedsstaaten zusammen. In der Vergangenheit hat der:die EDSB unter anderem zur Cybersicherheitsstrategie der EU und weiteren Vorschlägen, Empfehlungen und Mitteilungen der EK mit Cybersicherheitsbezug aus datenschutzrechtlicher Perspektive Stellung bezogen.

Auf Anfrage kann der:die EDSB für die **EK** und den **Rat der EU** beratend tätig werden. Der Rat der EU ist an der Benennung des:der EDSB beteiligt. Der:die EDSB übernimmt Aufsichtsfunktionen über **Europol** und **Eurojust**. Von deutscher Seite besteht Kontakt und Austausch mit dem:der **BfDI**⁶¹.



Europäischer Rat (ER)

Dem Europäischen Rat obliegt die Festlegung der „politischen Zielvorstellungen und Prioritäten“ der EU. Er kann hierzu themen- und anlassbezogene Schlussfolgerungen beschließen und hat darüber hinaus eine Strategische Agenda für die EU in den Jahren 2019-2024 angenommen. Im ersten Schwerpunktbereich „Schutz der Bürgerinnen und Bürger und der Freiheiten“ wird auch die Notwendigkeit des Schutzes vor böswilligen Cyberaktivitäten, hybriden Bedrohungen sowie Desinformation hervorgehoben.

- 60 [Annegret Bendiek, Gemeinsame Außen- und Sicherheitspolitik: von der Transformation zur Resilienz. Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#)
[ENISA, Foreign Information Manipulation Interference \(FIMI\) and Cybersecurity – Threat Landscape. European Commission, Factsheet: Joint Cyber Unit.](#)
[European Union External Action, The Crisis Management and Planning Directorate \(CMPD\). \(Webseite entfernt\)](#)
[Europäischer Rat/Rat der Europäischen Union, Politisches und Sicherheitspolitisches Komitee \(PSK\).](#)
[European Union External Action Service, High Representative. \(Webseite entfernt\)](#)
[EU-NATO, Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.](#)
[IMPETUS, An Integral Element of the EU Comprehensive Approach.](#)
- 61 [BfDI, Stellungnahme zu überarbeiteten Standarddatenschutzklauseln.](#)
[EDSB, Über den EDSB.](#)
[EDSB, EDPS formal comments in response to the „Cybersecurity Package“ adopted by the Commission.](#)
[EDSB, Häufig gestellte Fragen.](#)



Der Europäische Rat setzt sich aus den Staats- und Regierungschefs:innen der EU-Mitgliedstaaten sowie der:m Präsident:in der EK als auch des Europäischen Rates (beide ohne Stimmrecht) zusammen und trifft sich mindestens zweimal im Halbjahr. Letzterem:r obliegt der Vorsitz. An Sitzungen mit außenpolitischen Bezug nimmt zusätzlich der:die Hohe Vertreter:in (EAD) teil⁶².



Europäisches Amt für Betrugsbekämpfung (OLAF)

Das Europäische Amt für Betrugsbekämpfung ist für sämtliche Untersuchungen von Betrugsvorwürfen zu Lasten des EU-Haushalts, Korruption sowie schwerem Fehlverhalten innerhalb der EU-Institutionen zuständig. OLAF's Untersuchungen können die Einleitung von strafrechtlichen Maßnahmen, finanzielle Rückforderungen oder andere disziplinarische Maßnahmen zur Folge haben. Mit Themen der Cyber- und IT-Sicherheit kann OLAF im Rahmen seines operativen Eigenschutzes oder als Komponente innerhalb eines untersuchten Delikts in Verbindung kommen.

OLAF ist der EK unterstellt, aber in der Ausführung seines Mandates unabhängig. Der Arbeitsgruppe des Rates der EU zur Betrugsbekämpfung erstattet OLAF regelmäßig Bericht⁶³.



Europäisches Institut für Telekommunikationsnormen (ETSI)

Als europäische Normungsorganisation arbeitet ETSI an der Entwicklung und Annahme von überregionalen Standards für auf IKT-basierten Anwendungen und Systemen. Für den Bereich der Cybersicherheit finden die entsprechenden Hauptaktivitäten im Rahmen des Cybersecurity Technical Committee (TC CYBER) statt. Schwerpunkte stellen dabei beispielsweise die Cybersicherheit von nationalen Kritischen Infrastrukturen, Unternehmen oder Einzelpersonen dar.

ETSI steht in Austausch mit dem CEN, dem CENELEC sowie der EK. Deutsches Mitglied des ETSI ist die DKE. Die ISO listet ETSI als mit ihr kooperierende Organisation. Das TC CYBER kooperiert mit der ITU, der ISO, der ENISA und nominiert Repräsentant:innen für die ENISA AG. Das ETSI ist darüber hinaus Mitglied der SCCG. Innerhalb des DIN/DKE Gemeinschaftsgremiums „Cybersecurity“ wird u.a. die deutsche Beteiligung im TC Cyber koordiniert. ETSI gehört zu den Partnerorganisationen des JTC 1. Der BSIKT befasst sich u.a. auch mit Entwicklungen innerhalb des ETSI⁶⁴.

62 [Europäischer Rat, A New Strategic Agenda 2019–2024.](#)

[Europäischer Rat, Der Europäische Rat.](#)

63 [Europäisches Amt für Betrugsbekämpfung, About Us.](#)

[Europäisches Amt für Betrugsbekämpfung, Cooperation with EU institutions.](#)

64 [Europäisches Institut für Telekommunikationsnormen, About Us.](#)

[Europäisches Institut für Telekommunikationsnormen, Cybersecurity.](#)

[Europäisches Institut für Telekommunikationsnormen, ETSI in Europe.](#)

[Europäisches Institut für Telekommunikationsnormen, TC CYBER Roadmap.](#)

[Europäisches Institut für Telekommunikationsnormen, TC CYBER Activity Report 2020.](#)



Europäisches Komitee für elektrotechnische Normung (CENELEC)

CENELEC hat es sich zum Ziel gesetzt, freiwillige Standards für den Bereich der Elektrotechnik zu erarbeiten. Cybersicherheit stellt dabei eine der Standardisierungsprioritäten dar. Ein gemeinsames technisches Gremium mit dem CEN befasst sich mit cybersicherheits- und datenschutzrelevanten Standards (CEN/CLC/JTC 13). CEN/CLC/JTC 13 zielt dabei zum einen darauf ab, bereits erarbeitete Normen auf internationaler Ebene für die europäische Ebene zu implementieren und zum anderen auch eigene europäische Standards im Falle identifizierbarer Lücken zu erarbeiten.

CENELEC kooperiert mit der IEC und tauscht sich mit der EK und ETSI aus. Es besteht zudem eine Kooperationsvereinbarung zwischen CEN, CENELEC und der ENISA. CEN und CENELEC nominieren gemeinsam Repräsentant:innen für die ENISA AG. Die CSCG ist ein gemeinsames Koordinierungsgremium von CEN und CENELEC. Deutsches Mitglied im CENELEC ist die DKE. Das DIN stellt das Sekretariat der CEN/CLC/JTC 13. CEN/CLC/JTC 13 arbeitet mit der ENISA zusammen. Es prüft die Übernahme von Standards, die beispielsweise im Rahmen des ISO/IEC JTC 1, der ISO, der IEC oder der ITU entstanden sind. Innerhalb des DIN/DKE Gemeinschaftsgremiums „Cybersecurity“ wird u.a. die deutsche Beteiligung im CEN/CENELEC JTC 13 gesteuert. Der BSIKT befasst sich u.a. auch mit Entwicklungen innerhalb des CENELEC. Es ist außerdem Mitglied der SCCG⁶⁵.



Europäisches Komitee für Normung (CEN)

Das CEN beschreibt sich selbst als Plattform für die Erarbeitung von Normen und anderweitiger technischer Dokumente auf europäischer Ebene. Ein gemeinsames technisches Gremium mit dem CENELEC, das CEN/CLC/JTC 13, befasst sich dabei mit cybersicherheits- und datenschutzrelevanten Standards (Beschreibung s. Eintrag CENELEC).

Deutsches Mitglied des CEN ist das DIN. Es besteht eine Kooperationsvereinbarung zwischen CEN, CENELEC und der ENISA. Die CSCG ist ein gemeinsames Koordinierungsgremium von CEN und CENELEC. Die ENISA, EVA und GD JRC zählen zu den „Institutional Stakeholder“ des CEN und ETSI steht mit dem CEN in Austausch. Innerhalb des DIN/DKE Gemeinschaftsgremium „Cybersecurity“ wird beispielsweise die deutsche Beteiligung im CEN/CLC/JTC 13 gesteuert. Der BSIKT befasst sich u.a. auch mit Entwicklungen innerhalb des CEN. Es ist außerdem Mitglied der SCCG⁶⁶.

⁶⁵ [CEN/CENELEC, Business Plan CEN/CENELEC JTC 13: Cybersecurity and data protection.](#)

[Europäisches Komitee für elektrotechnische Normung, About CENELEC.](#)

[Europäisches Komitee für elektrotechnische Normung, CEN and CENELEC.](#)

[Europäisches Komitee für elektrotechnische Normung, CEN/CLC/JTC 13 – Cybersecurity and Data Protection.](#)

[Europäisches Komitee für elektrotechnische Normung, CEN/CLC/JTC 13/WG 4 – Cybersecurity services.](#)

[Europäisches Komitee für elektrotechnische Normung, Cybersecurity and data protection.](#)

[Europäisches Komitee für elektrotechnische Normung, ISO and IEC.](#)

[Europäisches Komitee für elektrotechnische Normung, List of CENELEC Members.](#)

⁶⁶ [Agentur der Europäischen Union für Cybersicherheit, Cyber-security collaboration agreement between ENISA & European standardisation bodies, CEN and CENLEC.](#)

[Europäisches Komitee für Normung, About CEN.](#)

[Europäisches Komitee für Normung, CEN Communities.](#)

[Europäisches Komitee für Normung, List of CEN Members.](#)



Europäisches Polizeiamt (Europol)

Europol ist die Strafverfolgungsbehörde der Europäischen Union und unterstützt die Europäische Kommission sowie die EU-Mitgliedsstaaten bei der Strafverfolgung von Cyberkriminalität, Terrorismus und organisiertem Verbrechen. Europol unterstützt so beispielsweise Mitgliedsstaaten bei zuvor eingeleiteten Ermittlungen und analysiert Kriminalitätstrends in der EU. Europol arbeitet dabei auch mit Nicht-EU-Mitgliedstaaten und internationalen Organisationen zusammen.

Im Bereich Cyberkriminalität stärkt Europol insbesondere die Strafverfolgung durch das ihm unterstellte EC3. Eine Teilnahme Europol's an der JCU ist vorgesehen. Die Eurojust, die eu-LISA, das ESVK, die HWPCI und die ECSO arbeiten mit Europol zusammen. Europol ist Mitglied der EUCTF, die es zusammen mit der EK und EU-Mitgliedsstaaten gegründet hat, der TGG und des ICTAC. Gemeinsam mit dem EC3 nominiert Europol Repräsentant:innen für die ENISA AG. Vertreter:innen von Europol sitzen im Beirat des ECTEG. Europol ist an EMPACT beteiligt und nimmt an Treffen des ECRB teil. Europol erhält Informationen und Einschätzungen des STAR (GD HOME). Das INTCEN erarbeitet mit Europol halbjährlich die vorausschauende Bedrohungslage, welche an den COSI (Rat der EU) übermittelt wird, in den Europol auch als Beobachter eingeladen werden kann. Dem:der EDSB kommt über Europol eine Aufsichtsfunktion in Bezug auf die rechtmäßige Verarbeitung personenbezogener Daten zu. Europol arbeitet mit Interpol sowie dem BKA zusammen. Das BKA dient Europol als Nationale Stelle und ist somit deutscher Ansprechpartner für Europol. Jährlich richten Europol (durch das EC3) und Interpol eine gemeinsame Konferenz zur Cyberkriminalität aus⁶⁷.



Europäisches Sicherheits- und Verteidigungskolleg (ESVK)

Am Europäischen Sicherheits- und Verteidigungskolleg wird ziviles und militärisches Personal von EU-Institutionen sowie EU-Mitgliedstaaten im Bereich der Gemeinsamen Außen- und Sicherheitspolitik sowie der Gemeinsamen Sicherheits- und Verteidigungspolitik aus- und weitergebildet. Als einer von sechs Schwerpunkt-

⁶⁷ [Bundeskriminalamt, Europol.](#)

[ENISA, Advisory Group \(AG\).](#)

[EU-Lisa, MoU Europol.](#)

[Europäische Kommission, Infographic: EU Cybersecurity Ecosystem.](#)

[Europäisches Parlament und Rat der Europäischen Union, Verordnung \(EU\) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA \(Agentur der Europäischen Union für Cybersicherheit\) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung \(EU\) Nr. 526/2013 \(Rechtsakt zur Cybersicherheit\).](#)

[European Central Bank, ECRB.](#)

[European Council and Council of the European Union, The Horizontal Working Party on Cyber Issues.](#)

[Eurojust, Europol.](#)

[Europol, About Europol.](#)

[Europol, common taxonomy for law enforcement and csirts.](#)

[Europol, EMPACT.](#)

[Europol, EUCTF.](#)

[Europol, European Cybercrime Centre – EC3.](#)

[ESDC, EAB.Cyber.](#)



bereichen wird am ESVK auch Training und Kurse zu Cybersicherheit und -verteidigung angeboten. Hierzu wurde am ESVK eine Cyber Education, Training, Evaluation and Exercise (ETEE) Plattform eingerichtet.

Institutionell ist das ESVK beim EAD angesiedelt. Seine Einrichtung geht auf eine Entscheidung des Rates der EU zurück. Austausch und Arbeitsbeziehungen bestehen mit ENISA, Europol, CEPOL, ECTEG, CERT-EU sowie dem Hybrid CoE und dem NATO CCDCOE. Das ESVK greift in seiner Ausbildung auf ein weites Netzwerk EU-weiter Ausbildungseinrichtungen zurück. Von deutscher Seite beteiligen sich unter anderem das AA, die BAKS und das BMVg an diesem Netzwerk. Das ESVK wiederum ist Mitglied der Community des EU CyberNet⁶⁸.



Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC)

Das Europäische Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit soll die europäische Autonomie in der Cybersicherheit stärken sowie den digitalen Binnenmarkt und die Wettbewerbsfähigkeit der europäischen Cybersicherheitsindustrie fördern. Durch das Kompetenzzentrum, dessen Existenz vorerst bis 2029 vorgesehen ist, werden die vorhandenen Mittel für Cybersicherheit innerhalb der Europäischen Union sowie Investitionen gezielt gebündelt (Förderprogramme Horizont Europa und Digitales Europa) und Forschungsvorhaben in der EU im Bereich der Cybersicherheit koordiniert. Diese finanzieren das Netzwerk nationaler Koordinierungszentren (NCCs), mit denen das Zentrum eng zusammenarbeitet.

Das ECCC basiert auf einem Vorschlag der EK (durch GD CONNECT vorbereitet), welche gemeinsam mit den EU-Mitgliedstaaten auch durch zwei Vertreter:innen im Verwaltungsrat des ECCC repräsentiert ist. Es soll die Aufgaben der ENISA ergänzen und mit dieser in der Ausübung seiner Aufgaben zusammenarbeiten. Einer:m Vertreter:in der ENISA kommt permanenter Beobachterstatus Verwaltungsrates. Die ECSO koordiniert sich beim Aufbau des ECCO mit dem ECCC. Darüber hinaus sieht die das ECCC errichtende EU-Verordnung unter anderem kooperative Arbeitsbeziehungen mit dem EAD, der GD JRC, dem EC3 und der EVA vor. Von deutscher Seite sind Ver-

⁶⁸ [ESVK, EAB.Cyber.](#)
[ESVK, Education & Training.](#)
[ESVK, Network Members.](#)
[ESVK, Who We Are.](#)
[EU CyberNet, Stakeholder Community.](#)



treter:innen des **BSI** im **ECCC-Verwaltungsrat** repräsentiert. Das **NKCS** ergänzt als nationaler Counterpart die Aufgaben des **ECCC** auf EU-Ebene⁶⁹.



Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität (EC3)

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Euro-pol soll die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU verstärken. Das EC3 ist im Kampf gegen Cyberkriminalität in drei Bereichen tätig: Forensik, Expertise und Stakeholder Management und Operatives. Es veröffentlicht jährlich das Internet Organised Crime Threat Assessment (IOCTA), seinen strategischen Bericht zu Erkenntnissen und aufkommenden Bedrohungen sowie Entwicklungen im Bereich Cyberkriminalität. Das EC3 beherbergt die Joint Cybercrime Action Taskforce (J-CAT), deren Aufgabe es ist, informationsgeleitetes und koordiniertes Vorgehen gegen cyberkriminelle Bedrohungen mittels grenzübergreifender Ermittlungen und Einsätze durch ihre Partner zu ermöglichen.

*EC3 ist bei **Europol** angesiedelt. Partner auf europäischer Ebene sind **CERT-EU**, **CEPOL**, **Eurojust**, **ENISA**, die **EK**, die **EZB** sowie die **ECTEG**. Zwischen EC3, **EVA**, **CERT-EU** und der **ENISA** besteht ein Memorandum of Understanding zur Zusammenarbeit und Austausch im Bereich der Cybersicherheit. Gemeinsam mit der **ENISA** richtet das EC3 jährliche Workshops zur Kooperation zwischen nationalen Computer Security Incident Response Teams und Strafverfolgungsbehörden aus. Das EC3 nominiert darüber hinaus gemeinsam mit **Europol** Repräsentant:innen für die **ENISA AG**. Außerdem stellt das EC3 gemeinsam mit dem **CERT-EU** forensische Analysen und andere technische Informationen für das **CSIRTs Netzwerk** bereit. Es ist an der **TGG** beteiligt. Jährlich richten **Europol** (durch das EC3) und **Interpol** eine gemeinsame Konferenz zur Cyberkriminalität aus⁷⁰.*

69 [Amtsblatt der Europäischen Union, Verordnung \(EU\) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren. Bundesamt für Sicherheit in der Informationstechnik, Nationales Koordinierungszentrum für Cybersicherheit \(NKCS\).](#)

[EC3, The European Cybersecurity Support project \(ECCO\) has kicked off. European Cybersecurity Competence Centre and Network, About us.](#)
[European Cybersecurity Competence Center and Network, National Coordination Centers.](#)
[Europäische Kommission, European Cybersecurity Industrial, Technology and Research Competence Centre.](#)
[European Council, EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres.](#)

70 [European Agency for Cybersecurity, 10th ENISA-EC3 Workshop: CSIRTs and LE cooperation.](#)
[European Defence Agency, MoU between EDA, ENISA, EC3 and CERT-EU.](#)
[Europol, Cybercrime.](#)
[Europol, European Cybercrime Center – EC3.](#)
[Europol, EC3 Partners.](#)
[Europol, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.](#)
[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU. Official Journal of the European Union, Recommendations Commission Recommendation \(EU\) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.](#)



European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

Das Hybrid CoE hat es sich zum Ziel gesetzt, die Fähigkeiten der teilnehmenden Staaten durch die Entwicklung von Resilienz und den Aufbau zur Bekämpfung hybrider Bedrohungen zu unterstützen. In der Praxis geschieht dies konkret durch Forschung, der Durchführung von Workshops und Konferenzen sowie dem Austausch von Best Practices zwischen unterschiedlichen Stakeholdern innerhalb von drei Communities of Interest (COI). Die COI-Gruppe zu Strategie und Verteidigung wird durch Deutschland koordiniert. Das Hybrid CoE konzentriert sich auf die Cyber-Domäne und neue Optionen für hybride Aktivitäten in der Grauzone der Schnittstelle von Frieden und Krieg und befasst sich auch mit der Ausnutzung der Cyber-Domäne, sowie der Entstehung neuer und disruptiver Technologien. Innerhalb der COI Strategie und Verteidigung ist auch ein Arbeitsstrang zu Cyber Power in Hybrid Conflict/Warfare (CPH) angesiedelt. Dessen Hauptziel besteht darin, für relevante strategische Fragen und Probleme in Bezug auf Cybermacht und die Cyber-Domäne im Kontext hybrider Konflikte/Kriegsführung zu sensibilisieren, diese zu identifizieren, anzugehen und sich auf identifizierte Forschungslücken zu konzentrieren. Der CPH-Arbeitsstrang umfasst auch die Identifizierung potenzieller Interessengruppen und Mitwirkender für die Schaffung eines Netzwerks von Expert:innen – hauptsächlich aus Militär, Wissenschaft und Industrie – zu diesem Thema und veranstaltet ein jährliches „CPH-Symposium“.

*Die Idee der Einrichtung des Hybrid CoE wurde sowohl vom **Rat der EU** als auch dem **NAC** befürwortet. Zusammen mit dem **GD JRC** hat Hybrid CoE Ende 2020 einen konzeptionellen Rahmen zu hybriden Bedrohungen vorgestellt. In der Vergangenheit haben Hybrid CoE und die **EVA** eine Zusammenarbeit als Beitrag zur Umsetzung der Prioritäten aus dem Capability Development Plan der EU vereinbart. Weitere Arbeitsbeziehungen bestehen mit dem **ESVK**. Deutschland ist als eine der neun Gründungsnationen am Hybrid CoE beteiligt. Zur Bundesebene bestehen Verbindungen mit dem **BMVg**, dem **KdoCIR**, dem **BMI** und dem **AA**. Das Hybrid CoE ist an dem EU-HYBNET-Projekt beteiligt, an dem auch die **ZITiS** als Projektpartner involviert ist⁷¹.*



European Cybercrime Training and Education Group (ECTEG)

Die ECTEG setzt sich aus Strafverfolgungsbehörden der Mitgliedstaaten sowie Mitgliedsstaaten des Europäischen Wirtschaftsraums, internationalen Institutionen, der Wissenschaft, der privaten Industrie und Experten zusammen. Ihr Ziel ist es, die globale Strafverfolgung von Cyberkriminalitätsvorfällen vorzubereiten.

⁷¹ [European Centre of Excellence for Countering Hybrid Threats, About Us.](#)
[Europäische Kommission, The JRC proposes a new framework to raise awareness and resilience against hybrid threats.](#)
[Europäische Kommission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.](#)



Die ECTEG arbeitet in Abstimmung mit dem [EC3](#) und [CEPOL](#) zusammen, um Cyberkriminalitätstrainings grenzübergreifend zu harmonisieren, Wissensaustausch zu ermöglichen und eine Standardisierung von Methoden für Trainingsprogramme voranzubringen. Vertreter:innen von [Europol](#) und [CEPOL](#) sitzen zudem im Beirat des ECTEG. Weiterer Austausch besteht mit dem [ESVK](#). Aus Deutschland sind die Polizeiakademie Hessen und die Albstadt-Sigmaringen Universität beteiligt⁷².



European Cyber Security Organisation (ECSO)

Die European Cyber Security Organisation wurde in Belgien als gemeinnützige Organisation zur Implementierung der ausgelaufenen Contractual Public Private Partnership on Cybersecurity (cPPP) gegründet. Die ECSO verbindet europäische Akteure im Bereich Cybersicherheit innerhalb der EU-Mitgliedsstaaten, so beispielsweise Forschungszentren, aber auch Unternehmen, Endnutzer und Mitgliedsstaaten des Europäischen Wirtschaftsraums. Zielsetzungen der ECSO sind die Entwicklung eines kompetitiven europäischen Ökosystems, die Unterstützung beim Schutz des European Digital Single Market mit vertrauenswürdigen Cybersicherheitslösungen und eine Beitragsleistung zur digitalen Autonomie der Europäischen Union.

Die ECSO ist Partner der [EK](#) und unterhält Arbeitsbeziehungen mit Repräsentant:innen aus [GD CONNECT](#), [GD RTD](#), [GD JRC](#), [GD DIGIT](#) sowie dem [EAD](#). Auf Einladung der jeweiligen EU-Ratspräsidentschaft wird ECSO regelmäßig eingeladen, über den aktuellen Stand seiner Arbeit gegenüber der [HWPCI](#) Bericht zu erstatten. Die ECSO ist Mitglied der [ECCG](#). Kontinuierliche Kooperationen bestehen zudem unter anderem mit der [ENISA](#), [Europol](#), [CEN](#), [CENELEC](#) sowie der [EVA](#). Auch das [BSI](#) ist Mitglied der ECSO Boards. Sie arbeitet mit der [ITU](#) zusammen und hat diese beispielsweise bei der Erstellung des [GCI](#) unterstützt. Die ECSO leitet zudem die strategischen Unterstützungsmaßnahmen für die Entwicklung der Europäischen Cybersicherheitsgemeinschaft (ECCO) im Rahmen der [ECCC-Verordnung](#)⁷³.



European Government CERTs group (EGC group)

Die European Government CERTs group ist ein informeller Zusammenschluss von derzeit 13 Regierungs-CERTs in Europa, deren Mitglieder im Bereich der Incident Response zusammenarbeiten, indem sie auf gegenseitigem Vertrauen und Ähnlichkeiten gemeinsame Maßnahmen zur Bewältigung von Cybersicherheitsvorfällen entwickeln. Zudem identifiziert sie Bereiche für gemeinsame Forschung und Ent-

⁷² [ECTEG, European Cybercrime Training and Education Group. ECTEG, Members.](#)
[ESDC, EAB.Cyber.](#)

⁷³ [ECSO, About ECSO.](#)
[ECSO, Membership.](#)
[ECCO, European Cybersecurity Community Support project.](#)
[ECSO, Board of Directors.](#)
[LinkedIn, European Cyber Security Organisation \(ECSO\).](#)



wicklung als auch Wissen in Spezialgebieten zur gemeinsamen Nutzung. Darüber hinaus ist der EGC group die Erleichterung des Informations- und Technologieaustauschs unter anderem im Bereich von Schwachstellen ein Anliegen. Dabei verfolgt die Gruppe, die dreimal jährlich zusammenkommt, einen technischen Fokus und befasst sich nicht mit der Formulierung von Policies.

Die EU ist durch das **CERT-EU** repräsentiert und deutsches Mitglied ist das **CERT-Bund**. Darüber hinaus besteht eine Kooperation mit der **ENISA**⁷⁴.



European Judicial Network (EJN)

Das European Judicial Network wurde durch den Rat der Europäischen Union als ein Netzwerk von nationalen Kontaktstellen zur Erleichterung der justiziellen Zusammenarbeit in strafrechtlichen Angelegenheiten, insbesondere der Bekämpfung von Formen der schweren Kriminalität, geschaffen. Hierzu organisiert das EJN Schulungsveranstaltungen, stellt Informationen bereit und ist bei der Herstellung von Kontakten zwischen den zuständigen Behörden behilflich.

Das Sekretariat des EJN ist bei **Eurojust** angesiedelt und es besteht eine Kooperation mit dem **EJCN**⁷⁵.



European Judicial Cybercrime Network (EJCN)

Das European Judicial Cybercrime Network soll Kontakte zwischen verschiedenen Akteuren, die eine Rolle im Erhalt der Rechtsstaatlichkeit im Cyberraum spielen, stärken, um die Effizienz von Ermittlungen und Strafverfolgungen zu erhöhen.

Eurojust ist im Board des **EJCN** beteiligt, veranstaltet die regelmäßigen **EJCN** Treffen und befragt das **EJCN** zur Policy-Entwicklung und anderen Stakeholder-Aktivitäten um einen regen Austausch zwischen **Eurojust**'s Expertise im Bereich internationaler juristischer Kooperation und der operativen und Sachgebietsexpertise der **EJCN** Mitgliedern zu gewährleisten. Es besteht zudem eine Kooperation mit dem **EJN**. Die **ZIT** ist Gründungsmitglied im **EJCN**⁷⁶.



European Judicial Training Network (EJTN)

Das European Judicial Training Network verantwortet als Plattform Fortbildung und Wissensaustausch der europäischen Justiz.

⁷⁴ [Bundesamt für Sicherheit in der Informationstechnik, Europäische CERTs in Bonn. EGC Group, Contact.](#)

[EGC Group, European Government CERTs \(EGC\) group.](#)

⁷⁵ [European Judicial Network, About EJN.](#)

[European Judicial Network, Network Atlas.](#)

⁷⁶ [Eurojust, Cybercrime.](#)

[Eurojust, European Judicial Cybercrime Network.](#)

[Staatsanwaltschaften Hessen, Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität \(ZIT\).](#)



Das EJTN arbeitet im Bereich Cybersicherheit mit **CEPOL** an den dort angebotenen Trainings sowie mit der **EK** zusammen. Auf der Basis eines MoU kooperiert EJTN zudem mit **Eurojust**, beispielsweise im Rahmen eines Austauschprogramms, bei dem praktizierende Richter und Staatsanwälte zu Eurojust abgeordnet werden⁷⁷.



European Multidisciplinary Platform Against Criminal Threats (EMPACT)

EMPACT ist eine europäische Initiative zur Ermittlung und Bekämpfung von Bedrohungen, die ihren Ursprung in organisierter und schwerer Kriminalität haben. Zu diesem Ziel soll u.a. durch Austausch von Informationen oder kriminalpolizeilichen Erkenntnissen, verstärkter Kooperation sowie im Rahmen von EMPACT koordinierter Maßnahmen beigetragen werden. An EMPACT beteiligt sind alle EU-Mitgliedsstaaten, EU-Organisationen sowie bei Bedarf auch Drittstaaten, internationale Organisationen oder weitere Akteure. Bedrohungen aus dem Cyberraum gehören zu den Prioritäten des EMPACT-Zyklus 2022–2025. In der Vergangenheit wurde im Rahmen von EMPACT beispielsweise der Takedown von Emotet oder VPN-Anbietern durchgeführt.

An EMPACT sind von EU-Seite u.a. die **EK**, **Europol**, **Eurojust**, **CEPOL**, **ENISA** und **eu-LISA** beteiligt⁷⁸.



European Union Cybercrime Task Force (EUCTF)

Die European Union Cybercrime Task Force wurde von Europol gemeinsam mit der Europäischen Kommission und den Mitgliedsstaaten aufgebaut. Sie ist ein vertrauensbasiertes Netzwerk, das halbjährig zusammentritt.

Mitglieder sind die Nationalen Cybercrime Einheiten der Mitgliedstaaten, Vertreter:innen von **CEPOL**, der **EK**, **Eurojust** und **Europol**. Gemeinsam mit **CEPOL**, **Eurojust**, **Europol** und **GD HOME** werden bei den Treffen Herausforderungen und Aktionen im Kampf gegen Cyberkriminalität identifiziert, diskutiert und priorisiert. Die EUCTF ist gemeinsam mit der **ENISA**, **CERT-EU** und **EC3** an der **TGG** beteiligt⁷⁹.

⁷⁷ [Emailaustausch mit CEPOL-Vertreter:innen im August 2019.](#)

[EJTN, About us.](#)

[Eurojust, EJTN.](#)

⁷⁸ [Europäische Kommission, EMPACT fighting crime together.](#)

[Europol, Coordinated action cuts off access to VPN service used by ransomware groups.](#)

[Europol, EU Policy Cycle – EMPACT.](#)

[Europol, World's most dangerous malware EMOTET disrupted through global action.](#)

[Rat der Europäischen Union, EMPACT Terms of Reference.](#)

[Rat der Europäischen Union, General Factsheet – Operational Action Plans \(OAPS\): 2020 Results.](#)

⁷⁹ [ENISA, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.](#)

[Europol, EUCTF.](#)



Gemeinsame Forschungsstelle (GD JRC)

Die Gemeinsame Forschungsstelle ist der Europäischen Kommission unterstellt. Die JRC stellt nationalen Behörden als auch Behörden der EU wissenschaftliche Erkenntnisse und innovative Instrumente während des gesamten Politikzyklus bereit. Dabei möchte es aufkommende Herausforderungen antizipieren und die Folgen verschiedener politischer Entscheidungen aufzeigen. Als einer von zehn Wissenschaftsbereichen wird am JRC auch zur „Information Society“ in 16 Forschungsthemen, beispielsweise zu Cybersicherheit und dem digitalen Binnenmarkt, geforscht.

Gemeinsam mit dem [Hybrid CoE](#) hat die Gemeinsame Forschungsstelle 2020 einen konzeptionellen Rahmen zu hybriden Bedrohungen vorgestellt. Weitere Arbeitsbeziehungen bestehen mit [GD RTD](#) und der [ECSO](#). GD JRC gehört zu den „Institutional Stakeholder“ des [CEN](#). Es gehört zu den Teilnehmer:innen der [CSCG](#). GD JRC ist am [EU-HYBNET](#)-Projekt beteiligt, an dem unter anderem auch [ZITiS](#) und ein Institut der [UniBw](#) als Projektpartner beteiligt sind⁸⁰.



Generaldirektion Forschung und Innovation (GD RTD)

Die Generaldirektion Forschung und Innovation der Europäischen Kommission verantwortet die Forschungs- und Innovationspolitik der Europäischen Union, um Wissenschaft, Technologie und Innovation im Sinne der Prioritäten der EK zu fördern und zu stärken. Hierzu analysiert es beispielsweise die nationalen Forschungs- und Innovationspolitiken der EU-Mitgliedstaaten, um deren Effektivität und Effizienz zu steigern und gibt bei Bedarf länderspezifische Empfehlungen ab.

In der Erfüllung seiner Aufgaben arbeitet GD RTD unter anderem mit [GD CONNECT](#), [GD HOME](#), [GD JRC](#) und der [ECSO](#) zusammen⁸¹.



Generaldirektion Informatik (GD DIGIT)

Die Generaldirektion Informatik ist für die IT-Sicherheit der Systeme der Kommission zuständig. Es ist für einen IT-Betrieb, der andere Kommissionsabteilungen und EU-Institutionen bei der täglichen Arbeit unterstützt sowie für eine verbesserte Zusammenarbeit zwischen den Verwaltungen der Mitgliedstaaten, verantwortlich.

Gemeinsam mit der:dem Direktor:in von [GD CONNECT](#), repräsentiert der:die Direktor:in von [GD DIGIT](#) die [EK](#) im Management sowie Executive Board der [ENISA](#). Arbeitsbeziehungen bestehen mit der [ECSO](#) sowie dem [ICTAC](#), an dessen Meetings auch ein:e Vertreter:in [GD DIGIT](#)'s teilnimmt. [CERT-EU](#) ist institutionell bei [GD DIGIT](#) angesiedelt.

80 [EU Science Hub, Information Society \(Webseite entfernt\)](#).
[EU Science Hub, JRC in brief](#).
[EU Science Hub, Organisation](#).
[EU Science Hub, Research Topics](#).

81 [Europäische Kommission, Strategic Plan 2016–2020: Directorate-General for Research and Innovation](#).



Gemeinsam arbeiten sie an einem IT-Sicherheitsprogramm zum Schutz der EK vor Cyberbedrohungen⁸².



Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD CONNECT)

Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien ist verantwortlich für die Entwicklung und Umsetzung der EK-Politik in den Bereichen Digitale Wirtschaft („digitaler Binnenmarkt“) und Gesellschaft, sowie Forschung und Entwicklung. Hierzu fördert es u.a. ausgewählte „kritische Digitaltechnologien“ und strebt eine europäische Führungsposition in den Bereichen Datenwirtschaft und Cybersicherheit an.

GD CONNECT ist die zuständige Generaldirektion für die ENISA und übernimmt die Repräsentation auf Generaldirektions-Ebene im CERT-EU Board. Je nach Sicherheitsvorfall kann GD CONNECT die federführende Dienststelle des ERCC sein. Arbeitsbeziehungen bestehen mit GD RTD und der ECSO. Der Vorschlag zur Einrichtung des ECCC seitens der Europäischen Kommission wurde von GD CONNECT vorbereitet, welche dessen Arbeit auch weiter unterstützt. GD CONNECT gehört zu den Teilnehmer:innen der CSCG⁸³.



Generaldirektion Migration und Inneres (GD HOME)

Die Generaldirektion Migration und Inneres arbeitet zu Migration und Asyl sowie innerer Sicherheit. Zu letzterem Bereich gehören der Kampf gegen organisierte Kriminalität und Terrorismus, polizeiliche Kooperation, die Organisation der EU-Außengrenzen sowie federführend auch Cyberkriminalität. Zur Bekämpfung von Cyberkriminalität arbeitet GD HOME beispielsweise gemeinsam mit EU-Mitgliedstaaten an der Sicherstellung der vollständigen Umsetzung bestehender EU-Gesetzgebung und ist für ihre Anpassung an aktuelle Entwicklungen verantwortlich. Zur Generaldirektion gehört zudem das Strategic Analysis and Response Center (STAR), welche Informationen und Einschätzungen, insbesondere Risikoanalysen, zur Verfügung stellt, um die Formulierung von Policies sowie Krisenmanagement, Lagekenntnis und Kommunikation zu unterstützen.

Diese werden mit Kommissionsdiensten, dem EAD und relevanten Agenturen (bspw. Europol) ausgetauscht. Arbeitsbeziehungen bestehen unter anderem mit eu-LISA, GD RTD, Europol, CEPOL sowie Interpol. GD HOME gehört zu den Teilnehmer:innen der CSCG⁸⁴.

⁸² [Europäische Kommission, Generaldirektion Informatik \(DIGIT\).](#)

[Europäische Kommission, Informatics.](#)

[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.](#)

⁸³ [Deutsches Institut für Normung, Cyber Security Coordination Group \(CSCG\).](#)

[European Commission, Strategic Plan 2020-2024 DG Communications Networks, Content and Technology.](#)

[Europäische Kommission, Annual Activity Report: DG CONNECT.](#)

[Europäische Kommission, Communication Networks, Content and Technology.](#)

⁸⁴ [Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#) [European Commission, Policies.](#)

[Europäische Kommission, Strategic Plan 2016–2020: DG Migration and Home Affairs.](#)



Gruppe der Interessenträger für die Cybersicherheitszertifizierung (SCCG)

Mit Inkrafttreten des Cybersecurity Acts wurde eine Gruppe der Interessenträger:innen für Cybersicherheitszertifizierung eingesetzt, die der ENISA und der Kommission den Zugang zu Interessenträg:innen erleichtert. Die Gruppe besteht aus sachverständigen Vertreter:innen der Interessenträger:innen, beispielsweise Anbieter digitaler Dienste oder nationaler Akkreditierungsstellen, die von der Europäischen Kommission auf Vorschlag der ENISA gewählt werden.

*Die Gruppe der Interessenträger:innen soll die **EK** bei Fragen im Zusammenhang mit dem EU-Rahmen für die Cybersicherheitszertifizierung, sowie bei der Erarbeitung des in Art. 47 aufgeführten fortlaufenden Arbeitsprogramms unterstützend agieren. Auf Ersuchen kann die Gruppe die **ENISA** bezüglich ihrer Aufgaben hinsichtlich des Marktes, der Zertifizierung und der Normung beraten. Den Vorsitz haben Vertreter:innen der **EK** und der **ENISA** gemeinsam inne. Die Sekretariatsfunktionen werden von der **ENISA** wahrgenommen. Sie arbeitet mit der **ECCG** zusammen. Mitglieder der **SCCG** sind unter anderem **CEN**, **CENELEC**, **ETSI**, **ISO**, **ITU**, **IEC**, **ECSO** und die **EA**⁸⁵.*



Horizontale Ratsarbeitsgruppe „Fragen des Cyberraums“ (HWPCI)

Die Horizontale Ratsarbeitsgruppe „Fragen des Cyberraums“ koordiniert die Arbeit des Rates der EU zu Cyberpolitik und der dazugehörigen Gesetzgebung. Die Aufgaben und Ziele der Arbeitsgruppe umfassen unter anderem die Vereinheitlichung bestehender Ansätze der europäischen Cybersicherheitspolitik, die Verbesserung des Informationsaustausches zu Cyber-Themen zwischen EU-Mitgliedsstaaten sowie die Festlegung von einheitlichen Prioritäten und strategischen Zielsetzungen der Cybersicherheitspolitik innerhalb der EU. Sie ist dabei sowohl in gesetzgebende als auch exekutive Prozesse eingebunden.

*Die HWPCI ist ein Vorbereitungsgremium des **Rates der EU**. Sie kann im Einzelfall beispielsweise Sitzungen des **PSK** vorbereiten. Die HWPCI arbeitet mit der **EK**, dem **EAD**, **Eurojust**, der **EVA** sowie der **ENISA** zusammen und steht zudem im Austausch mit anderen Arbeitsgruppen. Der:die Vorsitzende:r der HWPCI ist als unterstützende:r Teilnehmer:in der **JCU** vorgesehen. **ECSO** erstattet der HWPCI regelmäßig Bericht über den aktuellen Stand seiner Arbeit. An der HWPCI beteiligt sich Deutschland durch Vertreter:innen des **BMI** und des **AA**. Die letzte **UN GGE** hat im Rahmen der HWPCI auch eine regionale Konsultation mit EU-Mitgliedsstaaten geführt⁸⁶.*

⁸⁵ [Europäisches Parlament und Rat der Europäischen Union, Verordnung \(EU\) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA \(Agentur der Europäischen Union für Cybersicherheit\) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung \(EU\) Nr. 526/2013 \(Rechtsakt zur Cybersicherheit\). Stakeholder Cybersecurity Certification Group members.](#)

⁸⁶ [Amtsblatt der Europäischen Union, Empfehlung \(EU\) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.](#) Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheit in Europa gestalten. (Webseite entfernt) [Deutscher Bundestag \(Drucksache 19/11920\), Antwort der Bundesregierung auf die Kleine Anfrage: Beteiligung der Bundesregierung an Cybersicherheitsformaten.](#) [European Commission, Factsheet: Joint Cyber Unit.](#) [Europäischer Rat, Horizontal Working Party on Cyber Issues \(HWP\).](#) [The Council of the European Union, Establishment of a Horizontal Working Group on Cyber Issues.](#)



ICT Advisory Committee of the EU Agencies (ICTAC)

Das zweimal im Jahr zusammenkommende ICT Advisory Committee von EU-Institutionen soll als Forum zum Austausch von Best Practices, Erfahrungen und Wissen beitragen und dadurch die institutionsübergreifende Zusammenarbeit im IKT-Bereich auf der Basis gemeinsamer Interessen fördern. Es sieht einen Mechanismus vor, um gemeinsame Positionen zu erarbeiten und möchte zur Kooperation untereinander beispielsweise durch gemeinsame Nutzung von Ressourcen und bewährten Verfahren bei der Entwicklung, Wartung oder Einrichtung neuer IKT-Systeme beitragen. In der Vergangenheit hat das ICTAC zudem eine Cybersicherheitsübung (ICTAC Ex) organisiert, um zu verbesserter Zusammenarbeit und Informationsaustausch beizutragen.

*ICTAC setzt sich aus den für IKT zuständigen Leiter:innen innerhalb von EU-Institutionen, Exekutivagenturen und anderen Einrichtungen zusammen. Beteiligt sind unter anderem **CEPOL**, das **CERT-EU**, die **ENISA**, **Europol** und die **EVA**. Es steht in permanentem Austausch mit **GD DIGIT**, von der auch ein:e Vertreter:in an den Meetings von ICTAC teilnimmt⁸⁷.*



Institut der Europäischen Union für Sicherheitsstudien (EUISS)

Das Institut der Europäischen Union für Sicherheitsstudien leistet Forschungs- und Policy-Analysearbeiten im Bereich der Gemeinsamen Außen- und Sicherheitspolitik und soll so zu ihrer Implementierung beitragen. EUISS publiziert regelmäßig zu Fragen der Außen-, Sicherheits- und Verteidigungspolitik, organisiert Veranstaltungen und führt Kommunikationstätigkeiten in diesem Bereich durch. Zu dem Themenportfolio von EUISS gehört auch der Bereich Cybersicherheit, Cyber-Diplomatie sowie Cyber Capacity Building.

*EUISS wurde vom **Rat der EU** etabliert und arbeitet beispielsweise mit der **EK**, dem **EAD** und Regierungen der EU-Mitgliedsstaaten zusammen. Es ist Mitglied der Community des **EU CyberNet**. Der Verwaltungsrat setzt sich aus Vertreter:innen der Mitgliedsstaaten, sowie dem:der hohen Vertreter:in der EU für Außen- und Sicherheitspolitik als Repräsentant:in der EK zusammen. Beaufsichtigt wird das EUISS vom **PSK**⁸⁸.*

⁸⁷ [European Union Agency for Cybersecurity, Cybersecurity exercise boosts preparedness of EU Agencies to respond to cyber incidents.](#)

[ICTAC, ICTAC Annual Report 2018.](#)

[ICTAC, Terms of Reference of the Network of Heads of ICT of the European Agencies \(ICTAC\).](#)

[ICTAC, ICTAC Work Programme 2019–2020.](#)

⁸⁸ [EU CyberNet, Stakeholder Community.](#)

[EUR-Lex, Document 32001E0554.](#)

[EUR-Lex, Institut der Europäischen Union für Sicherheitsstudien.](#)

[EUR-Lex, Beschluss 2001/298/GASP des Rates vom 7. April 2008 zur Änderung des Beschlusses 2001/80/GASP zur Einsetzung des Militärstabs der Europäischen Union.](#)

[Europäische Union, Institut der Europäischen Union für Sicherheitsstudien \(EUISS\).](#)

[European Union External Action Service, Cyberspace: Strengthening cooperation in promoting security and stability.](#)

[European Union Institute for Security Studies, Organisational Chart.](#)

[European Union Institute for Security Studies, Cyber.](#)



Intelligence Directorate des EU-Militärstabs (EUMS INT)

Das Intelligence Directorate des EU-Militärstabs, hauptsächlich bestehend aus nationalen Expert:innen der EU-Mitgliedsstaaten, ist organisatorisch beim EAD aufgehängt. Basierend auf eingestufteten Informationen aus EU-Mitgliedstaaten oder EU-Einsatzgebieten stellt es militärische Lageanalysen und -bewertungen zur Frühwarnung, für den Entscheidungsprozess sowie der Planung von zivilen Einsätzen und militärischen Operationen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik zur Verfügung. Das EUMS INT trägt so zu den Kernaufgaben des EUMS, Frühwarnung, Lagebeurteilung und strategischer Planung bei. Der EUMS stellt militärisches Fachwissen innerhalb des Europäischen Auswärtigen Dienstes (EAD) zur Verfügung.

EUMS INT ist als Abteilung des EUMS im EAD angesiedelt und arbeitet mit dem zivilen Lagezentrum INTCEN im Rahmen des Einheitlichen Analyseverfahrens (SIAC) sowie der EU Hybrid Fusion Cell zusammen. SIAC fungiert als Zentrum zur Generierung strategischer Informationen, Frühwarnungen und umfassender Analysen, die sowohl EU-Gremien als auch Entscheidungsträgern in den Mitgliedsstaaten zur Verfügung gestellt werden. Seine Produkte stellt das EUMS INT (teils gemeinsam mit dem INTCEN) dem BMVg, dem AA, dem BND, sowie dem deutschen militärischen Vertreter bei der EU zur Verfügung⁸⁹.



Inter-Service Group „Community Capacity in Crisis-Management“ (ISG C3M)

Diese Inter-Service Gruppe ist als Netzwerk ausgelegt, welches regelmäßig alle Kommissionsdienste und EU-Agenturen, die im Krisenmanagement tätig sind, zusammenbringt, um Awareness zu stärken, Synergien zu identifizieren und Informationen auszutauschen. Die Gruppe fungiert dabei als Netzwerk der Kontaktpunkte aller operativen Krisen- und Lagezentren.

Der EAD ist bei der ISG C3M beteiligt⁹⁰.



Inter-Service Group „Countering Hybrid Threats“ (ISG CHT)

Die Inter-Service Gruppe zu „Countering Hybrid Threats“ soll im Bereich der hybriden Gefährdungen für eine umfassende Herangehensweise sorgen und überwacht Fortschritte der Aktivitäten, die in JOIN (2016)¹⁸ vorgesehen sind. Die Gruppe tagt vierteljährlich.

⁸⁹ [Deutscher Bundestag \(Drucksache 19/489\), Antwort der Bundesregierung auf die Kleine Anfrage: Pläne der Europäischen Kommission für eine geheimdienstliche „Europäische Aufklärungseinheit“.](#)
[Pia Seyfried, Red Herring & Black Swan: Five Eyes for Europe.](#)

[Europäisches Parlament, Parlamentarische Anfragen: Antwort von Frau Catherine Ashton – Hohe Vertreterin/Vizepräsidentin im Namen der Kommission.](#)

[Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik.](#)

⁹⁰ [Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#)



Den Vorsitz der ISG CHT haben sowohl Repräsentant:innen des *EAD* als auch der *EK* auf Generaldirektor:innen oder stv. Generaldirektor:innen-Ebene inne. Die ISG CHT erhält quartalsweise Berichte der *EU Hybrid Fusion Cell*⁹¹.



Joint Cyber Unit (JCU)

Zur Etablierung der in der EU-Cybersicherheitsstrategie vorgesehenen Joint Cyber Unit hat die EK einen Vorschlag gemacht. Bis Juni 2023 soll die JCU ihre volle Einsatzbereitschaft erreicht haben. Sie soll als physische und virtuelle Plattform die Zusammenarbeit zwischen EU-Institutionen und Behörden in EU-Mitgliedsstaaten auf technischer und operativer Ebene stärken, um Cyberoperationen zu verhindern, diese abzuschrecken sowie darauf in koordinierter Weise reagieren zu können. Um diese koordinierte Reaktion auf und Wiederherstellung nach Vorfällen gewährleisten zu können, soll die JCU unter anderem EU Cybersecurity Rapid Reaction Teams aufstellen und ein Verzeichnis aller innerhalb der EU verfügbaren operativen und technischen Kapazitäten erstellen und dieses kontinuierlich aktualisieren. Zudem soll auch gegenüber diesen Vorfällen bereits im Vorfeld das gemeinsame Situationsbewusstsein sowie die gemeinsame Vorbereitung verbessert werden. Hierzu soll die JCU unter anderem einen Integrated EU Cybersecurity Situation Report sowie im Einklang mit und basierend auf entsprechenden nationalen Plänen einen EU Cybersecurity Incident and Crisis Response Plan entwickeln und einen mehrjährigen Plan zur Koordinierung von Cybersicherheitsübungen erstellen. Die Zusammenarbeit aller Teilnehmer soll via Memoranda of Understandings festgehalten werden und auch die gegenseitige Unterstützung miteinschließen. Als letzten vorgesehenen Schritt ihrer Operationalisierung soll die JCU auch operative Kooperationsvereinbarungen mit Unternehmen aus dem Privatsektor anstreben, um den Austausch von Informationen zu gewährleisten.

Die JCU soll in Brüssel neben der *ENISA* und dem *CERT-EU* angesiedelt werden. Als operative Teilnehmer der JCU sieht der *EK*-Vorschlag die *ENISA*, *EuroPol*, das *CERT-EU*, den *EAD* (mit *INTCEN*), das *CSIRTs Netzwerk*, *CyCLONe* sowie unterstützend die Vorsitzenden der *NIS Cooperation Group* und der *HWPCI*, die *EVA* und ein:e Vertreter:in von relevanten *PESCO*-Projekten vor⁹².



Kontaktgruppe zum Schutz Kritischer Infrastrukturen (SKI-Kontaktgruppe)

Die Kontaktgruppe zum Schutz Kritischer Infrastrukturen ist für die strategische Koordinierung und Kooperation im Bereich des Europäischen Programmes für den

91 [Kristine Berzina et al., European Policy Blueprint for Countering Authoritarian Interference In Democracies: Annex A. European Efforts To Counter Disinformation.](#)

92 [Europäische Kommission, EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents.](#)

[Europäische Kommission, Factsheet: Joint Cyber Unit.](#)

[Europäische Kommission, Recommendation on building a Joint Cyber Unit.](#)



Schutz Kritischer Infrastrukturen (EPSKI) zuständig. Dieses identifiziert europäische Kritische Infrastrukturen und den Bedarf zu deren verbessertem Schutz. Das Programm sieht außerdem Unterstützung für die Mitgliedstaaten beim Schutz von nationalen Kritischen Infrastrukturen vor.

*Die Kontaktgruppe bringt die SKI-Kontaktpunkte der Mitgliedstaaten unter dem Vorsitz der **EK** zusammen. Jedes EU-Mitglied entsendet dabei einen SKI-Kontaktpunkt, der alle SKI-Themen mit den anderen Mitgliedstaaten, der **EK** und dem **Rat der EU** koordiniert⁹³.*



Kooperationsgruppe unter der NIS-Richtlinie (NIS Cooperation Group)

Durch die NIS-Richtlinie wurde eine Kooperationsgruppe unter dem Vorsitz der EU-Ratspräsidentschaft eingerichtet, die Repräsentant:innen der Mitgliedstaaten, der Kommission (welche als Sekretariat der Gruppe fungiert) und der ENISA zusammenbringt, die sich regelmäßig trifft. Von den EU-Mitgliedstaaten wird hierfür eine nationale Kontaktstelle benannt. Die Kooperationsgruppe agiert auf Grundlage der Konsensbildung und kann Untergruppen einrichten, die mit seiner Aufgabe verbundene, spezifische Fragen erörtern. Die Gruppe arbeitet auf der Grundlage zweijähriger Arbeitsprogramme. Ihre Hauptaufgabe liegt darin, die Arbeit der Mitgliedstaaten zur einheitlichen Umsetzung der NIS-Richtlinie durch strategische Kooperation und Informationsaustausch zwischen den Mitgliedsländern zu unterstützen. Hierfür erarbeitet die Gruppe unverbindliche Leitlinien für EU-Mitgliedstaaten und unterstützt diese zudem beim Kapazitätsaufbau.

*Operativ wird die Gruppe durch das ihr unterstellte **CSIRTs Netzwerk** unterstützt, für deren Aktivitäten die Gruppe die strategischen Leitlinien vorgibt. **ENISA** unterstützt die Gruppe unter anderem durch Identifizierung von bewährten Praktiken in der Umsetzung der NIS-Richtlinie oder bei der Stärkung des vorgesehenen Meldeprozesses für Cybersicherheitsvorfälle innerhalb der EU durch Erarbeitung von Schwellenwerten, Vorlagen und Tools. Auf Initiativen von Mitgliedern der Gruppe gehen unter anderem die Cybersicherheitsübung **Blue OLEx** (deutsche Beteiligung durch **BMI** und **BSI**) sowie **CyCLONe** zurück. Der/die Vorsitzende:r der NIS Cooperation Group zählt zu den designierten unterstützenden Teilnehmer:innen der **JCU**. Jährlich erstattet das **BSI** der NIS Cooperation Group Bericht, u.a. zu Zahl und Art gemeldeter Sicherheitsvorfälle⁹⁴.*

93 [Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection.](#)

94 [Europäische Kommission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.](#)
[Europäische Kommission, NIS Cooperation Group.](#)
[European Union Agency for Cybersecurity, NIS Directive.](#)



MeliCERTes

MeliCERTes ist eine Cybersecurity Core Service Plattform für Computer Emergency Response Teams in der EU und hat das Ziel die operative Kooperation und den Informationsaustausch zwischen ihnen zu stärken. Ihr Fokus liegt dabei auf der Erleichterung von grenzüberschreitender Kooperation zwischen ad hoc Gruppen von CERTs, die einer gegenseitigen vertrauensbasierten Zusammenarbeit, beispielsweise zum Datenaustausch, zustimmen. Die aktuelle Version von MeliCERTes arbeitet mit Open Source Tools, die von den Teams entwickelt und in Stand gehalten werden und es erlaubt, jegliche Funktionen, die von den CERTs durchgeführt werden, vom Vorfallsmanagement bis zur Gefahrenanalyse, umzusetzen.

ENISA hostet die ursprüngliche MeliCERTes-Plattform. Diese wird aktuell von einem Konsortium, u.a. bestehend aus fünf nationalen CERTs von EU-Mitgliedsstaaten, in Kooperation mit ENISA weiterentwickelt⁹⁵.



Militärausschuss der Europäischen Union (EUMC)

Der Militärausschuss der Europäischen Union verantwortet die Leitung sämtlicher militärischer Aktivitäten innerhalb der Europäischen Union (beispielsweise GSVP-Missionen) und ist für das Politische und Sicherheitspolitische Komitee in Verteidigungsfragen beratend sowie durch die Aussprache von Empfehlungen tätig. Dem EUMC gehören die Generalstabschefs der EU-Mitgliedstaaten (CHOD's) an, die wiederum durch ihre militärischen Delegierten vertreten werden.

Zusätzlich zu Beratungsaufgaben für das PSK, legt der EUMC die militärischen Leitvorgaben für den EU-Militärstab (EUMS) vor, welcher demnach die operationelle Umsetzung der GSVP verantwortet. Der Vorsitzende des EUMC (CEUMC) wird durch den Rat der EU ernannt und nimmt an Sitzungen des PSK sowie des NATO-Militärausschusses teil. Zwischen EUMC und NATO MC finden regelmäßige Treffen statt. Zudem ist der CEUMC an Sitzungen des Rates der EU beteiligt, sofern Themen mit Verteidigungsbezug diskutiert werden⁹⁶.



Politisches und Sicherheitspolitisches Komitee (PSK)

Das Politische und Sicherheitspolitische Komitee ist für die Gemeinsame Außen- und Sicherheitspolitik der EU (GASP) zuständig. Regulär tritt es zweimal wöchentlich, bei Bedarf auch häufiger zusammen. Das PSK beobachtet internationale Lageentwicklungen und verantwortet die politische Kontrolle sowie strategische Leitung von Einsätzen zur Krisenbewältigung. Das PSK ist in der Entscheidungsfindung von allen cyberbezogenen diplomatischen Maßnahmen involviert.

⁹⁵ [ENISA, Open platform and tools to facilitate the collaboration among Computer Security Incident Response Teams. Europäische Kommission, Tools and capacity building for better cyberspace monitoring, analysis and threat detection for Lithuania and EU.](#)

⁹⁶ [Amtsblatt der Europäischen Gemeinschaften, Beschluss des Rates vom 22. Januar 2001 zur Einsetzung des Militärausschusses der Europäischen Union. Europäischer Auswärtiger Dienst, European Union Military Committee \(EUMC\).](#)

Es setzt sich aus den Botschafter:innen der Mitgliedstaaten in Brüssel bzw. Vertreter:innen der Außenministerien, von deutscher Seite entsendet durch das AA, zusammen. Vertreter:innen des EAD haben den Vorsitz im PSK inne. Dem Rat der EU kann das PSK Empfehlungen zu strategischen Konzepten sowie politischen Optionen aussprechen. Der Vorsitzende des EUMC nimmt an Sitzungen des PSK teil. EU CyberNet hat das PSK zur Implementierung der EU-Cybersicherheitsstrategie gebrieft. Das PSK beaufsichtigt das EUISS. Das PSK kommt zu regelmäßigen Treffen mit dem Nordatlantikrat der NATO zusammen und erhält zudem periodische Briefings durch den:die NATO-Generalsekretär:in (oder Vertreter:in) sowie den:der SACEUR (ACO)⁹⁷.



Rat der Europäischen Union (Council)

In erster Linie sind die EU-Mitgliedstaaten für ihre eigene Cybersicherheit zuständig. Im Rat der Europäischen Union (zur Differenzierung vom Europäischen Rat auch oftmals nur „Rat“ genannt) koordinieren sie ihre Politik auf EU-Ebene. Der Rat, der auf Ebene der für ihren Politikbereich auf nationaler Ebene zuständigen Minister:innen tagt, kommt in zehn thematischen Konfigurationen – wie beispielsweise Auswärtige Angelegenheiten, Justiz und Inneres oder Wirtschaft und Finanzen – zusammen. Der Ratsvorsitz rotiert halbjährlich unter den EU-Mitgliedstaaten. Der Rat ist an dem EU-Gesetzgebungsprozess beteiligt und kann auch selbst EU-Rechtsakte erlassen. Darüber hinaus verantwortet der Rat die Umsetzung der Gemeinsamen Außen- und Sicherheitspolitik der EU auf Grundlage der im Europäischen Rat getroffenen Beschlüsse und Vorgaben. Im Falle einer EU-weiten Krise, die den Bereich der Cybersicherheit betrifft, übernimmt der Rat die Koordinierung auf der politischen Ebene der EU unter Bezug auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR). Hierbei kann er auch auf den informellen runden Tisch zurückgreifen, dem Vertreter:innen der Kommission, des Europäischen Auswärtigen Dienstes, der EU-Agenturen und der am meisten betroffenen Mitgliedstaaten, sowie Expert:innen oder Mitglieder des Kabinetts der:des Präsidenten:in des Europäischen Rates beiwohnen können. Der Rat hat außerdem zahlreiche Gremien für Koordinierung und Informationsaustausch und zur Vorbereitung der Zusammenkünfte der Minister eingerichtet, wozu auch die Horizontale Ratsarbeitsgruppe „Fragen des Cyberraums“ (HWPCI) oder der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der Inneren Sicherheit (COSI) gehören. Letzterer soll die operative Zusammenarbeit unter den EU-Mitgliedstaaten beispielsweise im Bereich der Strafverfolgung oder dem Grenzschutz stärken.

Der Rat kann die EK mit der Verhandlung internationaler Abkommen beauftragen, über deren Abschluss der Rat basierend auf einem Vorschlag der EK entscheidet.

⁹⁷ [Europäisches Parlament, Understanding EU-NATO cooperation: Theory and practice.](#)

[Europäischer Rat/Rat der Europäischen Union, Politisches und Sicherheitspolitisches Komitee \(PSK\).](#)

[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.](#)



Der/die Hohe Vertreter:in der Union für Außen- und Sicherheitspolitik übernimmt den Vorsitz der Ratskonstellation zu Auswärtigen Angelegenheiten (FAC). Der Vorsitzende des EUMC (CEUMC) wird durch den Rat der EU ernannt und nimmt an Sitzungen des Rates teil, sofern Themen mit Verteidigungsbezug diskutiert werden. Im COSI sind hohe Beamten der Innen- und/oder Justizministerien aller EU-Mitgliedsstaaten, Vertreter:innen der Kommission sowie des EAD beteiligt. Als Beobachter können Europol, Eurojust, CEPOL oder andere einschlägige Gremien eingeladen werden. Das ERCC koordiniert sich unter anderem mit dem Rat der EU. OLAF erstattet der Arbeitsgruppe des Rates zur Betrugsbekämpfung regelmäßig Bericht. EUISS wurde vom Rat der EU gegründet. Die Etablierung des EU CyberNet wurde unter anderem in Dokumenten des Rates der EU vorgesehen. Bis Juni 2022 soll ein Bericht zur Rolle und den Verantwortlichkeiten von teilnehmenden Akteuren innerhalb der JCU erarbeitet werden, der daraufhin dem Rat der EU zur Entscheidung vorgelegt werden soll⁹⁸.



Reference Incident Classification Taxonomy Task Force (TF-CSIRT)

Die Reference Incident Classification Taxonomy Task Force hat sich die Erstellung einer universellen Taxonomy über Sicherheitsvorfälle zum Ziel gesetzt. Dies soll über die Anfertigung eines Referenzdokuments, die Entwicklung eines Mechanismus für Updates und Versionierung, die Verwaltung des Referenzdokuments sowie die Organisation persönlicher Meetings der Akteure erreicht werden.

Mitglieder der Taskforce sind Mitglieder europäischer CSIRTs. Darunter befinden sich auch das CERT-Bund sowie der TGG (inkl. Vertreter:innen der ENISA und EC3)⁹⁹.



Senior Officials Group Information Systems Security (SOG-IS)

Die Senior Officials Group Information Systems Security ist ein Zusammenschluss von Regierungsorganisationen oder Regierungsagenturen der EU oder der Europäischen Freihandelsassoziation, die daran arbeiten, die Standardisierung von Schutzprofilen auf der Basis gemeinsamer Kriterien sowie Zertifizierungspolicies zwischen Europäischen Zertifizierungsbehörden zu koordinieren. SOG-IS entwickelt außerdem Schutzprofile für Richtlinien der Europäischen Kommission im Bereich IT-Sicherheit, die in nationale Gesetzgebung umgesetzt werden muss.

⁹⁸ [Council of the European Union, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.](#)

[Council of the European Union, The EU Integrated Political Crisis Response – IPCR – Arrangements.](#)

[Europäischer Rat/Rat der Europäischen Union, Horizontal Working Party on Cyber Issues \(HWP\).](#)

[Europäische Kommission, Anhang zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.](#)

[Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.](#)

[Rat der Europäischen Union, Cyberangriffe: EU plant Gegenmaßnahmen, einschließlich Sanktionen.](#)

[Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr \(Aktualisierung 2018\).](#)

[Rat der Europäischen Union, Ständiger Ausschuss für die operative Zusammenarbeit im Bereich der Inneren Sicherheit \(COSI\).](#)

[Rat der EU, Der Rat der Europäischen Union.](#)

[Europäische Union, Rat der Europäischen Union.](#)

⁹⁹ [ENISA, Building a common language to face future incidents – ENISA and European CSIRTs establish a dedicated task force.](#)

[ENISA, Reference Incident Classification Taxonomy.](#)



Deutsches Mitglied ist das **BSI**. Die **ENISA** unterstützt die **EK** bei der Ausarbeitung eines Zertifizierungssystems für Cybersicherheit, das als Nachfolger des bestehenden Abkommens über die gegenseitige Anerkennung (Mutual Recognition Agreement, MRA) der SOG-IS dienen soll.¹⁰⁰



Ständige Strukturierte Zusammenarbeit (PESCO)

Die Ständige Strukturierte Zusammenarbeit wurde im Rahmen der Zusammenarbeit im Bereich der Gemeinsamen Sicherheits- und Verteidigungspolitik geschaffen. Durch dedizierte PESCO-Projekte sollen auch Fähigkeiten der EU, Zusammenarbeit zwischen den Mitgliedstaaten sowie Interoperabilität im Bereich der Cyberabwehr und -verteidigung gestärkt werden. Im Rahmen der PESCO wurden zudem von Litauen koordinierte sogenannte *Cyber Rapid Response Teams (CRRTs)* geschaffen, die sich aus Cybersicherheitsexpert:innen der sechs teilnehmenden EU-Mitgliedsstaaten zusammensetzen. CRRTs sollen EU-Mitgliedstaaten, EU-Institutionen, EU-GSVP-Missionen und -Operationen sowie bestimmte Partnerländer bei der Prävention von und Reaktion auf IT-Sicherheitsvorfälle unterstützen.

Der **EAD** (inkl. EUMS) sowie die **EVA** bilden das PESCO-Sekretariat. Als Teil von PESCO-Projektpaketen wurde unter anderem das **CIDCC** auf Initiative des **KdoCIR** geschaffen. Ein:e Vertreter:in relevanter PESCO-Projekte ist als unterstützender Teilnehmer der **JCU** designiert¹⁰¹.



Taxonomy Governance Group (TGG)

Die Aufgabe der Common Taxonomy Governance Group ist die Instandhaltung und Aktualisierung des Dokuments „Common Taxonomy for Law Enforcement and the National Network of CSIRTs“, welches eine gemeinsame Taxonomie für die Klassifizierung von strafrechtlichen Vorfällen enthält. Die TGG kommt jährlich für ein reguläres Gruppentreffen zusammen.

Hierdurch soll die Kooperation zwischen internationalen Strafverfolgungsbehörden und den Computer Security Incident Response Teams (CSIRTs) sowie Staatsanwaltschaften verbessert und Präventions- und Ermittlungsfähigkeiten gestärkt werden. An der Arbeitsgruppe beteiligen sich die **ENISA**, **EC3/Europol**, die **EUCTF**, das **CERT-EU** sowie ausgewählte CSIRTs durch jeweilige Fachexpert:innen¹⁰².

¹⁰⁰ [SOGIS, Introduction.](#)

[Working Group on the MRA SOG-IS succession.](#)

¹⁰¹ [EEAS, Ständige Strukturierte Zusammenarbeit – SSZ.](#)

[European Commission, Joint Cyber Unit.](#)

[European Defence Agency, Activation of first capability developed under PESCO points to strength of cooperation in cyber defence.](#)

[PESCO, About PESCO.](#)

[PESCO, PESCO Secretariat.](#)

[Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr \(Aktualisierung 2018\).](#)

¹⁰² [Europol, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.](#)

[Rossella Mattioli und Yonas Leguesse, Reference Incident Classification Taxonomy Task Force Update.](#)



Zentrum für die Koordination von Notfallmaßnahmen (ERCC)

Das Zentrum für die Koordination von Notfallmaßnahmen der Kommission, angesiedelt bei der Generaldirektion Humanitäre Hilfe und Katastrophenschutz (GD ECHO), unterstützt und koordiniert verschiedene Aktivitäten in den Bereichen „prevention, preparedness and response“. So koordiniert es beispielsweise die Bereitstellung von Hilfsgütern für Länder, die von Katastrophen betroffen sind.

Es verantwortet das Krisenmanagement der EK und bildet den 24/7-verfügbaren Kontaktpunkt für die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR). Das ERCC kann zur „Bewältigung von Sicherheitsvorfällen während einer Cybersicherheitskrise“ auf technischer Ebene in Zusammenarbeit mit weiteren Akteuren zum Einsatz kommen. Federführende Dienststelle des ERCC wäre in diesem Fall GD CONNECT. Neben den EU-Mitgliedstaaten koordiniert sich das ERCC mit dem EAD und dem Rat der EU. Im Bedarfsfall werden von deutscher Seite Aktivierungsanfragen für das Katastrophen- und Krisenmanagement der EU vom GMLZ an das ERCC weitergeleitet¹⁰³.



Zentrum für Informationsgewinnung und -analyse (INTCEN)

Das Zentrum für Informationsgewinnung und -analyse (früher: EU Situation Centre (EU SITCEN)) ist eine zivile Analyseeinheit des Europäischen Auswärtigen Dienstes, die aufbereitetes Material aus den Mitgliedstaaten verarbeitet. Anders als etwa nationale Nachrichtendienste in den EU-Mitgliedstaaten, verfügt INTCEN, welches direkt der:m Hohen Vertreter:in der EU für Außen- und Sicherheitspolitik unterstellt ist, daher über keinerlei eigenständigen operativen Sammelfähigkeiten zur Informationsbeschaffung. Unter Berücksichtigung dieser, offen zugänglichen Informationen sowie beispielsweise Berichten aus europäischen Delegationen oder Erkenntnissen des EU-Satellitenzentrums, erstellt es strategische Lagebeurteilungen, Sonderberichte und ad hoc Briefings und leitet Handlungsoptionen daraus ab. Neben dem militärischen Intelligence Directorate des EU-Militärstabs (EUMS INT) sowie der Direktion Krisenbewältigung und Planung (CMPD) gehört es zu den Krisenmanagementstrukturen des Europäischen Auswärtigen Dienstes. Zusätzlich zur EU Hybrid Fusion Cell gehört zum Zentrum auch der EU Situation Room (SITROOM), der dem Europäischen Auswärtigen Dienst die notwendigen operativen Kapazitäten zur Verfügung stellt, um eine sofortige und effektive Antwort in Krisensituationen zu ermöglichen. Es ist die ständige zivil-militärische „Stand-by“-Behörde, die rund um die Uhr weltweites Monitoring und Lagebeurteilung bietet.

¹⁰³ [Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#)

[EUR-Lex, Empfehlung \(EU\) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.](#)

[European Commission, Emergency Response Coordination Centre \(ERCC\).](#)



Das *INTCEN* ist im *EAD* angesiedelt. Aus Deutschland tragen *BND* und *BfV* Berichte bei und entsenden Mitarbeiter an das *INTCEN*. *INTCEN*-Berichte wiederum gehen an das *BKAmt*, den *BND*, das *AA*, das *BMVg*, das *BAMAD*, das *BMI* und den *BfV* sowie themenbezogen auch an weitere Stellen. *INTCEN*-Produkte können auch anderen *EU*-Institutionen, die innerhalb der Gemeinsamen Außen- und Sicherheitspolitik, der Gemeinsamen Sicherheits- und Verteidigungspolitik oder der Terrorismusbekämpfung agieren, zur Verfügung gestellt werden. Gemeinsam mit dem *EUMS INT* bildet *INTCEN* die *Single Intelligence Analysis Capacity (SIAC)*. Es arbeitet mit der *ENISA* zusammen und ist als teilnehmende Organisation der *JCU* designiert. Das *INTCEN* erarbeitet mit *Europol* halbjährlich die vorausschauende Bedrohungslage, welche an den Ständigen Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit (*COSI*) übermittelt wird¹⁰⁴.

¹⁰⁴ [Council of the European Union, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.](#)

[Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats „EU Playbook“.](#)

[Deutscher Bundestag \(Drucksache 19/489\): Antwort der Bundesregierung auf die Kleine Anfrage: Pläne der Europäischen Kommission für eine geheimdienstliche „Europäische Aufklärungseinheit“.](#)

[Europäischer Auswärtiger Dienst, EU INTCEN Factsheet.](#)

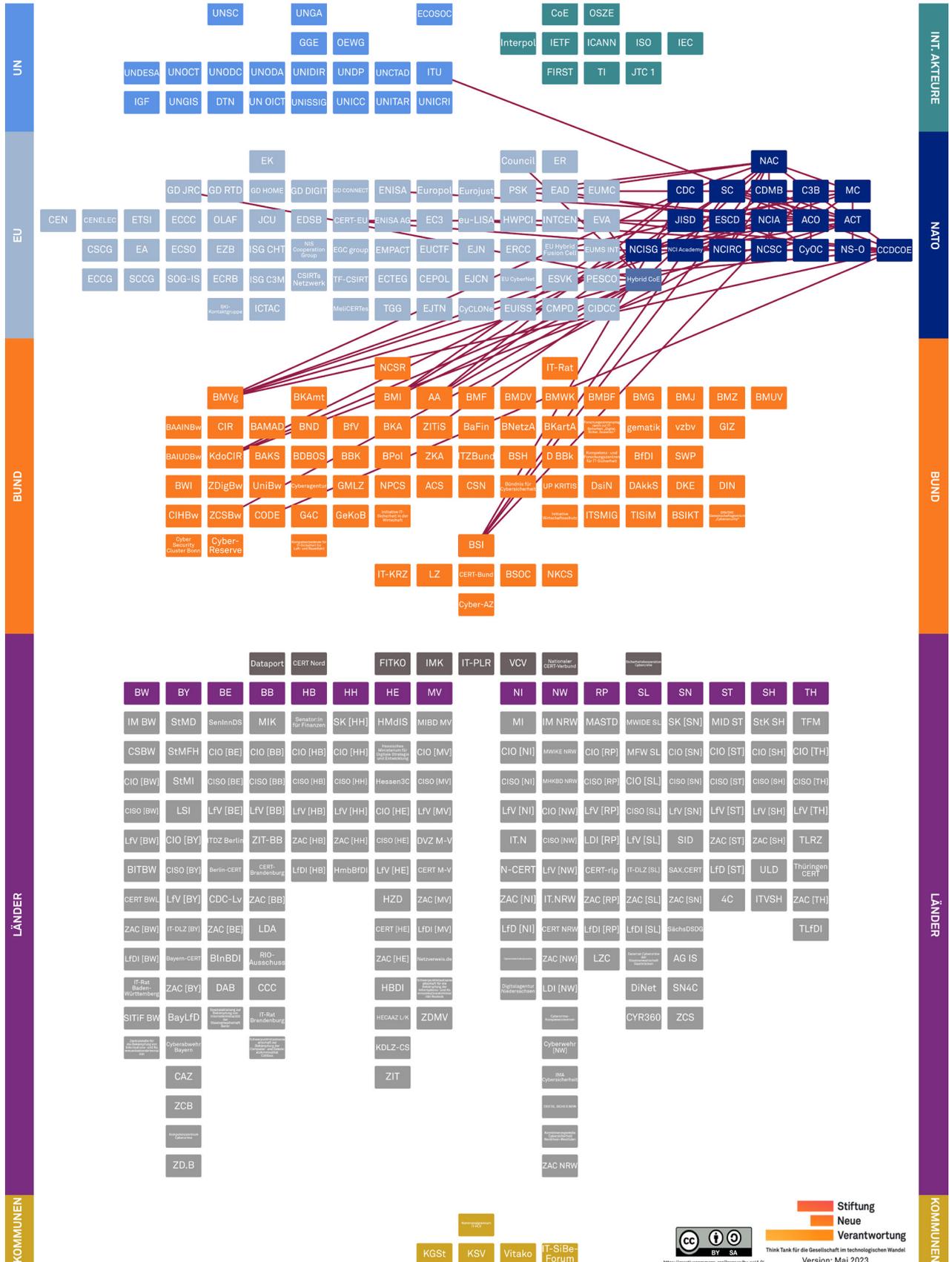
[Matthias Monroy, Europäisches Geheimdienstzentrum vor neuen Aufgaben.](#)

[Matthias Monroy, How European secret services organize themselves in „groups“ and „clubs“.](#)

[Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik.](#)



7. Erläuterung – Akteure auf NATO-Ebene





Policy-Überblick

Jahr	Name
2021	Brussels Summit Communiqué
2018	Brussels Summit Declaration
2016	Cyber Defence Pledge
2016	Warsaw Summit Communiqué
2014	Wales Summit Declaration
2012	Chicago Summit Declaration



Allied Command Operations (ACO)

Innerhalb der militärischen NATO-Kommandostruktur, die das Allied Command Operations (ACO) gemeinsam mit dem Allied Command Transformation (ACT) bildet, ist das ACO für die Planung und Durchführung sämtlicher NATO-Operationen zuständig und berät die politische und militärische Führung der NATO in militärischen Fragen. Unter Leitung des Supreme Allied Commander Europe (SACEUR) verfügt das ACO, für das das Supreme Headquarters Allied Powers Europe (SHAPE) mit Sitz in Mons, Belgien als Hauptquartier fungiert, über verschiedene Kommandos auf operativer und taktischer Ebene, die innerhalb des NATO-Bündnisgebiets geographisch verstreut stationiert sind. Unter den sechs taktischen Kommandos befinden sich neben Einheiten für Luft, Land und See zudem drei Kommandos für Spezialeinsätze, Logistik sowie Cyberoperationen. Im militärischen Bereich obliegt ACO die strategische Ausgestaltung von Cyberverteidigung.

*Diese strategische Ausgestaltung wird auf taktischer Ebene durch Lagebilder der **NCIA** unterstützt. Das **CyOC** untersteht dem ACO Deputy Chief of Staff (DCOS) für den Cyberraum. Vertreter:innen des ACO nehmen an Sitzungen des **C3B**, dem **CDMB** und des **SC** teil. Der:die SACEUR erhält seine:ihre Weisungen durch das **MC**. ACO steht mit der **JISD** im Austausch. **NCISG** und die Abteilung für Cyberverteidigung im ACO bei dem SACEUR sind in ihren Aufgaben interdependent. Gemeinsam mit dem **SECGEN** hat der SACEUR bereits an Briefings seitens der NATO gegenüber dem **PSK** der EU teilgenommen¹⁰⁵.*

¹⁰⁵ [NATO, Allied Command Operation.](#)

[NATO Public Diplomacy Division, Allied Command Operations.](#)

[SHAPE, Allied Command Operations overview: An introduction to the organisation and responsibilities. \(Webseite entfernt\)](#)



Allied Command Transformation (ACT)

Im Vergleich zu dem operationellen Fokus des ACO verantwortet das Allied Command Transformation innerhalb der militärischen NATO-Kommandostruktur Ausbildung, Training, Übungen und Fähigkeitsentwicklung um zu Interoperabilität sowie der Zukunftsfähigkeit der Allianz beizutragen. ACT untersteht dem Supreme Allied Commander Transformation (SACT). Für Cyberverteidigung und Cybersicherheit ist innerhalb des ACT federführend das Capability Development Directorate zuständig. Dort werden unter anderem Übungen im Cyberbereich, wie die jährliche NATO Cyber Coalition Exercise oder die Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX), vorbereitet.

Vertreter:innen des ACT nehmen an Sitzungen des SC, C3B und CDMB teil. ACT steht mit der JISD in Austausch. An der NATO Cyber Coalition Exercise, die mit Unterstützung des NATO MC durchgeführt wird, nimmt die Bundeswehr teil. In Besuchsfunktion ist auch die ENISA vertreten. KdoCIR nimmt zudem an der CWIX teil, die das ACT im Auftrag von NAC, MC und C3B steuert. NATO Centres of Excellence (CoE), wie beispielsweise das CCDCOE werden durch ACT akkreditiert. ACT kann das CCDCOE zur Übernahme bestimmter Aufgaben beauftragen. Im Auftrag von ACT übernimmt das CCDCOE derzeit die Funktion als Education and Training Department Head (E&T DH) für den Cyberbereich und koordiniert die Ausbildung in diesem Bereich, wie beispielsweise an der ACT unterstellten NS-O. Das Kursangebot der NCI Academy wird mit Unterstützung des ACT erstellt. Es kommt zu regelmäßigen Treffen zwischen dem SACT und dem Chief Executive der EVA¹⁰⁶.



Cyber Defence Committee (CDC)

Das Cyber Defence Committee (früher: Defence Policy and Planning Committee (Cyber Defence)) ist ein dem Nordatlantikrat unmittelbar unterstelltes Gremium, dem die Federführung für Cyberverteidigung/-abwehr innerhalb der NATO obliegt. Das CDC, welches auf Expertenebene zusammenkommt, beaufsichtigt und steuert Anstrengungen und Aktivitäten der NATO im Bereich der Cyberverteidigung/-abwehr.

Das CDMB hat gegenüber dem CDC eine Berichtspflicht. Beispielsweise im Falle eines schweren Cybersicherheitsvorfalls kann das CDC die Situation zur weiteren Befassung an den NAC verweisen. Der:die deutsche Vertreter:in im CDC erhält eine von AA, BMI und BMVg abgestimmte Weisung, das BSI ist in den Weisungsgebungsprozess beratend eingebunden¹⁰⁷.

¹⁰⁶ [Allied Command Transformation, Who We Are.](#)
[Bundeswehr, Multinational Interoperabilität testen – CWIX 2021.](#)
[Joint Force Training Centre, CWIX 2021 Execution.](#)
[NATO, Cyber defence.](#)

¹⁰⁷ [Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.](#)
[NATO, Cyber defence.](#)
[NATO CCDCOE, North Atlantic Treaty Organization.](#)



Emerging Security Challenges Division (ESCD)

Die Emerging Security Challenges Division ist organisatorisch innerhalb des NATO International Staff (IS) angesiedelt. Die ESCD soll unter anderem Fähigkeiten der NATO in Bezug auf die Antizipation und Bewältigung neuer Herausforderungen stärken und politische Lösungen zur Verteidigung des Bündnisses gegen diese erarbeiten. Hierzu bewertet sie beispielsweise potenzielle Krisen und resultierende Konsequenzen für die NATO aus strategischer Perspektive und unterhält themenbezogene Dialoge mit NATO-internen als auch externen Organisationen und Akteuren. Sie wird durch eine:n Assistant Secretary General (ASG) für Emerging Security Challenges geleitet. Innerhalb der ESCD werden Themen mit Cybersicherheitsbezug von der Cyber and Hybrid Policy Section verantwortet. Als ziviler Counterpart zu der Befassung aus militärischer Perspektive innerhalb von SHAPE (ACO), koordiniert die ESCD Anstrengungen zum Schutz der NATO-Netzwerke gegen Cyberoperationen, unterstützt Bündnispartner bei der Stärkung ihrer Resilienz und entwickelt cyberverteidigungspolitische Kooperationen und Partnerschaften. Darüber hinaus verfügt die ESCD über eine Cyber Threat Assessment Cell, die Themen und Entwicklungen mit Cybersicherheitsbezug monitoren.

Die Entscheidung zur Errichtung der ESCD geht auf eine Entscheidung des NAC zurück. Die ESCD leitet das CDMB. Ihre Cyber Threat Assessment Cell operiert in Austausch mit dem CyOC. Für Diskussionen zu Cyberverteidigung/-abwehr ist die ESCD bereits zu Treffen mit Vertreter:innen des EAD zusammengekommen. Die gemeinsame Vereinbarung über die Benennung des BSI als National Cyber Defence Authority (NCDA) gegenüber der NATO wurde von NATO-Seite aus von der ESCD geschlossen¹⁰⁸.



Joint Intelligence and Security Division (JISD)

Die Joint Intelligence and Security Division innerhalb des NATO IS soll zur Entscheidungsfindung auf höchster politischer Ebene durch verbesserte Lageerkennung sowie Sammlung unterschiedlichster nachrichtendienstlichen Ressourcen beitragen. In der JISD ist hierfür beispielsweise auch eine Einheit zur Analyse hybrider Bedrohungen (Hybrid Analysis Branch) angesiedelt.

Produkte der JISD werden hauptsächlich Entscheidungsträger:innen innerhalb des NAC und MC zur Verfügung gestellt. Austausch seitens JISD besteht sowohl mit ACT und ACO. Besonders enge Beziehungen bestehen zu ACO im Prozess der Aussprache von Warnungen. Über die NATO hinaus kooperiert und tauscht die JISD zudem regelmäßig Informationen mit der EU Hybrid Fusion Cell aus. Jährlich nehmen beide Ak-

¹⁰⁸ [NATO Emerging Security Challenges Division, Science for Peace and Security \(SPS\) Programme. NATO HQ, ESCD.](#)

[NATO International Staff, Vacancy Notification: Cyber Threat Analyst, Cyber Threat Assessment Cell. NATO, NATO, European Union experts review cyber defence cooperation.](#)



teure parallel eine koordinierte Bewertung der Sicherheitslandschaft vor, um zu einer einheitlichen Betrachtung der Bedrohungslage beizutragen¹⁰⁹.



NATO Communications and Information Agency (NCIA)

Als Fusion von sieben ehemaligen NATO-Organisationen wurde die NATO Communications and Information Agency (NCIA) gegründet. Die NCIA ist für die Vernetzung der Allianz sowie die Beschaffung und den Schutz ihrer Kommunikations- und Informationsinfrastruktur zuständig. Jedes Jahr erwirbt die NCIA neue C4ISR-Technologien, wodurch unter anderem auch die Interoperabilität der IKT-Systeme gestärkt werden soll. Zudem unterstützt die NCIA NATO-Bündnis- als auch Partnerstaaten bei der Entwicklung interoperabler IKT-Fähigkeiten. Bei der NCIA sind auch die Smart Defence Initiatives der NATO mit Cyberverteidigungsbezug, wie bspw. die Smart Defence Multinational Cyber Defence Capability Development (MN CD2) oder Malware Information Sharing Platform (MISP), organisatorisch angesiedelt.

Der NCIA sind das NATO Cyber Security Centre (NCSC) sowie die NCI Academy unterstellt. Zudem betreibt es über das NCSC die NCIRC. NCIA befindet sich in ständigem Austausch mit dem CyOC, an das es Statusupdates zu den NATO-Netzwerken übermittelt und auf dessen operative Anweisungen es bei Cybersicherheitsvorfällen reagiert. Sie ist im CDMB vertreten und arbeitet mit der NCISG zusammen. Im Krisenfall verfügt ACO über die Befugnis, Anstrengungen und Aktivitäten der NCIA zu priorisieren. Zwischen dem CERT-EU und der NCIA werden Informationen ausgetauscht und es finden regelmäßige Treffen auf Arbeitsebene statt¹¹⁰.



NATO Communication and Information System Group (NCISG)

Der NATO Communication and Information Systems Group unterstehen die drei sogenannten Signal Bataillone der NATO, die in Wesel, Grazzanise (Italien) und Bydgoszcz (Polen) ansässig sind. Jährlich organisiert die NCISG mit „Steadfast Cobalt“ die größte Kommunikations- und Informationssystemübung innerhalb der NATO.

NCISG und die Abteilung für Cyberverteidigung im ACO bei dem SACEUR sind in ihren Aufgaben interdependent. Beide werden durch denselben/dieselbe Kommandeur:in (COM NCISG und DCOS Cyberspace SHAPE) geführt. Zudem arbeiten die NCISG und die NCIA arbeiten zusammen. KdoCIR beteiligt sich an Steadfast Cobalt¹¹¹.

¹⁰⁹ [Arndt Freytag von Loringhoven, A new era for NATO intelligence. EU-NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.](#)

[NATO, NATO's response to hybrid threats. NATO, Structure.](#)

¹¹⁰ [Don Lewis, What is NATO Really Doing in Cyberspace?.](#)

[NATO, Cyber defence. NCIA, Who we are.](#)

¹¹¹ [Bundeswehr, CWIX 2021 findet als Remote Event statt.](#)

[NATO Communications & Information Systems Group, About us. NATO Communications & Information Systems Group, Exercise STEADFAST COBALT 2021. NATO Communications & Information Systems Group, Leadership.](#)



NATO Computer Incident Response Capability (NCIRC)

Die der NCIA unterstellte NATO Computer Incident Response Capability verfügt organisatorisch über ein Technical (NCIRC TC) und Coordination Centre (NCIRC CC), die bei SHAPE ansässig sind. Beide sollen sämtliche NATO-eigenen Netzwerke im Alltag und rund um die Uhr vor Operationen in technischer Hinsicht schützen und diese abwehren. Dabei verantwortet das NCIRC TC beispielsweise neben der Verhinderung, die Erkennung sowie Bearbeitung von etwaigen Cybersicherheitsvorfällen oder -Bedrohungen und gibt anlassbezogene Informationen weiter. Darüber hinaus verfügt das NCIRC TC über sog. Rapid Reaction Teams (RRT) als permanentes Standby-Element, die – wenn angefragt – im Falle eines Vorfalls von nationaler Bedeutung innerhalb von maximal 24 Stunden reagieren und dadurch zur Wiederherstellung der Systeme beitragen können. Dem NCIRC CC wiederum obliegt die Koordinierung von Cyberverteidigungsaktivitäten innerhalb der NATO, unter NATO-Bündnisstaaten sowie Internationalen Organisationen.

Die NCIRC wird durch das NCSC betrieben, das der NCIA untersteht. Sie unterstützt das CyOC bei der Lagerkennung. Zudem unterstützt das NCIRC CC den CDMB in personeller Hinsicht und unterhält auch Beziehungen zu anderen internationalen Organisationen wie der EU. NCIRC TC sowie das CERT-EU kooperieren in technischer Hinsicht, um den Informationsaustausch zu verbessern sowie Best Practices zu teilen. Zusätzliche Zusammenarbeit auf Arbeitsebene besteht von Seiten NCIRC TC mit dem CERT-Bw. Anfragen nach einem Einsatz der RRT's müssen bei Bündnisstaaten durch das CDMB und bei Nicht-NATO-Staaten durch den NAC stattgegeben werden. Die Expert:innen der RRT's nehmen an den Cybersicherheitsübungen Cyber Coalition Exercise sowie Locked Shields teil¹¹².



NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Das NATO Cooperative Cyber Defence Centre of Excellence ist ein durch die NATO akkreditiertes multinationales Kompetenzzentrum mit Sitz in Tallinn, Estland im Bereich der Cybersicherheit. Es gehört zwar als NATO-akkreditiertes Kompetenzzentrum zur NATO-Rechtskörperschaft, bildet jedoch keinen Teil der NATO-Kommandostruktur. Zum einen bietet es für die NATO, seine Bündnisstaaten und Partner Training und Ausbildung in strategischen, operativen, technischen und rechtlichen Aspekten der Cyberverteidigung an. Unter diesen Aufgabenschwerpunkt fällt auch die Organisation der jährlichen Cybersicherheitsübung Locked Shields. Darüber hinaus wird am CCDCOE zu diesen vier Dimensionen auch selbst geforscht. Diese Forschungsergebnisse, wie beispielsweise INCYDER oder die Cyber Defence Library, werden der breiten Öffentlichkeit zur Verfügung gestellt. In 2020 hat das CCDCOE einen fünfjährigen Prozess zur Erstellung eines Tallinn Manual 3.0 zur Anwendbarkeit des Völkerrechts im Cyberraum als Aktualisierung des aktuellen Leitfadens (Tallinn Manual 2.0) initiiert. Jährlich organisiert das CCDCOE zudem die Internati-

¹¹² [Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.](#)
[NATO, Factsheet: NATO Cyber defence.](#)
[NATO, Men in black – NATO's cybermen.](#)
[NATO, NATO Rapid Reaction Team to fight cyber attack.](#)

onal Conference on Cyber Conflict (CyCon), die Vertreter:innen aus Politik, Industrie und Wissenschaft zu interdisziplinären Diskussionen zusammenbringt.

Seitens der NATO erfolgte die Akkreditierung des CCDCOE durch ACT, welches das CCDCOE auch zu bestimmten Aufgaben beauftragen kann. Derzeit ist das CCDCOE von ACT mit der Übernahme des Department Head for Cyber Defence Operations Education and Training (E&T DH) beauftragt und koordiniert sämtliche Ausbildungsvorhaben der NATO im Bereich der Cyberverteidigung. Zur Erfüllung seines Mandats unterhält das CCDCOE Arbeitsbeziehungen beispielsweise mit der NS-O, der NCI Academy sowie der EVA, der EU Hybrid Fusion Cell, dem ESKV und dem CODE der Universität der Bundeswehr. Das CCDCOE unterhält Kontakte auf Arbeitsebene mit der eu-LISA. Als eine von sieben Gründungsnationen des CCDCOE stellt Deutschland den Deputy Director und beteiligt sich durch Bw- und BMVg-Vertreter:innen an Locked Shields. Gemeinsam mit der ITU und weiteren Akteuren war das CCDCOE an der Erstellung einer Handreichung zur Entwicklung einer nationalen Cybersicherheitsstrategie beteiligt¹¹³.



NATO Consultation, Control and Command Board (C3B)

Das NATO Consultation, Control and Command Board (C3B) berät und agiert im Auftrag des Nordatlantikrates im Bereich der Beratung, Kontrolle und Steuerung (C3) wozu beispielsweise schwerpunktmäßig Informationsaustausch, Interoperabilität sowie Überwachung und Aufklärung gehören. In Bezug auf Cybersicherheit ist es innerhalb der NATO das Haupt-Gremium für Diskussionen, die auf die Implementierung von Cyberverteidigung/-abwehr aus technischer Perspektive fokussiert sind. Für strategische Schwerpunktsetzungen kommt das C3B zwei Mal im Jahr zusammen. Regelmäßige Treffen, die die Erfüllung der strategischen Ziele überprüfen, finden im C3B in Permanent Session-Format statt, welches sich aus nationalen C3-Repräsentant:innen (NC3REPs) zusammensetzt. Es verfügt zudem über mehrere spezialisierte Untergremien, wie beispielsweise das Information Assurance and Cyber Defence Capability Panel. Das C3B wird in seiner Arbeit durch den NATO Headquarter C3 Staff (NHQC3S), einer gemeinsamen Einheit des Internationalen Militärstabes und International Staff, unterstützt.

An dem C3B nehmen neben nationalen Repräsentant:innen, Vertreter:innen des MC, ACT sowie ACO teil. Das C3B kann Befassungen des SC anstrengen. Von deutscher Seite wird diese Funktion federführend vom BMVg wahrgenommen. Im untergeordneten Information Assurance and Cyber Defence Capability Panel sind BMVg und BSI vertreten¹¹⁴.

¹¹³ Hintergrundgespräch, 2021.

[NATO CCDCOE, About Us.](#)

[NATO CCDCOE, Training.](#)

[NATO CCDCOE, Research.](#)

[Rat der EU, EU Cyber Defence Policy Framework.](#)

¹¹⁴ [NATO, Consultation, Command and Control Board \(C3B\).](#)

[NATO, Cyber defence.](#)



NATO Cyber Defence Management Board (CDMB)

In dem NATO Cyber Defence Management Board werden auf Arbeitsebene sämtliche Cyberverteidigungsaktivitäten innerhalb der zivilen und militärischen Organisationsstruktur der NATO durch strategische Planung koordiniert. Außerdem kann das CDMB Memoranda of Understanding mit NATO-Bündnisstaaten abschließen, beispielsweise um den Informationsaustausch zwischen beiden Ebenen zu verbessern.

Das CDMB kommt unter dem Vorsitz der ESCD zusammen und ist verpflichtet, an das CDC zu berichten. Es setzt sich aus Vertreter:innen aller NATO-Akteure mit Mandat im Bereich Cyberverteidigung/-abwehr, unter anderem ACO, ACT und NCIA, zusammen und wird durch das NCIRC CC in personeller Hinsicht unterstützt¹¹⁵.



NATO Cyber Security Centre (NCSC)

Innerhalb der NCIA verantwortet das NATO Cyber Security Centre die gesamte „Cyber Security Service Line“, um durch spezialisierte Dienstleistungen zur Vorbeugung, Erkennung und Reaktion auf Cybersicherheitsvorfälle beizutragen. Zudem wurde ein Cyber Security Collaboration Hub zur besseren Vernetzung, Informationsbeschaffung und Schulung zwischen den nationalen CERT's der NATO-Bündnisstaaten geschaffen. Unter dem Dach des NCSC besteht zudem die NATO Industry Cyber Partnership (NICP) zwischen NATO-internen Akteuren, nationalen CERTs sowie Industrie-Vertreter:innen aus NATO-Bündnisstaaten. Durch die NICP soll Cyberverteidigung innerhalb der NATO-Lieferkette verbessert, schnelle Informationswege und Austausch bei Cyberbedrohungen gestärkt sowie Best Practices im Allgemeinen gefördert werden sollen.

Das NCSC ist institutionell bei der NCIA angesiedelt. Dem NCSC untersteht die NCIRC. Informationsaustausch und Arbeitsbeziehungen bestehen mit dem CyOC, welche auch durch die gemeinsame Ansässigkeit bei SHAPE gefördert werden¹¹⁶.



NATO Cyberspace Operations Centre (CyOC)

Bis 2023 soll die Errichtung des NATO Cyberspace Operations Centre abgeschlossen und dieses voll einsatzbereit sein. Das CyOC soll auf strategischer Ebene durch Entwicklung eines Situationsbewusstseins und Lageerkennung unterstützen sowie auf operativer Ebene alle Aktivitäten der NATO im Cyberraum, beispielsweise im Kontext von NATO-Operationen koordinieren. Zum Zwecke der Koordination soll CyOC unter anderem über Verbindungselemente zu regionalen Kommandos des ACO verfügen.

¹¹⁵ Jeffrey L. Caton, [NATO Cyberspace Capability: A Strategic and Operational Evolution](#).
[NATO, Cyber defence](#).

¹¹⁶ [NCIA, Securing the Cloud](#).
[NCIA, What We Do: NATO's Cybersecurity Centre](#).
[NICP, Objectives and Principles](#).



Zur Lageerkennung ist das CyOC auf nachrichtendienstliche Informationen der Bündnisstaaten angewiesen und wird in seiner Aufgabenerfüllung unter anderem durch die Cyber Threat Assessment Cell (CTAC) der ESCD im NATO HQ sowie dem NCSC und der NCIRC unterstützt. Es befindet sich in ständigem Austausch mit der NCIA, von der es Statusupdates zu den NATO-Netzwerken erhält und auf dessen operative Anweisungen es bei Cybersicherheitsvorfällen reagiert. CyOC ist dem DCOS Cyberspace im ACO unterstellt und bei SHAPE in Belgien angesiedelt¹¹⁷.



NATO-Militärausschuss (MC)

Als oberstes militärisches Gremium der NATO komplementiert der NATO-Militärausschuss die Entscheidungsfindung auf höchster Ebene. Als Bindeglied verantwortet es die operationale Umsetzung politischer Entscheidungen in militärische Anweisungen, unterstützt die Erstellung strategischer Gesamtkonzepte der Allianz und kann zudem auch Empfehlungen für Maßnahmen zur bestmöglichen Verteidigung des Bündnisses aussprechen. In der jüngsten Vergangenheit hat der MC beispielsweise auch Cyberoperationen und die Einmischung in Wahlen diskutiert. Jährlich nimmt der MC eine Stärke- und Fähigkeitsbewertung von Ländern, die NATO-Interessen gefährden, vor. Der MC kommt mindestens einmal wöchentlich auf Ebene der national entsandten militärischen Vertreter:innen als Representant:innen der Generalstabschefs zusammen. Letztere treffen sich im MC-Format dreimal im Jahr.

Dem MC obliegt federführend die Beratung des NAC in militärpolitischen Fragen. Die Strategischen Kommandeure des ACT und ACO erhalten ihre Weisungen durch das MC. Es ist einer der Adressaten der Produkte der JISD und kann Sitzungen des SC anstrengen. Deutschland wird durch Vertreter:innen der Bw (BMVg) im MC repräsentiert. Der MC kommt regelmäßig zu Treffen mit seinem Counterpart in der EU, dem EUMC, zusammen¹¹⁸.



NATO School Oberammergau (NS-O)

Als eine der NATO-Ausbildungseinrichtungen innerhalb der NATO-Kommandostruktur bietet die NATO School in Oberammergau, die von Deutschland und den USA zu gleichen Teilen finanziert wird, Ausbildungseinheiten und Kurse mit operativem und technischem Fokus an. Im Bereich der Cybersicherheit und Cyberverteidigung möchte die NS-O die Fähigkeiten von NATO-Bündnisstaaten sowie Partnernationen stärken, kritische Kommunikation und Informationsinfrastruktur gegen Operationen zu schützen. Hierzu hat die NS-O auch (gemeinsam mit der Naval Postgraduate School (NPS)) ein Cyber Security Certificate Programme ins Leben gerufen.

¹¹⁷ [Don Lewis, What is NATO Really Doing in Cyberspace?](#)

[BrigGen Sandor Vass, Cyberspace Operations Centre: A Capability User Perspective.](#)

[Robin Emmott, NATO cyber command to be fully operational in 2023.](#)

¹¹⁸ [Europäisches Parlament, Understanding EU-NATO cooperation: Theory and practice.](#)

[NATO, Military Committee.](#)

[U.S. Department of Defense, NATO Military Committee Gets Virtual Check on Alliance Missions.](#)



NS-O ist dem **ACT** unterstellt. Die Ausbildung an der NS-O im Bereich der Cybersicherheit und Cyberverteidigung wird durch das **CCDCOE** koordiniert¹¹⁹.



NATO Security Committee (SC)

Das Security Committee befasst sich mit sicherheitspolitischen Fragestellungen und erarbeitet Empfehlungen für die Sicherheitspolitik der NATO. In dieser Hinsicht wird es beratend gegenüber dem Nordatlantikrat tätig. In seinen Aufgabenbereich fallen zudem die Verabschiedung von Richtlinien und Leitfäden, unter anderem auch im Bereich der Informationssicherheit. Das SC kommt dabei in unterschiedlichen Formationen, wie beispielsweise dem SC in CIS Security Format (SC(CISS)), zusammen.

Von deutscher Seite hat das **BMI** die Federführung im SC inne. Das **BSI** ist beratend tätig und repräsentiert Deutschland im SC (CISS). Gegenüber dem **NAC** besteht seitens SC eine Berichtspflicht, der mindestens einmal jährlich nachgekommen werden muss. Befassungen des SC können durch den NAC, NATO-Bündnisstaaten, den **MC** oder das **C3B** angestrengt werden. An Sitzungen des SC sind zudem Vertreter:innen des C3B sowie von **ACO** und **ACT** anwesend. Weitere NATO-Gremien und -Akteure können anlassbezogen eingebunden werden¹²⁰.



NCI Academy

Mit der NCI Academy wurden vier früher separate NATO-Ausbildungseinrichtungen (NATO CIS School, Applications Training Facility The Hague, Air Command and Control Systems Training Centre sowie das SHAPE CIS Training Centre) unter dem Dach der NCIA vereint. Durch Standardisierung von Kurskatalogen sollen Kursteilnehmer durch die NCI Academy bestmöglich in Cybersicherheit sowie Führung, Information, Kommunikation, Computersysteme, Nachrichtenwesen, Überwachung und Aufklärung (C4ISR) ausgebildet werden. Ausbildung an der NCI Academy wird für NATO-Bündnisstaaten sowie auch Nicht-Mitgliedsstaaten angeboten. Die NCIA hat sich zum Ziel gesetzt, zwischen 2020 und 2027 10.000 „cyber defenders“ für die NATO sowie die EU an der NCI Academy auszubilden. Hierzu unterhält die NCI Academy auch Partnerschaften mit Wissenschaft und Privatsektor.

Die NCI Academy ist der **NCIA** unterstellt. Das aktuelle Kursangebot der NCI Academy wurde mit Unterstützung des **ACT** erstellt. Das **CCDCOE** übernimmt auch für die NCI Academy den E&T DH im Cyberbereich¹²¹.

¹¹⁹ [NATO School, NATO School Oberammergau – Naval Postgraduate School Cyber Security Professional Programme Closure in Morocco.](#)

[NATO School, Organization.](#)

¹²⁰ [NATO, Security Committee \(SC\).](#)

¹²¹ [NCIA, About the NCI Academy.](#)

[NCIA, Introducing the NCI Academy.](#)

[NCIA, 10,000 Cyber Defenders: Cyber education for the NATO-EU workforce.](#)



Nordatlantikrat (NAC)

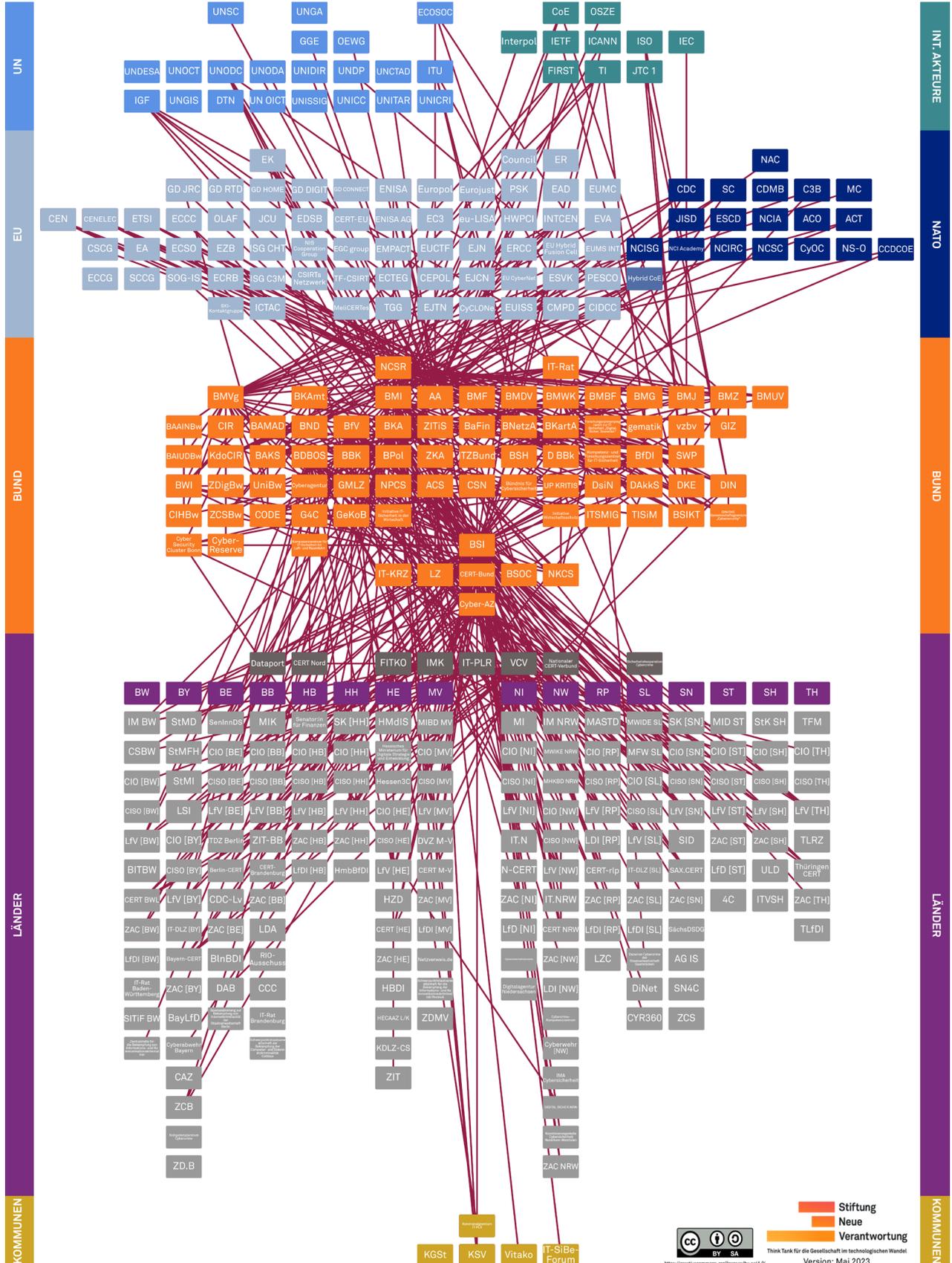
Der bereits im Nordatlantikvertrag aus 1949 vorgesehene Nordatlantikrat besteht aus Vertreter:innen der NATO-Bündnisstaaten. Mindestens einmal wöchentlich treten diese auf Botschafter:innen-Ebene und halbjährlich auf Ebene der Außen- und Verteidigungsminister:innen zusammen. Etwa alle zwei Jahre kommt der NAC mit einem Gipfeltreffen (Brussels Summit) aller Staats- und Regierungschef:innen zusammen. Der NAC ist das primäre politische Entscheidungsgremium innerhalb der NATO. Im Falle eines schweren Cybersicherheitsvorfalls würde der NAC hinsichtlich einer einheitlichen NATO-Reaktion entscheiden und eventuell den Bündnisfall nach Artikel 5 Nordatlantikvertrag ausrufen sowie das Krisenmanagement verantworten. Der NAC fasst seine Entscheidungen dem Prinzip der Einstimmigkeit folgend. Zudem kann der NAC auch gemeinsame Statements abgeben und darin beispielsweise bestimmte Verhaltensweisen verurteilen.

Auf Botschafter:innen-Ebene wird Deutschland durch den Ständigen Vertreter bei der NATO (AA) im NAC vertreten. Den Vorsitz des NAC hat der:die NATO-Generalsekretär:in inne. Das CDC untersteht dem NAC unmittelbar und unterstützt dessen Arbeit als Unter-Gremium. Aus hierarchischer Perspektive folgt nach dem CDC das CDMB und danach wiederum die NCIRC. Dem MC obliegt die Beratung des NAC in militärpolitischen Fragen und das SC berichtet mindestens einmal jährlich an den NAC. Der NAC hat die Einrichtung des Hybrid CoE befürwortet und die Errichtung der ESCD geht auf eine Entscheidung des NAC zurück. Er erhält Produkte der JISD. NAC und das PSK der EU kommen zu regelmäßigen formellen sowie auch informellen Treffen zusammen. In der Vergangenheit hat der:die Hohe Vertreter:in der Union für Außen- und Sicherheitspolitik (oder EAD-Vertreter:innen) regelmäßig an Treffen des NAC auf Ebene der Verteidigungsminister:innen teilgenommen¹²².

¹²² [Center for European Policy Analysis, Moving Toward NATO Deterrence for the Cyber Domain. NATO, North Atlantic Council.](#)
[NATO, Statement by the North Atlantic Council concerning malicious cyber activities.](#)
[Ständige Vertretung der Bundesrepublik Deutschland bei der NATO, Botschafter König.](#)



8. Erläuterung – Akteure auf Bundesebene





Policy-Überblick

Jahr	Name
2023	<u>Agenda Cybersicherheitsforschung des Bundesministeriums für Bildung und Forschung</u> . Maßnahmen im Zuge der Zeitenwende
2022	<u>Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat</u> . Ziele und Maßnahmen für die 20. Legislaturperiode
2022	<u>Digitales Deutschland – Souverän. Sicher. Bürgerzentriert. Digitalpolitische Ziele und Maßnahmen bis 2025 des Bundesministeriums des Innern und für Heimat</u>
2022	<u>Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten</u> (IT-Sicherheitsverordnung Portalverbund, ITSIV-P)
2022	<u>Zweite Verordnung zur Änderung der BSI-Kritisverordnung</u> Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2016: <u>Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz</u> (BSI-Kritisverordnung, BSI-KritisV)
2021	<u>Cybersicherheitsstrategie für Deutschland</u> (CSS) Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2016: <u>Cyber-Sicherheitsstrategie für Deutschland</u>• 2011: <u>Cyber-Sicherheitsstrategie für Deutschland</u>
2021	<u>Digitalisierung gestalten. Umsetzungsstrategie der Bundesregierung</u>
2021	<u>Gesetz über das Bundesamt für Sicherheit in der Informationstechnik</u> (BSI-Gesetz, BSIG)
2021	<u>Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten</u> (Bundeskriminalamtgesetz, BKAG)
2021	<u>Gesetz über den Bundesnachrichtendienst</u> (BND-Gesetz, BNDG)
2021	<u>Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz</u> (Bundesverfassungsschutzgesetz, BVerfSchG)
2021	<u>Gesetz zur Anpassung des Verfassungsschutzrechts</u>
2021	<u>Position Paper on the Application of International Law in Cyberspace</u>
2021	<u>Telekommunikationsgesetz</u> (TKG)
2021	<u>Telemediengesetz</u> (TMG)
2021	<u>Weißbuch Multilateralismus</u>



Jahr	Name
2021	<u>Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme</u> (IT-Sicherheitsgesetz 2.0) Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2015: <u>Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme</u> (IT-Sicherheitsgesetz)
2020	<u>Gesetz für ein Zukunftsprogramm Krankenhäuser</u> (Krankenhauszukunftsgesetz, KHZG)
2020	<u>Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia</u>
2018	<u>Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung</u>
2017	<u>Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen</u> (Onlinezugangsgesetz, OZG)
2017	<u>Umsetzungsplan Bund 2017: Leitlinie für Informationssicherheit in der Bundesverwaltung</u>
2016	<u>Digitale Strategie 2025</u>
2016	<u>Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr</u>
2014	<u>Digitale Agenda 2014-2017</u> <ul style="list-style-type: none">• 2017: <u>Legislaturbericht Digitale Agenda 2014–2017</u>
2009	<u>Nationale Strategie zum Schutz Kritischer Infrastrukturen</u> (KRITIS-Strategie)
2005	<u>Nationaler Plan zum Schutz der Informationsinfrastrukturen</u> (NPSI) <ul style="list-style-type: none">• 2007: <u>Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen</u>
1999	<u>Eckpunkte der deutschen Kryptopolitik</u>



Agentur für Innovation in der Cybersicherheit (Cyberagentur)

Die Cyberagentur soll nach einer Interimsphase in Halle (Saale) dauerhaft am Flughafen Leipzig-Halle untergebracht werden. Der Gründungsprozess der Cyberagentur wurde im August 2020 abgeschlossen und erste Beauftragungen sollen Ende 2020 vorgenommen worden sein. Die Cyberagentur identifiziert Innovationen und vergibt konkrete Aufträge für die Entwicklung von Lösungsmöglichkeiten. Letztere sollen ambitionierte Forschungsvorhaben mit hohem Innovationspotenzial im Bereich Cybersicherheit und diesbezügliche Schlüsseltechnologien für die Bedarfsdeckung des Staates bezüglich innerer und äußerer Sicherheit fördern. Dabei betreibt die Agentur keine eigene Forschung, Entwicklung und Innovation, sondern koordiniert den Bedarf der Sicherheitsbehörden und verbessert die Kooperation zwischen Bund, Wissenschaft und Wirtschaft. Sie stellt ein Element der Bundesregierung zum



Schutz der Bürger:innen im Cyberraum dar. Die Cyberagentur wurde als GmbH mit parlamentarischen Kontrollmechanismen und Auflagen gegründet.

*Die gemeinsame Federführung der Cyberagentur haben **BMI** und **BMVg** inne. Sie ist Teil des **NPCS**. Beide sind als Initiativen der „Hightech-Strategie 2025“ der Bundesregierung entstanden. Insbesondere zur Vermeidung von Redundanzen gibt es eine Abstimmung der Arbeitsprogramme zwischen beiden Agenturen, zum Beispiel durch gegenseitige Beauftragungen bei agenturübergreifenden Themen. Um weitere Redundanzen zu vermeiden, steht die Cyberagentur ebenfalls im Austausch mit **ZITiS**, dem **CIHBw** und **CODE**. Der Aufsichtsrat der Agentur soll zukünftig aus Vertreter:innen des **BMI**, **BMVg** und **BMF** sowie Personalrät:innen der Beschaffungssämter der Bundeswehr und Vertreter:innen der Wissenschaft bestehen¹²³.*



Auswärtiges Amt (AA)

Das Auswärtige Amt setzt sich im Rahmen seiner Cyberaußenpolitik für internationale Cybersicherheit, universelle Menschenrechte im digitalen Raum sowie die Nutzung wirtschaftlicher Chancen durch die Digitalisierung ein. Hierzu wurde der „Koordinierungsstab für Cyber-Außenpolitik und Cybersicherheit“ (KS-CA) im Auswärtigen Amt geschaffen, welcher der:dem Beauftragten für Cyberaußenpolitik und Cybersicherheit (CA-B) untersteht. An ausgewählten Auslandsvertretungen hat das AA Zuständigkeiten für Cyberaußenpolitik eingerichtet, die unter anderem mit der Berichterstattung an die Zentrale in Berlin betraut sind. Das AA ist zudem für die Informations- und Kommunikationstechnik als auch die Sicherstellung eines eigenen Kommunikationsnetzes in seinem Geschäftsbereich sowie für die Bundesverwaltung im Ausland (Auslands-IT), beispielsweise an deutschen Auslandsvertretungen, verantwortlich. Das Auswärtige Amt koordiniert das nationale Attribuierungsverfahren der Bundesregierung, welches die „Zuschreibung der Verantwortung für erhebliche Cyberattacken internationalen Ursprungs regelt“.

*Das AA ist im **NCSR** vertreten. Es stellt im Wechsel mit dem **BMVg** die Leitung der **BAKS** und finanziert die **SWP** durch Drittmittel. Das AA zählt zu den Empfängern anlassbezogener eingestufte „Cyber-Spezial“-Berichte des **BfV**. Das AA ist zudem am **BSOC**-Verbund beteiligt und im **IT-Rat** sowie Verwaltungsrat des **ITZBund** vertreten. Deutsche Hilfsangebote im Rahmen des **GMLZ** werden in Absprache mit **BMI** und **AA** koordiniert. Auf **EU**-Ebene ist das AA unter anderem in Vorgänge und Diskussionen*

¹²³ [Andre Meister und Anna Biselli, Bundesrechnungshof bezweifelt Sinn der neuen Cyberagentur.](#)
[Bundesministerium des Innern, für Bau und Heimat, Cyberagentur des Bundes nach Halle/Saale und Leipzig.](#)
[Bundesministerium des Innern, für Bau und Heimat, Startschuss für die Cyberagentur.](#)
[Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.](#)
[Deutscher Bundestag \(Drucksache 19/22958\), Antwort der Bundesregierung auf die Kleine Anfrage: Agentur für Innovation in der Cybersicherheit GmbH \(Cyberagentur\).](#)
[Die Bundesregierung, Agentur für Innovation in der Cybersicherheit. \(Webseite entfernt\)](#)
[Lina Rusch, Cyberagentur kommt – mit strengen Auflagen.](#)



der *HWPCI* involviert, Teil des Ausbildungsnetzwerks des *ESVK* und Kuratoriumsmitglied von *EU CyberNet*. Das AA erhält Berichte des *INTCEN* und des *EUMS INT*. Auf NATO-Ebene ist das AA durch seinen:ihre Ständige:n Vertreter:in bei der NATO im *NAC* vertreten und unter anderem an der deutschen Weisungsgebung für das *CDC* beteiligt. Deutschland ist regelmäßiges nicht-ständiges Mitglied des *UNSC*. Vertreter:innen der Ständigen Vertretung Deutschlands bei den UN in New York haben sich in der Vergangenheit auch an *UNSC*-Debatten zu Cybersicherheit beteiligt. Das AA verantwortet die deutsche Teilnahme in den *GGE*'s und den *OEWG*'s. Vertreter:innen des AA haben zudem an Sitzungen und Treffen der *CCPCJ (ECOSOC)* als auch der *IEG Cybercrime (UNODC)* teilgenommen. Finanziell unterstützt das AA *UNODA*, das *UNIDIR* sowie das *UNODC*. Mit *UNIDIR* hat das AA auch eine gemeinsame Veranstaltung mit Cyberbezug ausgerichtet. Der:die deutsche Botschafter:in bei den UN in Genf ist im Kuratorium des *UNITAR* vertreten und ein:e weitere:r AA-Vertreter:in ist im Steering Committee des deutschen *IGF (IGF-D)* repräsentiert. Der:die deutsche Außenminister:in bzw. der:die Leiter:in der Ständigen Vertretung Deutschlands beim Europarat vertritt Deutschland im *CoE*-Ministerkomitee. Das AA ist auch für im Rahmen der *Budapest-Konvention* ersuchter Rechtshilfe oder Auslieferungen durch andere Vertragsparteien Ansprechpartner. Das AA unterhält zudem eine Ständige Vertretung der Bundesrepublik bei der *OSZE*¹²⁴.



Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit (BfDI)

Der:die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit berät und kontrolliert als oberste Bundesbehörde die Daten- und Informationsverarbeitung der öffentlichen Stellen des Bundes und nicht-öffentlicher Stellen. Das BfDI-Referat 25 befasst sich mit technischem Datenschutz und ist u.a. auch zuständig für die „Beratung, Sensibilisierung und Aufklärung, insbesondere der öffentlichen Stellen des Bundes über technikadäquaten und rechtskonformen Einsatz der Informationstechnik“. In der Vergangenheit hat der:die BfDI auch Stellungnahmen zu geplanten Gesetzesvorhaben wie dem IT-Sicherheitsgesetz 2.0 oder einer Anhörung des Innenausschusses des Bundestages zum Recht auf Verschlüsselung Stellung bezogen. Sie:er ist in der Ausübung seines:ihrer Amtes politisch unabhängig und unterliegt lediglich der parlamentarischen Kontrolle durch den Bundestag.

BfDI und *BSI* kooperieren miteinander. Er:sie ist beratendes Mitglied im *IT-PLR*. Der:die BfDI überprüft regelmäßig die Daten- und Informationsverarbeitung des *ITZ-Bund* und verfügt gegenüber der *ZITiS* über das Recht auf Akteneinsicht um die Ein-

¹²⁴ [Auswärtiges Amt, Auslands-IT.](#)

[Auswärtiges Amt, Cyber-Außenpolitik.](#)

[Auswärtiges Amt, Einrichtung einer Zuständigkeit für Cyber-Außenpolitik.](#)

[Bundesamt für Justiz, Gesetz über den Auswärtigen Dienst \(GAD\).](#)

[Deutscher Bundestag \(Drucksache 20/1657\), Unterrichtung durch die Bundesregierung Bericht der Bundesregierung zum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitung sowie über die Entwicklung der Streitkräftepotenziale \(Jahresabrüstungsbericht 2021\).](#)



haltung von Datenschutzvorschriften zu kontrollieren. Die:der BfDI ist im Beirat der DsiN sowie dem Beirat des *Cyber Security Clusters Bonn* vertreten. Kontakte bestehen zudem mit dem:der *EDSB*¹²⁵.



Bundeskanzleramt (BKAm)

Das Bundeskanzleramt unterstützt den:die Bundeskanzler:in bei ihrer inhaltlichen Arbeit. Dazu unterhält es durch seine „Spiegelreferate“ Kontakt zu den Bundesministerien. Mit Themen der Cybersicherheit kommt es u.a. bei der Dienst- und Fachaufsicht des Bundesnachrichtendienstes und der Finanzierung der Stiftung Wissenschaft und Politik in Berührung.

*Das BKAm ist im NCSR vertreten und ihm ist der BND nachgeordnet. Den Vorsitz des IT-Rates haben der:die Chef:in des BKAm sowie der:die CIO Bund inne. Das BKAm ist auch im Verwaltungsrat des ITZBund vertreten. Der:die Chef:in des BKAm nimmt den Tätigkeitsbericht des IT-PLR zur Kenntnis. Aus seinem Haushalt wird die institutionelle Zuwendung an die SWP gezahlt. Das BKAm zählt zu den Adressaten eingestufte „Cyber-Spezial“-Berichte des BfV sowie Berichten des INTZEN. Es ist im Kuratorium der BAKS vertreten*¹²⁶.



- **Bundesnachrichtendienst (BND)**

Der Bundesnachrichtendienst ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland und handelt im Auftrag der Bundesregierung. Im Ausland erfasst er Vorfälle, die der Cyberspionage oder -sabotage in Deutschland dienen sollen und warnt betroffene Akteure im Inland entsprechend vor, damit Abwehrmechanismen eingeleitet werden können. Bekannt ist dieser Teil seiner Arbeit der Fernmelde- und elektronischen Aufklärung auch unter dem Akronym SSCD (SIGINT Support to Cyber Defense).

Der BND gehört zum Geschäftsbereich des BKAm. Zwischen BND, BfV und BAMAD werden Informationen ausgetauscht und es bestehen gegenseitige Unterrichtungspflichten. Er ist an der Initiative Wirtschaftsschutz beteiligt und im Cyber-AZ vertreten. Er kann auf Leistungen der ZITiS zurückgreifen. Sofern zur

¹²⁵ [Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.](#)

[Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Europäische Einrichtungen zur Strafverfolgung.](#)

[Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Geschäftsverteilungsplan.](#)

[Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme an den Deutschen Bundestag zum IT-Sicherheitsgesetz 2.0.](#)

[Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zur öffentlichen Anhörung des Innenausschusses zum Thema „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“.](#)

[Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 28. Tätigkeitsbericht zum Datenschutz 2019.](#)

¹²⁶ Bundeskanzleramt, Chef des Bundeskanzleramtes. (Webseite entfernt)



*Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, erforderlich, kann das **BSI** auch gegenüber anderen Stellen wie Polizeien, Strafverfolgungsbehörden aber auch Verfassungsschutzbehörden wie dem **BND** unterstützend tätig werden. Sein Personal wird unter anderem an der **UniBw** München ausgebildet. Der **BND** erhält Produkte des **EUMS INT** und trägt Berichte an das **INTCEN** bei¹²⁷.*



Bundesministerium der Justiz (BMJ)

Das Bundesministerium der Justiz ist vor allem ein Gesetzgebungsministerium, das auch andere Bundesministerien bei ihren Rechtsetzungsvorhaben unterstützt.

*Das **BMJ** ist im **NCSR** und dem Kuratorium der **BAKS** vertreten. Zudem ist es im **IT-Rat**, dem Verwaltungsrat des **ITZBund** sowie im Beirat des **CODE** repräsentiert. Vertreter:innen des **BMJ** haben an Sitzungen der **IEG Cybercrime (UNODC)** sowie der **CCPCJ (ECOSOC)** auf UN-Ebene teilgenommen. Vertreter:innen des **BMJ** nehmen an Treffen des **Cybercrime Convention Committee (T-CY)** des **CoE** teil. Es finanziert zu 97 Prozent die Kernarbeit des **vzbv**¹²⁸.*



Bundesministerium der Verteidigung (BMVg)

Das Bundesministerium der Verteidigung ist innerhalb der Bundesregierung das Fachressort für die militärische Verteidigung – und somit auch für die Verteidigung Deutschlands im Cyberraum verantwortlich. Zusätzlich verantwortet es die „Gewährleistung der Cybersicherheit in bundeswehreigenen Netzen und Rechenzentren“. Im Ministerium ist hierfür der Chief Information Security Officer Bundeswehr (CISOBw) in der Abteilung Cyber/IT (CIT) federführend zuständig. Dem **BMVg** untersteht die Bundeswehr, die u.a. für die Landes- und Bündnisverteidigung verantwortlich. Neben den Teilstreitkräften Heer, Luftwaffe und Marine verfügt die Bundeswehr ebenso über die Streitkräftebasis (SKB), den Sanitätsdienst (ZSan) sowie dem Cyber- und Informationsraum (CIR) als militärische Organisationsbereiche (MilOrgBer). Letzterer verantwortet die Verteidigung des Cyber- und Informationsraums ganzheitlich. Im Rahmen der Amtshilfe kann die Bundeswehr andere Behörden zum Beispiel bei der Vorfallsbearbeitung unterstützen.

*Das **BMVg** ist im **NCSR** vertreten. Ihm ist die Bundeswehr (**Bw**) (auch mit **BAMAD**, **BAAINBw**, **BAIUDBw**, **KdoCIR**, **ZDigBw**, **ZCSBw**, **UniBw**, **CODE**) nachgeordnet und die **BAKS** gehört zu seinem Geschäftsbereich. Die **Bw** bildet Teile ihres Personals an*

¹²⁷ [Bundesnachrichtendienst, Cybersicherheit.](#)

[Bundesnachrichtendienst, Die Arbeit.](#)

[Heinz Fromm, Stellungnahme zur Vorbereitung der öffentlichen Anhörung am 17. Mai 2018 zum Thema „Föderale Sicherheitsarchitektur“.](#)

[Kurt Graulich, Sicherheitsrecht des Bundes – Recht der Nachrichtendienste in Deutschland. \(Webseite entfernt\)](#)

¹²⁸ [Bundesministerium der Justiz und für Verbraucherschutz, Aufgaben und Organisation.](#)

[Bundesministerium der Justiz und für Verbraucherschutz, Schutz von Bürgern und Onlinehandel vor Cyberkriminalität. \(Webseite entfernt\)](#)

[Bundesministerium der Justiz und für Verbraucherschutz, Wir dürfen Cybermobbing nicht ignorieren. \(Webseite entfernt\)](#)

den UniBw (inkl. CODE) aus. Die Bundeswehr nimmt an der ACS teil und wird sich für den Bund auch dem GeKoB beteiligen. Das BMVg ist im IT-Rat sowie dem Verwaltungsrat des ITZBund vertreten. Zum Zwecke der gesamtstaatlichen Sicherheitsvorsorge unterstützt die Cyber-Reserve die Aufgabenwahrnehmung der Bundeswehr. Innerhalb der Bundeswehr analysiert und identifiziert das BAMAD unter anderem extremistische Bestrebungen und Spionagevorhaben. Deutschland wird durch Vertreter:innen der Bw im NATO MC repräsentiert. Das BAAINBw versorgt die Bw mit IT sowie digitalisierten Waffensystemen und die BWI operiert als IT-Systemhaus der Bw. Die Cyberagentur wurde unter gemeinsamer Federführung des BMVg und BMI eingerichtet. Das BMVg ist am NKCS beteiligt. Dem BMVg wird die Analyse der Situation im Cyber- und Informationsraum durch die Operationszentrale im KdoCIR bereitgestellt. Es erhält zudem von EU-Ebene Berichte des INTCEN und durch den EUMS INT. Vertreter:innen des BMVg sind im Beirat des CODE sowie im Stiftungsrat der SWP repräsentiert. Das BMVg setzt zudem auf nationale und internationale Kooperationen und Partnerschaften, zum Beispiel mit dem CIHBw oder dem NATO CCDCOE. Es ist Teil des Netzwerks EU-weiter Ausbildungseinrichtungen des ESKV. Auf NATO-Ebene verantwortet das BMVg die deutsche Repräsentation im C3B und ist in den Weisungsgebungsprozess für das CDC eingebunden. Die Bw nimmt an der durch das ACT organisierten Cyber Coalition Exercise sowie der durch das CCDCOE organisierten Übung Locked Shields teil¹²⁹.



- **Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)**

Hauptaufgabe des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr ist die Ausstattung des deutschen Militärs. Dies erfolgt sowohl durch Gerätschaften als auch durch IT-Systeme. Die Systeme werden vom BAAINBw meist in Auftrag gegeben und nicht eigenständig entwickelt. Durch die Rolle als Projektleiter und Nutzungsleiter der beschafften und betriebenen Systeme trägt es wesentliche Mitverantwortung dafür, die Bundeswehr bestmöglich vor Cyberoperationen zu schützen. Die Leitung des BAAINBw und die einzelnen Projektleiter werden durch einen CISO Rüstung unterstützt.

Das BAAINBw gehört zum Geschäftsbereich des BMVg. Es versorgt die Bw mit IT und digitalisierten Waffensystemen und verantwortet die Steuerung der BWI. Zukünftig soll bei neuen IT-Beschaffungen für die Bw im Rahmen einer trilateralen

¹²⁹ [Bundesministerium der Verteidigung, Cybersicherheit.](#)
[Bundesministerium der Verteidigung, Cyber Innovation Hub.](#)
[Bundesministerium der Verteidigung, Die Abteilungen des Verteidigungsministeriums.](#)
[Bundeswehr, Amtshilfe in Bitterfeld – IT-Soldaten im zivilen Einsatz.](#)
[Bundeswehr, Auftrag und Aufgaben der Bundeswehr.](#)
[Bundeswehr, Das Kommando Cyber- und Informationsraum.](#)
[Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land 2018.](#)



Zusammenarbeit zwischen **BSI**, dem **CISOBw** sowie dem **BAAINBw Security by Design** stärker berücksichtigt werden¹³⁰.



– Bundesweite IT-Systemhaus GmbH (BWI)

Die Bundesweite IT-Systemhaus GmbH ist eine Gesellschaft des Bundes und sowohl IT-Dienstleister der Bundeswehr als auch ein IT-Dienstleistungszentrum des Bundes. Schwerpunkte der Arbeit sind das Betreiben und Modernisieren der Informations- und Kommunikationstechnik der Bundeswehr und die Unterstützung in den Bereichen Logistik und Administration. Die BWI ist unter anderem auch für das Software-Management und die IT-Sicherheit der von ihr betriebenen IT-Infrastruktur verantwortlich. Für die von der BWI für die Bw betriebenen Netze und Systeme gelten die Sicherheitsvorgaben der Bundeswehr, das Cyber Security Operations Center der Bundeswehr (CSOCBw) überwacht diese mit dem CERT der BWI zusammen. Die BWI und die Bundeswehr haben zudem eine Kooperationsvereinbarung mit dem Ziel einer engeren Zusammenarbeit geschlossen, die ehemaligen Soldat:innen eine Eingliederung und die Arbeit im BWI ermöglichen soll.

Die BWI GmbH ist eine Bundesgesellschaft und IT-Systemhaus für Bw (BMVg) und Bund. Die Steuerung der BWI obliegt dem BAAINBw. Der CIHBw ist als eigene Abteilung in der BWI angesiedelt. Gemeinsam mit dem BSI wurde eine Absichtserklärung zur verstärkten Zusammenarbeit geschlossen. In diesem Rahmen ist die BWI beispielsweise dem BSOC-Verbund beigetreten. Sie ist Multiplikator der ACS. Das CERT der BWI ist im Nationalen CERT-Verbund vertreten, bei TI zertifiziert sowie bei FIRST involviert¹³¹.



→ Cyber Innovation Hub (CIHBw)

Der Cyber Innovation Hub der Bundeswehr bietet eigenen Mitarbeiter:innen in Zusammenarbeit mit Startups eine Plattform zur Erforschung und Weiterentwicklung innovativer Technologien. Das Ziel ist dabei, die Konkurrenzfähigkeit der Bundeswehr in den Bereichen Cyber und IT zu garantieren. Durch die Verknüpfung von Bundeswehr und Startups sollen Ideen schneller verwirklicht und fortschrittliche Technologien besser umgesetzt werden können. Die Soldat:innen arbeiten gemeinsam mit Zivilpersonen vor allem auch an der Entwicklung von disruptiven Technologien für die Bundeswehr.

¹³⁰ [Bundesministerium der Verteidigung, Zentrale Dienstvorschrift Informationssicherheit \(A-960/1\). CIR Bundeswehr \[@cirbw\], #Informationssicherheit funktioniert am besten, wenn sie von Anfang an mitgedacht wird. Daher wollen @BSI_Bund, @BaainBw und #CISOBw #SecurityByDesign bei #IT-Beschaffungen... \[Tweet\]. Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, Das BAAINBw.](#)

¹³¹ [Bundesministerium der Verteidigung, Auf engere Kooperation geeinigt: Bundeswehr und BWI GmbH. Bundesweite IT-Systemhaus GmbH, Cyber-Sicherheit: BSI und BWI wollen künftig enger zusammenarbeiten. Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.](#)



*Der CIHBw ist als eigene Abteilung in die **BWI GmbH** und somit in eine Verwaltung mit Weisungsbindung eingegliedert. Um Redundanzen zu vermeiden, steht der Cyber Innovation Hub im Austausch mit der **Cyberagentur**¹³².*



- **Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (BAIUDBw)**

Das BAIUDBw verantwortet im Rahmen seiner Abteilung Infrastruktur entsprechende Bedarfe der Bundeswehr im In- und Ausland sowie in Einsatzsituationen u.a. durch Planung und den Betrieb von Liegenschaften. Im Lichte der zunehmenden Digitalisierung der Gebäude- und Liegenschaftstechnik und davon operationell abhängiger Bundeswehr-Systeme befasst sich das BAIUDBw auch mit Cybersicherheit. Im BAIUDBw berät ein CISO Infrastruktur die Leitung sowie alle Infrastruktureferate in sämtlichen Fragen zur Informationssicherheit.

*Das BAIUDBw gehört zum Geschäftsbereich des **BMVg**¹³³.*



- **Bundesakademie für Sicherheitspolitik (BAKS)**

Die Bundesakademie für Sicherheitspolitik ist eine Weiterbildungsstätte des Bundes für Sicherheitspolitik. In unterschiedlichen Veranstaltungsformaten setzt sie sich auch mit den sicherheitspolitischen Herausforderungen im Cyberraum auseinander.

*Die BAKS gehört zum Geschäftsbereich des **BMVg**. Präsident:in und Vizepräsident:in kommen abwechselnd aus **BMVg** und **AA**. Im Kuratorium der **BAKS** sind unter dem Vorsitz der:s Bundeskanzlers:in Vertreter:innen aller im Bundessicherheitsrat vertretenen Ministerien (**AA**, **BMVg**, **BMF**, **BMJ**, **BMWK**, **BMZ** und das **BKAmt**) repräsentiert. Als Beiratsmitglieder der **BAKS** fungieren unter anderem Vertreter:innen der **Bw** und der **UniBw**. Die **BAKS** ist Teil des Netzwerkes EU-weiter Ausbildungseinrichtungen des **ESVK**¹³⁴.*



- **Bundesamt für den Militärischen Abschirmdienst (BAMAD)**

Das Bundesamt für den Militärischen Abschirmdienst ist eine Bundesoberbehörde und der militärische Nachrichtendienst des Bundes. Zu den Aufgaben des dritten und kleinsten Nachrichtendienstes des Bundes, neben dem Bundesnachricht-

¹³² [Bundesministerium der Verteidigung, Cyber Innovation Hub. Die Bundesregierung, Regierungspressekonferenz vom 2. Dezember 2019. MDR Sachsen-Anhalt, Der Chef der Cyberagentur in Halle. Matthias Punz, BMVg: Führung springt beim Cyber Innovation Hub ab. Sebastian Christ, Wehrbeauftragter kritisiert Umwandlung des Cyber Innovation Hub.](#)

¹³³ [Bundeswehr, Das Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr. Bundesministerium der Verteidigung, Zentrale Dienstvorschrift Informationssicherheit \(A-960/1\).](#)

¹³⁴ [Bundesakademie für Sicherheitspolitik, Cyber-Realität zwischen Freiheit und Sicherheit. Bundesakademie für Sicherheitspolitik, Der Beirat. Bundesakademie für Sicherheitspolitik, Das Kuratorium, der Bundessicherheitsrat.](#)



tendienst und dem Bundesamt für Verfassungsschutz, zählen Extremismus- und Terrorismusabwehr sowie die Bekämpfung von (Cyber-)Spionage und Sabotage in der Bundeswehr. Die BAMAD-Cyberabschirmung umfasst dabei „alle operativen, reaktiven, aber auch präventiven Maßnahmen des BAMAD zur Abwehr von nachrichtendienstlichen sowie sicherheitsgefährdenden Tätigkeiten oder extremistischen/terroristischen Bestrebungen“ im Cyber- und Informationsraum.

*Das BAMAD gehört zum Geschäftsbereich des **BMVg** und ist im **Cyber-AZ** vertreten. Innerhalb der Bundeswehr analysiert und identifiziert das BAMAD unter anderem extremistische Bestrebungen und Spionagevorhaben. Zwischen **BND**, **BfV** und **BAMAD** werden Informationen ausgetauscht und es bestehen gegenseitige Unterrichtungspflichten. Sofern zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, erforderlich, kann das **BSI** auch gegenüber anderen Stellen wie Polizeien, Strafverfolgungsbehörden aber auch Verfassungsschutzbehörden wie dem **MAD** unterstützend tätig werden. Es kann auf Dienstleistungen der **ZITiS** zurückgreifen. Das BAMAD erhält Berichte des **INTCEN**¹³⁵.*



- **Cyber-Reserve**

Parallel zum Aufbau des militärischen Organisationsbereiches CIR innerhalb der Bundeswehr wurde eine sog. Cyber-Reserve beschlossen, deren Aufbau durch eine Reservistenarbeitsgemeinschaft (RAG) innerhalb des Verbands der Reservisten der Deutschen Bundeswehr (VdRBw) unterstützt wird. Zur schnellen Reaktionsfähigkeit wird eine „Speerspitze Cyber-Reserve“ aufgebaut, die bei Bedarf frühzeitig aktiviert und bei IT-Vorfällen der Bundeswehr oder bei Amtshilfe unterstützen können. Im Unterschied zu anderen Reserveeinheiten, sollen für die Cyber-Reserve neben ehemaligen Soldat:innen auch explizit ziviles Personal und Führungskräfte mit IT-Expertise angeworben werden. Durch diese Bündelung unterschiedlichster Hintergründe soll die Cyber-Reserve „gemeinsame Übungen von Cyber-Spezialisten aus Behörden, Gesellschaft und Wirtschaft zur Cyber-Verteidigung ermöglichen [...] einen Wissenstransfer fördern“ sowie Cyber-Expert:innen ausbilden.

*Zum Zwecke der gesamtstaatlichen Sicherheitsvorsorge unterstützt die Cyber-Reserve die Aufgabenwahrnehmung der Bundeswehr, dabei insbesondere **KdoCIR** und **ZCSBw**¹³⁶.*

¹³⁵ [Bundesamt für den Militärischen Abschirmdienst, Über uns.](#)
[Bundesamt für den Militärischen Abschirmdienst, Aufgaben und Befugnisse.](#)
[Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Militärischer Abschirmdienst \(MAD\).](#)

¹³⁶ [Benjamin Vorhölter, Cyber-Reserve: Dienstleister für die Bundeswehr.](#)
[Bundesministerium der Verteidigung, Cyber-Reserve: Bundeswehr öffnet sich für IT-Community.](#)
[Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: RAG Cyber des VdRBw.](#)
[Bundeswehr, Reservist im Cyber- und Informationsraum.](#)
[Reservistenverband, Die Cyber-Reserve geht neue Wege.](#)



- **Organisationsbereich Cyber- und Informationsraum (CIR)**

Der militärische Organisationsbereich (MilOrgBer) Cyber- und Informationsraum der Bundeswehr ist für die militärische Domäne Cyber- und Informationsraum zuständig. Er ist der sechste militärische Organisationsbereich der Bundeswehr und soll bis 2021 mit über 13.500 Beschäftigten voll ausgebaut sein. CIR ist für den Schutz der inländischen IT-Systeme der Bundeswehr sowie den Schutz der IT-Systeme im Einsatz zuständig. Darüber hinaus verantwortet er die Stärkung von Fähigkeiten zur Aufklärung und Wirkung im Cyberraum, die Bereitstellung von Geoinformationsdaten an andere Einheiten der Bundeswehr, sowie den Austausch mit anderen Institutionen zur Sicherheitsvorsorge. Es wurde eine Strukturreform „CIR 2.0“ initiiert, die bis 2025 abgeschlossen sein soll. Sie sieht unter anderem die Bündelung von „Verantwortung und Kompetenzen in den Bereichen Konzeption und Weiterentwicklung in einem ‚Cyber and Information Domain Warfare Centre‘ [... sowie die] Zusammenführung aller Elemente in einem ‚Systemhaus Cyber- und Informationsraum/Zentrum Digitalisierung der Bundeswehr‘“ vor. Bis 2025 soll zudem ein Ausbildungszentrum CIR aufgestellt sein. Der militärische Organisationsbereich CIR beschäftigt insgesamt ca. 13.500 Soldat:innen und zivile Mitarbeiter:innen.

CIR ist Teil der Bw (BMVg) und wird vom KdoCIR geführt, dem wiederum das ZCSBw und das ZDigBw unterstellt sind. Zur Zusammenarbeit im Cyber-AZ hat sich CIR in der Vergangenheit mit dem BBK ausgetauscht¹³⁷.



- **Kommando Cyber- und Informationsraum (KdoCIR)**

Das Kommando Cyber- und Informationsraum führt den militärischen Organisationsbereich Cyber- und Informationsraum (CIR). Als Kommando des CIR führt das KdoCIR die Bereiche „Cyber, IT, Strategische Aufklärung, Geoinformationswesen der Bundeswehr und Operative Kommunikation“. Die Operationszentrale des KdoCIR erstellt eine Lageanalyse der Situation im Cyber- und Informationsraum. Vorrangig soll das Kommando jedoch den CIR strukturieren und die Personalführung gewährleisten. Zudem ist es „Dienst-sitz des Inspektors CIR und seines Vertreters, der in seiner Funktion als Chief Information Security Officer (CISOBw) die Gesamtverantwortung für die Informationssicherheit der Bundeswehr innehat“. Dem CISOBw untersteht fachlich das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) mit dem Cyber Security Operations Center der Bundeswehr (CSOCBw). Letzteres beheimatet das CERTBw und stellt Incident Response Teams im Falle

¹³⁷ [BBK \[@BBK_Bund\], BBK-Präsident @armin_schuster sprach heute mit dem Inspekteur #Cyber- und #Informationsraum Vizeadmiral Dr. Thomas Daum über die Zusammenarbeit von @BBK_Bund... \[Tweet\]](#). [Bundeswehr, Auftrag des Organisationsbereichs CIR](#). [Bundeswehr, CIR 2.0 – Der Organisationsbereich CIR gliedert sich neu](#). [Bundeswehr, „Liebe Hacker, hiermit laden wir Sie herzlich ein...“](#).



eines IT-Sicherheitsvorfalls zur Verfügung. CIR verfügt über eine Vulnerability Disclosure Policy (VDPBw), die durch den CISOBw verantwortet wird, in dessen Kontext es die aktive Meldung von Schwachstellen in IT-Systemen der Bw durch Externe ersucht. KdoCIR beschäftigt insgesamt ca. 800 Soldat:innen und zivile Mitarbeiter:innen. Der Standort des KdoCIR ist in Bonn.

Innerhalb des Organisationsbereichs sind ihm u.a. das ZDigBw und das ZCSBw unterstellt. Der CISOBw ist im KdoCIR verortet. Es ist im Cyber-AZ als ständiges Mitglied vertreten und stellt einen der stellvertretenden Koordinatoren. Die Analyse der Situation im Cyber- und Informationsraum wird u.a. dem BMVg und dem Cyber-AZ bereitgestellt. Auf eine Initiative des KdoCIR geht die Etablierung des CIDCC als PESCO-Projekt zurück. KdoCIR ist von deutscher Seite das übungskoordinierende Kommando der von dem ACT durchgeführten NATO-Übung Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX). Es nimmt zudem an der durch die NCISG jährlich organisierten Übung Steadfast Cobalt teil. Das KdoCIR ist als Beiratsmitglied im Cyber Security Cluster Bonn vertreten. Die Aktivitäten der Bundeswehr zur Cyber-Reserve werden vom KdoCIR gesteuert¹³⁸.



→ **Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw)**

Im ZDigBw sollen alle Digitalisierungsaufgaben im Geschäftsbereich des BMVgs gebündelt werden. Es gliedert sich in neun Kompetenzzentren die jeweils unterschiedliche inhaltliche Bereiche abbilden. Bereits bestehende oder anstehende IT-Projekte (insbesondere Softwareprojekte) sollen im ZDigBw zentralisiert für den gesamten Geschäftsbereich BMVg verwaltet werden. Die Zuständigkeit umfasst sowohl Entwicklung, Zertifizierung, Verifizierung, Validierung, Integration und Erprobung, sowie die Sicherstellung der Interoperabilität in der NATO. Dabei soll sowohl die Wiederverwertung bestehender oder abgeschlossener Projekte als auch die Beschaffung und Eigenentwicklung zum Portfolio des ZDigBw gehören, um einen wachsenden „Baukasten“ für verschiedene Anwendungsbereiche zu schaffen.

Das ZDigBw ist Teil des Organisationsbereiches CIR¹³⁹.

¹³⁸ [Bundesamt für Sicherheit in der Informationstechnik, BSI Magazin 2020/01: Mit Sicherheit. Bundesministerium der Verteidigung, FAQ: Cyber-Abwehr. Bundesministerium der Verteidigung, Lagezentrum Cyber- und Informationsraum im Pilotbetrieb. Bundeswehr, Auftrag des Organisationsbereichs CIR. Bundeswehr, Kommando Cyber- und Informationsraum. Bundeswehr, Multinational Interoperabilität testen – CWIX 2021. BWI, Von Big Data bis KI – Bundeswehr und BWI starten zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR. Deutscher Bundestag \(Drucksache 19/2645\), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.](#)

¹³⁹ [Bundeswehr, ZDigBw.](#)



- **Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)**

Das ZCSBw verantwortet den informationstechnischen Schutz der Systeme der Bundeswehr im In- und Ausland sowie in Einsatzkontexten. Im ZCSBw ist das Cyber Security Operations Centre der Bundeswehr (CSOCBw), und dort das CERTBw verortet. Im Falle von Bedrohungen oder Vorfällen, können im ZCSBw eingerichtete Incident Response Teams auf diese reagieren.

*Das ZCSBw untersteht dem **KdoCIR**. Das CSOCBw und das **BSOC** arbeiten zusammen. Zusammenarbeit auf Arbeitsebene besteht zwischen dem CERT der Bw und dem **NCIRC TC**. Das CERTBw beteiligt sich zudem an **FIRST**. Die **Cyber-Reserve** unterstützt u.a. das ZCSBw¹⁴⁰.*



- **Universitäten der Bundeswehr (UniBw)**

Die Universitäten der Bundeswehr München (UniBwM) und Hamburg (HSU/UniBw Hamburg) bilden Offiziere und Offiziersanwärter:innen wissenschaftlich aus. Die Studiengänge umfassen unter anderem Informatik, Informationstechnik, Cybersicherheit, Mathematisches Ingenieurwesen und Wirtschaftsinformatik.

*Die UniBw bilden das Personal der Bw wissenschaftlich aus und die UniBwM beheimatet **CODE** als fakultätsübergreifendes Forschungszentrum. Eine:Vertreter:in der UniBw fungiert als Beiratsmitglied der **BAKS**. Ein Institut der UniBwM ist an der **ACS** beteiligt. Die UniBw ist auch als Projektpartner am EU-HYBNET Projekt beteiligt, dem unter anderem auch **ZITIS** und **GD JRC** angehören¹⁴¹.*



- **Forschungsinstitut Cyber Defence (CODE)**

Das Forschungsinstitut Cyber Defence (CODE) an der Universität der Bundeswehr München wurde vom BMVg mit dem Ziel gegründet, innovative technische Neuerungen für Bundeswehr und Bund zum Schutz von Daten, Software und Systemen zu verwirklichen. Hierfür wurden drei Forschungscluster eingerichtet, die sich der Cyberverteidigung, Smart Data, künstlicher Intelligenz und Machine Learning sowie der Quantentechnologie widmen. Darüber hinaus ist das interdisziplinäre, unabhängige Forschungsinstitut an die wissenschaftliche Aus-, Fort- und Weiterbildung der Universität der Bundeswehr angebunden. Jährlich veranstaltet das CODE eine Jahrestagung.

*Als Teil der **UniBw** München wird auch am **CODE Bw**-Personal wissenschaftlich ausgebildet. **CODE** ist an dem **NKCS** beteiligt. Ein:e Vertreter:in des **BMVg** sitzt im Beirat des **CODE**. Es steht unter anderem mit der **Cyberagentur** und dem **CCDCOE** in Austausch. Das **CODE** ist im Beirat des **DsiN** vertreten¹⁴².*

¹⁴⁰ [Bundeswehr, Zentrum für Cyber-Sicherheit der Bundeswehr.](#)

¹⁴¹ [Universität der Bundeswehr München, Hintergrundinformationen.](#)
[Universität der Bundeswehr Hamburg, Studium.](#)

¹⁴² [Universität der Bundeswehr München, Beirat des Forschungsinstituts CODE.](#)
[Universität der Bundeswehr München, Forschungsinstitut CODE.](#)
[Universität der Bundeswehr München, Forschungsinstitut CODE. Unsere Mission.](#)
[Universität der Bundeswehr München, Program to the Annual Meeting CODE 2021.](#)



Bundesministerium des Innern und für Heimat (BMI)

Das Bundesministerium des Innern und für Heimat ist u.a. für die zivile Sicherheit im Cyberraum zuständig. Der Abteilung Cyber- und Informationssicherheit (CI) des BMI obliegt unter anderem die Cybersicherheit der IKT-Systeme der Bundesregierung, die Entwicklung der deutschen Cybersicherheitsstrategie, die den ressortübergreifenden, strategischen Rahmen der Bundesregierung bildet, sowie die Vorbereitung weiterer Rechtsetzung. Das BMI koordiniert die Umsetzung der Cybersicherheitsstrategie durch den:die Bundesbeauftragte:n für Informationstechnik (CIO Bund), dem auch die Zuständigkeit für die Steuerung der Bundes-IT zukommt. Weitere Referate der Abteilung CI befassen sich zudem mit den Themen Cybersicherheitsforschung, Cybersicherheit für Wirtschaft und Gesellschaft sowie den Cyberfähigkeiten deutscher Sicherheitsbehörden, insbesondere des BfV und BKA.

Das BMI ist im **NCSR** vertreten, dessen Vorsitz durch den:die CIO Bund wahrgenommen wird. Seinem Geschäftsbereich sind **BPol**, **BKA**, **BSI**, **BfV**, **BDBOS** und **BBK** zugeordnet. Die Gründung von **ZITiS** geht auf einen Erlass des BMI zurück. Der Abteilung CI kommt dabei die Fachaufsicht über das BSI, die BDBOS, der ZITiS, sowie bestimmten Einheiten des BfV und BKA zu. Ihm obliegt zudem die Aufsicht über die **DAkKS** in Cybersicherheitsfragen. Das BMI ist in den Initiativen **UP KRITIS**, **DsiN** (Beirat) sowie der **ACS** vertreten. Das BMI ist am **NKCS** beteiligt. Der **NPCS** geht auf eine BMI-Initiative zurück und wird durch das BSI operativ weitergeführt. Das BMI ist für den **IT-Rat** zuständig, den Vorsitz des IT-Rates haben der:die Chef:in des BKAmtes sowie der:die CIO Bund inne. Dem:der CIO der Bundesregierung obliegt der Vorsitz im **IT-PLR**. Das BMI gehört zu den Auftraggebern für die Umsetzung von Maßnahmen zur IT-Konsolidierung durch das **ITZBund** und ist auch in seinem Verwaltungsrat repräsentiert. Vertreter:innen des BMI sind zudem im Stiftungsrat der **SWP** sowie dem Beirat der **ITSMIG** repräsentiert. Die **Cyberagentur** wurde unter gemeinsamer Federführung des BMI und BMVg eingerichtet. Der:die Bundesinnenminister:in nimmt an der **IMK** teil. Das **Bündnis für Cybersicherheit** basiert auf einer Vereinbarung zwischen dem BMI und dem Bundesverband der deutschen Industrie. Bei der **Initiative Wirtschaftsschutz** kommt dem BMI eine koordinierende Rolle zu. Deutsche Hilfsangebote im Rahmen des **GMLZ** werden in Absprache mit BMI und AA koordiniert. Die Errichtung des **GeKoB** geht auf eine Vereinbarung zwischen dem BMI und den für das Innenressort zuständigen obersten Landesbehörden zurück. Das BMI erhält Berichte des **INTCEN** und ist an der deutschen Repräsentation im **HWPCI** beteiligt. Das BMI ist des Weiteren durch eine:n Vertreter:in im Management Board der **eu-LISA** vertreten. Auf NATO-Ebene ist es im **SC** vertreten und in den Weisungsgebungsprozess für den:die deutsche Vertreter:in im **CDC** eingebunden. Vertreter:innen des BMI haben an Treffen der IEG Cybercime (**UNODC**) teilgenommen und sind im Steering Committee des deut-



schen *IGF* (IGF-D) vertreten. Ein:e Vertreter:in des BMI ist im Governmental Advisory Committee des *ICANN* repräsentiert¹⁴³.



- **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)**

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe übernimmt Funktionen im Gesamtkonzept der nationalen Sicherheitsarchitektur. In diesem Rahmen beschäftigt es sich zunehmend auch mit den Risiken von Cyberoperationen auf Kritische Infrastrukturen. In der Vergangenheit hatte die von dem BBK organisierte und alle zwei Jahre stattfindende Länder- und Ressortübergreifenden Krisenmanagementübung (LÜKEX) bereits Bedrohungen durch Cyberoperationen zum Thema. Die LÜKEX in 2023 wird sich mit dem Thema „Cyberangriff auf das Regierungshandeln“ befassen.

*Das BBK ist im **Cyber-AZ** vertreten und sein Personal besetzt das **GMLZ**. Es gehört zum Geschäftsbereich des **BMI** und ist im **UP KRITIS** sowie der **ACS** vertreten. Ihm steht der durch die **BDBOS** betriebene Digitalfunk zur Verfügung. Das **GeKoB** wurde beim BBK angesiedelt, welches auch die GeKoB-Geschäftsstelle stellt. Das **BSI** arbeitet mit dem BBK zusammen, um Effekte von Risiken für die Verfügbarkeit Kritischer Infrastrukturen zu analysieren¹⁴⁴.*



- **Gemeinsames Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern (GeKoB)**

Im Rahmen des GeKoB soll u.a. durch intensivierten Informationsaustausch, dem Aufbau von Fähigkeiten im Prognosebereich sowie der Unterstützung politisch-strategischer Bund- und Länder-Krisenstäbe eine verbesserte Koordination zwischen Akteuren im Bevölkerungsschutz ermöglicht werden. Dadurch soll zur Vorbeugung etwaiger Krisen, verstärktem Krisenmanagement sowie, je nach vorherrschender Lagesituation oder auftretenden Gefahren, zu einer zeitnahen gemeinsamen Reaktion beigetragen werden, sofern diese erforderlich ist. Das GeKoB verantwortet das Gemeinsame Lagebild Bevölkerungsschutz, welches alle zwei Wochen erstellt wird. Bei Bedarf kann das GeKoB lageangepasst beispielsweise personell aufwachsen oder einen 24/7-Betrieb sicherstellen.

143 [Bundesministerium des Innern, für Bau und Heimat, Cyber-Sicherheitsstrategie für Deutschland. Bundesministerium des Innern, für Bau und Heimat, IT & Cybersicherheit. Bundesministerium des Innern, für Bau und Heimat, Unsere Abteilungen und ihre Aufgaben. Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land 2018.](#)

144 [Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Gemeinsames Melde- und Lagezentrum von Bund und Ländern. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Krisenübung für den Bevölkerungsschutz. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, LÜKEX 22: Cyberangriff auf das Regierungshandeln.](#)



Das GeKoB wurde beim **BBK** angesiedelt, welches auch die GeKoB-Geschäftsstelle stellt. Seine Errichtung geht auf eine Vereinbarung zurück die zwischen dem **BMI** (für den Bund) sowie den für das Innenressort zuständigen obersten Landesbehörden (u.a. **IM BW**, **StMI [BY]**, **SenInnDS [BE]**, **MIK [BB]**, **MIBD MV**, **MI [NI]**, und **IM NRW**) geschlossen wurde. Diese bilden den „Kern des Kompetenzzentrums“. Für den Bund wird sich zudem auch die Bundeswehr (**BMVg**) und die **BPol** am GeKoB beteiligen. Bei Bedarf können zudem weitere Fachbehörden beteiligt werden. Die Leitung des GeKoB wechselt alle zwei Jahre zwischen Bund und Ländern. Die strategische Steuerung des GeKoB verantwortet ein Lenkungskreis, in dem Bund und die sechzehn Bundesländer auf gleichberechtigter Basis vertreten sind. Das GeKoB arbeitet eng mit dem **GMLZ** zusammen, mit welchem es auch (gemeinsam mit der KRITIS-Zelle) die redaktionelle Betreuung des Gemeinsamen Lagebildes Bevölkerungsschutz sichergestellt¹⁴⁵.



– **Gemeinsames Melde- und Lagezentrum von Bund und Ländern (GMLZ)**

Das Gemeinsame Melde- und Lagezentrum (GMLZ) hat die Aufgabe für Bund, Länder und Fachbehörden ein einheitliches Lagebild für den Bevölkerungsschutz abzubilden. Dafür verfolgt und bewertet es rund um die Uhr relevante Geschehnisse im In- und Ausland und berichtet im täglichen Lagebericht oder gezielten Lagemeldungen. Neben seiner Rolle im Lagemanagement und als nationale Kontaktstelle kann das GMLZ im Falle von „großflächigen bevölkerungsschutzrelevanten Ereignissen, Ereignissen von länderübergreifender oder bundesweiter Bedeutung [...] sowie erheblichen Störungen Kritischer Infrastruktur“, die beispielsweise durch gezielte Cyberoperationen herbeigeführt werden könnten, unterstützend im Ressourcenmanagement tätig werden und sogenannte Engpassressourcen vermitteln.

Das **BBK** ist im GMLZ vertreten. Partner des GMLZ sind unter anderem **BPol**, **BKA** und die **EK**. Es arbeitet mit dem **LZ** zusammen. Im Bedarfsfall leitet das GMLZ Aktivierungsanfragen für das Katastrophen- und Krisenmanagement der EU an das **ERCC** weiter. Hilfsangebote Deutschlands werden durch das GMLZ in Absprache mit dem **BMI** und **AA** koordiniert. Das **GeKoB** arbeitet eng mit dem GMLZ zusammen, mit welchem es auch (gemeinsam mit der KRITIS-Zelle) die redaktionelle Betreuung des Gemeinsamen Lagebildes Bevölkerungsschutz sichergestellt¹⁴⁶.

145 [Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Das Gemeinsame Kompetenzzentrum Bevölkerungsschutz, Bundesministerium des Innern und für Heimat, Bund und Länder geben Startschuss für das Gemeinsame Kompetenzzentrum Bevölkerungsschutz.](#)

[Bundesregierung, Das Gemeinsame Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern. Ministerium des Innern des Landes Nordrhein-Westfalen, Verwaltungsvereinbarung über die Errichtung des Gemeinsamen Kompetenzzentrum Bevölkerungsschutz.](#)

146 [Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Ressourcenmanagement. Bundesministerium des Innern, für Bau und Heimat, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.](#)

[Deutsches Zentrum für Luft- und Raumfahrt, Katastrophen- und Krisenmanagement.](#)



- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Dem Bundesamt für Sicherheit in der Informationstechnik kommt als zentraler nationaler Stelle für die Informationssicherheit die Aufgabe zu, Sicherheit in der Informationstechnik des Bundes zu stärken und den Schutz der Regierungsnetze zu gewährleisten. Hierzu ist es u.a. zur Abwehr entsprechender Gefahren und Risiken sowie deren Sammlung und Analyse befugt und stellt für Einrichtungen des Bundes auch IT-Sicherheitsprodukte zur Verfügung.

Das BSI ist zudem eine zentrale Meldestelle sowohl für Bundesbehörden als auch Dritte und übernimmt die Funktion als zentrale Stelle für informationstechnische Sicherheit in Bezug auf Kritische Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse oder digitale Dienste. Es kann entsprechende zielgruppenspezifische Warnungen, beispielsweise vor Sicherheitslücken, aussprechen oder „Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen“. Zudem ist das BSI für die Cybersicherheitszertifizierung zuständig.

In Absprache mit den Bundesressorts legt das BSI darüber hinaus für die Informationstechnik des Bundes sicherheitsbezogene Mindeststandards fest, die u.a. von Stellen des Bundes umgesetzt werden müssen. Gegenüber Ressorts der Bundesregierung wird das BSI auf der „Grundlage wissenschaftlich-technischer Erkenntnisse“ (§1 BSIG) tätig. Um im Falle eines IT-Sicherheitsvorfalls von herausragender Bedeutung unmittelbar Abhilfe leisten zu können, verfügt das BSI über Mobile Incident Response Teams (MIRT), die an Bundesverwaltung sowie KRITIS-Unternehmen entsendet werden können.

Als Behörde mit technischer Expertise fördert es darüber hinaus die Informations- und Cybersicherheit in Verwaltung, Wirtschaft und Gesellschaft durch zahlreiche Aktivitäten, Kooperationen und Initiativen. Auf Wunsch der Bundesländer kann das BSI diese in gewissem Rahmen in Fragen der IT-Sicherheit beraten und unterstützen. Ähnliche Angebote von Information, über Beratung bis hin zu technischem Support sowie der Bereitstellung technischer Schutzmaßnahmen stehen auch deutschen Kommunen auf deren Anfrage zur Verfügung.

Um sich regional noch stärker zu vernetzen hat das BSI deutschlandweit Verbindungsbüros in den Städten Berlin (zuständig für Berlin und Brandenburg), Hamburg (zuständig für die Region Nord: Hamburg, Bremen, Niedersachsen, Schleswig-Holstein, Sachsen-Anhalt und Mecklenburg-Vorpommern), Wiesbaden (zuständig für die Region Rhein-Main: Hessen, Saarland und Rheinland-Pfalz), Bonn (zuständig für die Region West: Nordrhein-Westfalen) und Stuttgart (zuständig für Region Süd: Baden-Württemberg und Bayern) aufge-



baut. Der Zweitstandort des BSI in Freital übernimmt unter anderem die Arbeit des Verbindungswesens in der Region Ost (Thüringen und Sachsen). Ein dritter Standort des BSI mit dem Schwerpunktthema KI wurde in Saarbrücken eröffnet.

Jährlich veröffentlicht das BSI einen Lagebericht zur IT-Sicherheit in Deutschland. Der Koalitionsvertrag sieht vor, dass BSI im Laufe der aktuellen Legislaturperiode „unabhängiger“ aufzustellen.

Das BSI gehört zum Geschäftsbereich des BMI (Fachaufsicht durch Abteilung CI) und ist an der UP KRITIS beteiligt. Es beherbergt unter anderem das Cyber-AZ, die ACS, das LZ, das CERT-Bund, das BSOC, das Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt, das CSN und das Bürger-CERT. Das BSI fungiert als Single Point of Contact des NKCS. Es ist Mitglied des NCSR. Es ist beratendes Mitglied in der AG InfoSic des IT-PLR. Der NPCS geht auf eine BMI-Initiative zurück und wird durch das BSI operativ weitergeführt. Sofern zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, erforderlich, kann das BSI auch gegenüber anderen Stellen wie Polizeien, Strafverfolgungsbehörden aber auch Verfassungsschutzbehörden (BfV und LfV's), dem MAD oder dem BND unterstützend tätig werden. Das BSI arbeitet mit dem BBK zusammen, um Effekte von Risiken für die Verfügbarkeit Kritischer Infrastrukturen zu analysieren. Neben Bundes- und Landesverwaltungen erhalten auch alle im VCV organisierten Länder-CERTs anlassbezogene Cybersicherheitswarnungen durch das BSI. Das CERT-Bund ist zudem selbst am VCV beteiligt. Zusammen mit dem ITZBund hat das BSI einen „Lenkungskreis Informationssicherheit“ etabliert und eine Rahmenverwaltungsvereinbarung geschlossen, die eine engere Zusammenarbeit zwischen beiden Institutionen ermöglichen sollen. Das BSI hat zudem eine Kooperationsvereinbarung mit dem vzbz unter anderem bezüglich digitalen Verbraucherschutzes geschlossen. Im Falle eines Cybersicherheitsvorfalls tauscht die BaFin Informationen mit dem BSI aus. Zur Sicherung der NdB arbeitet die BDBOS als Partnerbehörde mit dem BSI zusammen. Zudem kooperiert das BSI mit dem:der BfDI und im Bereich des digitalen Verbraucherschutzes mit dem BKartA. Das BSH hat mit dem BSI eine Verwaltungsvereinbarung zur Stärkung der Cybersicherheit in der Seeschifffahrt unterzeichnet. Ebenso wurde mit der BWI Absichtserklärung zur verstärkten Zusammenarbeit geschlossen. Der Umsetzungsrahmen von TIBER-DE der D BBk wurde mit Beteiligung des BSI erarbeitet. Das BSI ist im Beirat des DsiN sowie des Cyber Security Clusters Bonn vertreten und kooperiert mit dem G4C. Darüber hinaus ist es im Aufsichtsrat der DAKkS und im Steuerungskreis der Initiative IT-Sicherheit in der Wirtschaft vertreten. Im Rahmen einer Verwaltungsvereinbarung haben das BSI und die DAKkS außerdem eine verstärkte Zusammenarbeit vereinbart, unter anderem mit einem Fokus auf Akkreditierungsverfahren für Cybersicherheitsprüfungen. Es ist auch an der Initiative Wirtschaftsschutz beteiligt. Gemeinsam mit der



BNetzA hat das BSI den IT-Sicherheitskatalog für Strom- und Gasnetze herausgebracht, zu dessen Umsetzung alle Betreiber verpflichtet sind. Der wissenschaftlichen Arbeitsgruppe des NCSR gehört neben wissenschaftlichen Vertreter:innen auch ein:e Repräsentant:in des BSI an. Auf Länderebene arbeitet das BSI unter anderem mit dem IM BW, dem IT.NRW, dem LSI, dem MASTD, dem MIBD MV, dem MI Niedersachsen, dem saarländischen Ministerium für Finanzen und Europa, der SenInnDS, der SK [SN] sowie der ZAC NRW zusammen bzw. steht mit diesen in Austausch. Die nordrhein-westfälische Koordinierungsstelle für Cybersicherheit ist als zentrale Kontaktstelle des Landes gegenüber dem BSI designiert. Mit dem Land Niedersachsen (NI) und dem Saarland (SL) hat das BSI eine Kooperationsvereinbarung unterzeichnet und arbeitet in diesem Rahmen im Saarland mit DiNet und CYBR360 zusammen. Zudem besteht eine Vereinbarung über den Informationsaustausch und die Zusammenarbeit in der Informationssicherheit mit Dataport. Das Berliner Verbindungsbüro des BSI steht in Austausch mit dem CDC-Lv. Das BSI unterstützt das IT-SiBe-Forum und hat gemeinsam mit den KSV unter anderem ein IT-Grundschutzprofil für Kommunen erarbeitet. Alle zwei Jahre muss das BSI der EK bestimmte Informationen übermitteln und erstattet auch der NIS Cooperation Group jährlich Bericht, u.a. zu Zahl und Art gemeldeter Sicherheitsvorfälle. Es arbeitet mit der ENISA und der EZB zusammen, ist für Deutschland im Verwaltungsrat des ECCC vertreten sowie dem Board des ECSO, ist Mitglied im SOG-IS sowie der Stakeholder Community des EU CyberNet. Zudem ist das BSI in NATO-Gremien (CDC, C3B und SC) vertreten bzw. an entsprechenden Weisungsprozessen beteiligt. Gegenüber der NATO ist das BSI von deutscher Seite als nationale „NATO Cyber Defence Authority“ (NCDA) benannt. Von NATO-Seite wurde diese Vereinbarung durch die ESCD geschlossen¹⁴⁷.



– **Allianz für Cybersicherheit (ACS)**

Die Allianz für Cyber-Sicherheit bietet einen vertrauensvollen Austausch und entsprechende Netzwerk- sowie Veranstaltungsformate zwischen den über 6.000 Mitgliedern und dem Bundesamt für Sicherheit in der Informations-

¹⁴⁷ [Bundesamt für Justiz, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik \(BSI-Gesetz – BSIg\). Bundesamt für Sicherheit in der Informationstechnik, Auftrag.](#)
[Bundesamt für Sicherheit in der Informationstechnik, BSI und das Saarland rücken enger zur Stärkung der Cyber-Sicherheit zusammen.](#)
[Bundesamt für Sicherheit in der Informationstechnik, Bundesgesetzblatt Teil I Nr. 54, Jahrgang 2009, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes.](#)
[Bundesamt für Sicherheit in der Informationstechnik, Themen.](#)
[Bundesamt für Sicherheit in der Informationstechnik, Vorfallsunterstützung.](#)
[Bundesamt für Sicherheit in der Informationstechnik, Zweitstandort der Bundesbehörde BSI entsteht in Freital. \(Webseite entfernt\)](#)
[Bundesregierung, Besserer Schutz vor Cyber-Angriffen.](#)
[Deutscher Bundestag \(Drucksache 19/3398\), Antwort der Bundesregierung auf die Kleine Anfrage: Nationale und internationale Kooperationen des Bundesamtes für die Sicherheit in der Informationstechnik.](#)
[Hintergrundgespräche, 2019.](#)
[Fabienne Tegeler, Angebote des BSI für Kommunen.](#)
[Lina Rusch, BSI bekommt KI-Ableger in Saarbrücken.](#)
[Sozialdemokratische Partei Deutschlands, BÜNDNIS 90/DIE GRÜNEN, Freie Demokratische Partei, Mehr Fortschritt Wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit.](#)



technik zu Cyberbedrohungen, Schutzmaßnahmen und Vorfallsmanagement. Außerdem erhalten die Mitglieder Informationen wie aktuelle Lagebilder oder Warnungen im Rahmen eines Online-Informationspools und können ihre Cybersicherheitskompetenzen durch kostenfreie Partnerangebote ausbauen. Mitglied kann jede Institution mit Sitz in Deutschland werden, die Teilnahme ist kostenlos. Mitglieder können sich in der ACS auch als Partner oder Multiplikatoren engagieren. Die Arbeit der ACS wird durch einen Beirat begleitet, welcher auch Impulse für ihre zukünftige Aufstellung leistet.

*Die ACS ist im **BSI** angesiedelt und wurde als eine Public-Private-Partnership zwischen BSI und Bitkom ins Leben gerufen. Im Beirat der ACS sind unter anderem Vertreter:innen aus **BMI** und **BSI** Mitglied. Das **CSN** ist mit der ACS verbunden, die es durch reaktive Angebote ergänzt. Die ACS ist einer der Adressaten des täglichen Lageberichts IT-Sicherheit des **LZ**. Teilnehmer:innen der ACS sind unter anderem das **BBK**, die **BaFin**, das **BKartA**, das **BKA**, das **BMDV**, das **BMWK**, die **Bw**, ein Institut der **UniBw** München sowie die **Vitako**. Von Akteuren auf der Länder- und Kommunalebene sind der Deutsche Landkreistag (**KSV**), das **MWIKE NRW**, die **SenInnDS**, der **SID** und die **ZCB** Mitglied. Das **MI** Niedersachsen engagiert sich als Multiplikatoren in der ACS. Die **TISiM** tauscht sich mit seinen Projektträgern im Rahmen der ACS aus. Die ACS kooperiert mit **DsiN**¹⁴⁸.*



– **Bundes Security Operations Center (BSOC)**

Das Bundes Security Operations Center nutzt Systeme und Verfahren zur Detektion und Analyse, wie beispielsweise Antivirus-Signaturen, technische Plattformen und Detektoren um zielgerichtete und komplexe Operationen zu erkennen und so zum Schutz der Regierungsnetze und Bundes-IT beitragen zu können. Diese immer wieder neu an die Bedrohungslage angepassten und größtmöglich automatisierten Instrumente operativer Cybersicherheit beinhalten unter anderem die „Erfassung und Auswertung von Protokollierungs- und Sensordaten sowie [...die] Erkennung und Abwehr von Schadsoftware in E-Mails und im Webverkehr“. Es wurde zudem ein BSOC-Verbund etabliert, der BSI und IT-Dienstleister des Bundes vernetzen soll.

*Das BSOC wird durch das **BSI** betrieben und arbeitet mit dem **CSOCBw** (**ZCSBw**) zusammen. Neben der **BWI** sind **AA**, **BDBOS** und **ITZBund** Teil des BSOC-Verbundes¹⁴⁹.*

¹⁴⁸ [Bundesamt für Sicherheit in der Informationstechnik, 10 Jahre Allianz für Cyber-Sicherheit.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Allianz für Cyber-Sicherheit.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Allianz für Cyber-Sicherheit – Über uns.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Beirat der Allianz für Cyber-Sicherheit.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Teilnehmerliste der Allianz für Cyber-Sicherheit.](#)

¹⁴⁹ [Bundesamt für Sicherheit in der Informationstechnik, Abteilung OC – Operative Cyber-Sicherheit.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Digitalisierung in der Bundesverwaltung absichern.](#)

[Bundesweite IT-Systemhaus GmbH, Cyber-Sicherheit: BSI und BWI wollen künftig enger zusammenarbeiten.](#)



- **Computer Emergency Response Team der Bundesverwaltung (CERT-Bund)**
Das Computer Emergency Response Team des Bundes ist Notfallteam und Anlaufstelle für alle Bundesbehörden im Falle eines sicherheitsrelevanten IT-Vorfalles. Darüber hinaus spricht es präventive und ggf. reaktive Handlungsempfehlungen aus. Weiterhin weist es auf Schwachstellen hin, schlägt Maßnahmen zu ihrer Behebung vor und ist 24 Stunden täglich erreichbar. Neben dem CERT-Bund verfügt das BSI ebenfalls über ein Bürger-CERT, welches als Warn- und Informationsdienst für Privatpersonen Interessierte kostenlos über aktuelle Sicherheitslücken informiert.

*Das CERT des Bundes ist im **BSI** aufgehängt und arbeitet mit dem **LZ** zusammen. Im Bedarfsfall wächst das **IT-KRZ** gemeinsam aus LZ und CERT-Bund auf. Es kooperiert mit dem **CERT-Verbund** und im Rahmen des VCV auch mit den **Länder-CERTs**. Weitere Arbeitsbeziehungen bestehen unter anderem mit dem **Hessen3C**. Auf europäischer Ebene arbeitet CERT-Bund mit der **EGC Group** sowie der **ENISA** zusammen. Es ist zudem am **CSIRTs Netzwerk**, der **TF-CSIRT** und **FIRST** beteiligt sowie bei **TI** akkreditiert¹⁵⁰.*



- **Cyber-Sicherheitsnetzwerk (CSN)**
Das kürzlich ins Leben gerufene Cyber-Sicherheitsnetzwerk operiert als freiwilliger Zusammenschluss qualifizierter Expert:innen, durch das eine flächendeckende dezentrale Struktur zur Ermöglichung einer „digitalen Rettungskette“ in der Reaktion und Vorfallsbearbeitung von IT-Sicherheitsvorfällen aufgebaut werden soll. Das CSN soll hier als erste Anlaufstelle für KMU und individuelle Bürger:innen dienen. Die Unterstützungsleistungen können variieren und sehen Hilfe zur Selbsthilfe, eine Kontakt-Hotline, digitale Ersthelfer:innen, Vorfall-Expert:innen oder IT-Dienstleister mit einem Team von Vorfall-Expert:innen vor. Zu diesem Zwecke hat das CSN zudem ein Qualifizierungsprogramm etabliert, durch welches systematisch vor Ort Digitale Ersthelfer:innen und Vorfalls-Expert:innen nach einem einheitlichen Ausbildungsprogramm geschult werden sollen. Zusätzlich sollen Räume für kollektiven Erfahrungsaustausch geschaffen und diese gesammelt werden, um die Zielgerichtetheit von Empfehlungen in Bezug auf präventive Maßnahmen sowie auch reaktive Tätigkeiten des CSN selbst zu verbessern. Das CSN wird durch eine Geschäfts- und Koordinierungsstelle unterstützt, die jeweils die Organisation des CSN und seine strategische Ausrichtung verantworten.

¹⁵⁰ [Bundesamt für Sicherheit in der Informationstechnik, CERT-Bund.](#)
[Bundesamt für Sicherheit in der Informationstechnik, Nationale und internationale Zusammenarbeit.](#)
[CERT-Bund, Über CERT-Bund.](#)



Das CSN ist institutionell im **BSI** angesiedelt und mit der **ACS** verbunden, die es durch reaktive Angebote ergänzt. Das Saarland (**SL**) ist eine Pilotregion des CSN¹⁵¹.



– **Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt**

Die Etablierung des Kompetenzzentrums für IT-Sicherheit für Luft- und Raumfahrt ist bis 2022 geplant. Es soll im Kontext von „zivilbehördlichen sowie militärischen Luft- und Raumfahrtanwendungen und -systemen“ tätig werden und eine koordinierende Funktion in Deutschland übernehmen. Für seinen Tätigkeitsbereich soll das Kompetenzzentrum u.a. cybersicherheitsrelevante Mindestanforderungen durch Erarbeitung eines Anforderungskatalogs und einer Technischen Richtlinie bestimmen. Darüber hinaus soll das Kompetenzzentrum u.a. zudem hierzu beratend tätig werden sowie für generelle Auskünfte, beispielsweise zu relevanten Cybersicherheitsstandards oder der Bedrohungssituation, zur Verfügung stehen.

*Institutionell wird das Kompetenzzentrum im **BSI** angesiedelt sein¹⁵².*



– **Nationaler Pakt Cybersicherheit (NPCS)**

Der Nationale Pakt Cybersicherheit soll als deutscher Beitrag den Paris Call for Trust and Security in Cyberspace unterstützen, wozu jährlich ein nationaler Beitrag veröffentlicht werden soll. Ziel ist es, alle gesellschaftlich relevanten Gruppen, Hersteller, Anbieter und Anwender sowie die öffentliche Verwaltung in einem Nationalen Pakt einzubinden, in dem die gemeinsame Verantwortung für digitale Sicherheit niedergelegt wird. Im Rahmen des Paktes wurden in einem Online-Kompendium wesentliche Akteure der Cybersicherheit in Deutschland erfasst sowie eine gesamtgesellschaftliche Erklärung zur Cybersicherheit verfasst.

*Der NPCS geht auf eine **BMI**-Initiative zurück und wird durch das **BSI** operativ weitergeführt. Teil des Paktes sind unter anderem das **Bündnis für Cybersicherheit** und die **Cyberagentur**¹⁵³.*

151 [Bundesamt für Sicherheit in der Informationstechnik, Curriculum zur Qualifikation von Vorfall-Experten.](#)

[Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheitsnetzwerk.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheitsnetzwerk: Informationen zum Cyber-Sicherheitsnetzwerk.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Saarland wird zweite Pilotregion des Cyber-Sicherheitsnetzwerks.](#)

152 [Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheit für Weltraumanwendungen.](#)

153 [Bundesministerium des Innern, für Bau und Heimat, Gesamtgesellschaftliche Erklärung zur Cybersicherheit.](#)

[Bundesministerium des Innern, für Bau und Heimat, Nationaler Pakt Cybersicherheit.](#)

[Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Nationaler Pakt Cybersicherheit.](#)



– **Nationales IT-Lagezentrum (LZ)**

Das 24 Stunden täglich operierende Nationale IT-Lagezentrum hat die Aufgabe, ein IT-Lagebild zu erstellen, um auftretende IT-Sicherheitsvorfälle für staatliche Stellen und Wirtschaftsunternehmen rechtzeitig zu entdecken, schnell einschätzen zu können sowie ggf. vorbeugende Maßnahmen früh ergreifen zu können und Handlungsempfehlungen vorzubereiten. Dies wird über konstantes Monitoring von und Auswertung verschiedenster Quellen erreicht, die in der Gesamtschau eine möglichst umfassende Übersicht zu der IT-Sicherheitslage in der Bundesrepublik liefern. Die Erkenntnisse des LZ leisten zusätzlich einen langfristigen Beitrag zur Arbeit des BSI, da durch diese auch Anpassungs- oder Aktualisierungsbedarf von entsprechenden Maßnahmen oder Richtlinien identifiziert werden kann. KRITIS-Betreibern steht im LZ ein:e spezielle:r Ansprechpartner:in zur Verfügung.

Das LZ ist im BSI angesiedelt arbeitet mit dem GMLZ, CERT-Bund und Cyber-AZ zusammen. Der tägliche Lagebericht IT-Sicherheit des LZ geht unter anderem an UP KRITIS, den VCV sowie die ACS. Die Kapazitäten und Strukturen des LZ erlauben es zudem, gemeinsam mit dem CERT-Bund gegebenenfalls zum IT-KRZ aufzuwachsen¹⁵⁴.



– **Nationales IT-Krisenreaktionszentrum (IT-KRZ)**

Das IT-KRZ tritt bei Bedarf zur „Reaktion und Bewältigung von schweren Cyber-Sicherheitsvorfällen und IT-Krisen“ zusammen. In solchen Situationen übernimmt das IT-KRZ fallspezifische Analysen und Bewertungen, auf deren Basis weitere Maßnahmen vorgenommen werden können. Zusätzlich kommt dem IT-KRZ in solchen Fällen eine Koordinierungsfunktion zwischen relevanten oder betroffenen Organisationen zu. Organisatorisch ist das IT-KRZ dabei flexibel aufgestellt und kann sich quantitativ sowie auch fachlich situationsbedingt je nach Eskalationsgrad oder Lageeinschätzung zusammensetzen.

Im Bedarfsfall wächst das IT-KRZ gemeinsam aus LZ und CERT-Bund auf¹⁵⁵.



– **Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS)**

Das NKCS ist in ein Netz zu errichtender nationaler Koordinierungszentren aus allen EU-Mitgliedsstaaten eingebettet. Dadurch sollen Investitionen in

¹⁵⁴ [Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021.](#)
[Bundesamt für Sicherheit in der Informationstechnik, Immer im Einsatz: Ein Tag im nationalen IT-Lage- und Analysezentrum.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Nationales IT-Lagezentrum.](#)
[Deutscher Bundestag \(Drucksache 19/2645\), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.](#)

¹⁵⁵ [Bundesamt für Sicherheit in der Informationstechnik, Das Nationale IT-Krisenreaktionszentrum im BSI.](#)



Cybersicherheitsforschung und -entwicklung innerhalb der EU über Landesgrenzen hinweg und zwischen unterschiedlichen Sektoren vereinfacht und verstärkt aufeinander abgestimmt werden. Auf nationaler Ebene möchte das NKCS hierzu u.a. für Interessierte eine Informationsplattform etablieren, das Netzwerken untereinander unterstützen und Beratungsmöglichkeiten bereitstellen. Als Zielgruppe sollen vor allen Dingen KMUs und Start-ups angesprochen und involviert werden.

Das NKCS ergänzt als nationaler Counterpart die Aufgaben des ECCO auf EU-Ebene. Am NKCS beteiligt sind das BMI, BMWK, BMBF, BMVg und CODE. Während die Gesamtkoordination des NKCS durch das BMI verantwortet wird, ist die Kopfstelle (Single Point of Contact) des NKCS im BSI angesiedelt¹⁵⁶.



- **Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)**

Der BDBOS obliegt der Betrieb des Digitalfunks BOS sowie der Netze des Bundes (NdB). Ersterer stellt ein Funknetz als Kommunikationsmittel für alle Behörden und Organisationen mit Sicherheitsaufgaben in Bund und Ländern sicher. In letzteren wurden unter anderem der Informationsverbund Berlin-Bonn (IVBB) sowie der Informationsverbund der Bundesverwaltung/Bundesverwaltungsnetz (IVBV) zu einer einheitlichen Netzinfrastruktur zusammengeführt. Langfristig soll die derzeitige Struktur gemeinsam mit dem Bund-Länder-Kommunen-Verbindungsnetz (NdB-VN) in den Informationsverbund der öffentlichen Verwaltung (IVÖV) aufgehen.

Die BDBOS gehört zum Geschäftsbereich des BMI und der: die CIO Bund übernimmt den Vorsitz des Verwaltungsrates der BDBOS. Zur Sicherung der NdB arbeitet die BDBOS als Partnerbehörde mit dem BSI zusammen. Der Digitalfunk steht unter anderem der BPol, dem BKA, ZKA, BBK sowie dem BfV und den LfV zur Verfügung. Es ist zudem am BSOC-Verbund beteiligt¹⁵⁷.

¹⁵⁶ [Bundesamt für Sicherheit in der Informationstechnik, Das Nationale Koordinierungszentrum für Cybersicherheit nimmt Arbeit auf.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Nationales Koordinierungszentrum für Cybersicherheit \(NKCS\).](#)

[Bundesministerium des Innern und für Heimat, Nationales Koordinierungszentrum für Cybersicherheit \(NKCS\).](#)

¹⁵⁷ [Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Chronik.](#)

[Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Die Bundesanstalt.](#)

[Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Netze des Bundes.](#)

[Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Netze des Bundes – Zukunftsweisende Kooperation vereinbart.](#)

[Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Nutzergruppen.](#)

[Bundesregierung, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme.](#)



- **Bundesamt für Verfassungsschutz (BfV)**

Das Bundesamt für Verfassungsschutz untersucht und beobachtet, wie neue technische Möglichkeiten von anderen Staaten – beispielsweise durch ihre Nachrichtendienste – genutzt werden, um in Deutschland Spionage, Desinformation oder Computersabotage zu betreiben. Dies umfasst auch die Nutzung von „in Deutschland gehostete[r] Infrastruktur von fremden Akteuren“, die zur Durchführung von Cyberoperationen gegen ausländische Akteure genutzt wird. Cyberoperationen mit kriminellem Hintergrund fallen explizit nicht in das Aufgabenportfolio des BfV. Das BfV versucht Cyberoperationen auf staatliche und private Einrichtungen in Deutschland abzuwehren und aufzuklären. Neben der Detektion und Prävention übernimmt die Cyberabwehr des BfV auch Aufgaben zur Attribution von Cyberoperationen, beispielsweise zu einem Staat oder einer APT-Gruppierung. Jährlich veröffentlicht das BfV einen Verfassungsschutzbericht, der unter anderem auch über den Status quo der Bedrohung durch Cyberoperationen und etwaiger Vorkommnisse in Deutschland informiert. In unregelmäßigen Abständen werden auch öffentlich zugängliche sog. Cyber-Briefs publiziert, in denen über bestimmte Bedrohungen unterrichtet wird.

*Das BfV gehört zum Geschäftsbereich des **BMI**. Anlassbezogene eingestufte Berichte („Cyber-Spezial“) gehen von Seiten des BfV an **BMI**, **BKAmt** sowie das **AA**. Zwischen BfV, **BND** und **BAMAD** werden Informationen ausgetauscht und es bestehen gegenseitige Unterrichtungspflichten. Das BfV kann, sofern zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, erforderlich, durch das **BSI** unterstützt werden. Es ist im **Cyber-AZ** und der **Initiative Wirtschaftsschutz** vertreten und greift auf die Expertise von **ZITIS** zurück. Ihm steht der durch die **BDBOS** betriebene Digitalfunk zur Verfügung. Darüber hinaus besteht Austausch seitens der Cyberabwehr des BfV mit ihren entsprechenden Counterparts in den Landesbehörden für Verfassungsschutz (**LfV**), sofern vorhanden. In der Vergangenheit wurde der Aufgabenbereich der Cyberabwehr im Rahmen einer Verwaltungsvereinbarung seitens der Berliner **SenInnDS** an das BfV übertragen. Es zählt zu den Empfängern von **INTCEN**-Berichten und trägt auch selber Informationen bei und entsendet Mitarbeiter:innen an das **INTCEN**¹⁵⁸.*



- **Bundeskriminalamt (BKA)**

Das Bundeskriminalamt hat als Zentralstelle der deutschen Polizei sein Aufgabenfeld der nationalen Verbrechensbekämpfung auch auf den Cyberraum

¹⁵⁸ [Bundesamt für Verfassungsschutz, Cyberabwehr.](#)
[Bundesamt für Verfassungsschutz, Cyberabwehr: Begriff und Auftrag.](#)
[Bundesamt für Verfassungsschutz, Akteure und Angriffsmethoden.](#)
[Deutscher Bundestag \(Drucksache 19/2645\), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.](#)

ausgeweitet. Es klärt Straftaten im Cyberraum auf, ermittelt und versucht Cyberkriminalität vorzubeugen. Dem BKA fällt hier die „originäre Strafverfolgungskompetenz in Fällen von Cybercrime unter Betroffenheit von Behörden oder Einrichtungen des Bundes, der inneren oder äußeren Sicherheit Deutschlands oder zum Nachteil Kritischer Infrastrukturen“ zu. In sonstigen Fällen sind prinzipiell zunächst die Landespolizeien zuständig. Das BKA hat dazu eine Abteilung „Cybercrime“ (CC) eingerichtet, in der Kompetenzen zur Verfolgung von Cyberkriminalität im engeren Sinne gebündelt werden. Hierzu führt sie u.a. entsprechende Ermittlungen durch, geht Cyberoperationen auf Einrichtungen des Bundes sowie Kritischen Infrastrukturen nach und disruptiert „kriminelle Netzwerke und Strukturen“ auf deren Basis beispielsweise solche Cyberoperationen durchgeführt werden. Im Falle von entsprechenden Cyberoperationen verfügt das BKA auch über eine Quick Reaction Force (QRF), die zügig erste strafprozessuale Maßnahmen veranlassen kann. In der Abteilung CC ist zudem die Nationale Kooperationsstelle Cybercrime (NKC) verortet, die die Zusammenarbeit zwischen Behörden und Privatsektor verantwortet. Zur Bekämpfung der Cyberkriminalität kann das BKA unter anderem Quellen-TKÜ sowie Online-Durchsuchungen durchführen, wofür es auch Überwachungssoftware einsetzt. Zusätzlich verfügt das BKA zur Bekämpfung der Cyberkriminalität über eine 24/7-Bereitschaft. Jährlich veröffentlicht das BKA ein Bundeslagebild Cyber-Crime. Neben Cyberkriminalität untersucht das BKA auch Cyberspionage innerhalb seiner Abteilung „Staatsschutz“ (ST). Zur Bekämpfung der Cyberkriminalität hat das BKA zudem verschiedene Schulungsprogramme im Bereich der IKT-Forensik etabliert und jährlich findet eine interne Basisschulung zum Thema Cyberkriminalität statt.

Das BKA gehört zum Geschäftsbereich des BMI und zählt zu den Teilnehmern der ACS. Es ist im Cyber-AZ sowie im G4C und der Initiative Wirtschaftsschutz vertreten. Es ist Partner des GMLZ. Das BSI hat einen CSIRT-LE Liaison Officer in das BKA entsendet. Es ist im DsiN Beirat vertreten und greift auf die Expertise von ZITiS zurück. Das BKA beteiligt sich mit ZITiS am EK-finanzierten-Projekt OVERCLOCK. Auf Bundesebene übernimmt die Abteilung CC des BKA die Aufgaben der ZAC. Dem BKA steht der durch die BDBOS betriebene Digitalfunk zur Verfügung. Das BKA ist unter anderem neben der ZITiS am durch das BMBF geförderte KISTRA-Projekt beteiligt. Auf Länderebene arbeiten unter anderem das Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern, die baden-württembergische Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität und die ZCB mit dem BKA zusammen. Die ZIT ist erster Ansprechpartner des BKA für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland und bei Massenverfahren gegen mehrere Tatverdächtige deutschlandweit. Der Abteilung CC des BKA kommt auch die Geschäftsführung im Bund-Länder-Verbund der ZAC's zu. Zusammen mit den



*KSV und dem BSI hat das BKA Empfehlungen für kommunale Verwaltungen zur Reaktion auf durch den Einsatz von Verschlüsselungstrojanern zurückzuführende Lösegeldforderungen ausgesprochen. Das BKA ist der deutsche Ansprechpartner für **Europol** und dient als Nationale Stelle. Auch für **Interpol** übernimmt das BKA die Funktion als nationales Zentralbüro. Vertreter:innen des BKA haben an Sitzungen der IEG Cybercrime (**UNODC**) auf UN-Ebene teilgenommen. Dem BKA kommt die in der Budapest-Konvention des **CoE** vorgesehene Rolle als 24/7-verfügbare Kontaktstelle zu¹⁵⁹.*



- **Bundespolizei (BPol)**

Die Bundespolizei übernimmt Aufgaben im Bereich des Grenzschutzes, der Luftsicherheit, Bahnpolizei und Kriminalitätsbekämpfung. Hierunter fällt auch zunehmend die Bekämpfung von Internet- und Cyberkriminalität. Hierzu kann im Inland beispielsweise die GSG 9 als Spezialeinheit für entsprechende Zugriffe und Festnahmen eingesetzt werden. Zum Schutz ihrer Einrichtungen und der Informations- und Kommunikationstechnik betreibt sie ihr eigenes Computer Emergency Response Team (CERT BPol).

*Die BPol gehört zum Geschäftsbereich des **BMI**. Sie ist durch Verbindungsbeamte:innen des CERT BPol im **Cyber-AZ** vertreten, ist Partner des **GMLZ** und greift auf die Expertise von **ZITiS** zurück. Ihr steht der von der **BDBOS** betriebene Digitalfunk zur Verfügung. Das CERT BPol ist Gast im **CERT-Verbund**. Für den Bund wird sich u.a. auch die BPol am **GeKoB** beteiligen¹⁶⁰.*



- **Bündnis für Cybersicherheit**

Das Bündnis für Cybersicherheit soll die Zusammenarbeit zwischen Staat und Wirtschaft stärken. Das Ziel des Bündnisses ist dabei eine bessere Vernet-

¹⁵⁹ [Bundeskriminalamt, Abteilung „Cybercrime“ \(CC\).](#)

[Bundeskriminalamt, Cybercrime.](#)

[Bundeskriminalamt, Europol.](#)

[Bundeskriminalamt, Straftaten im Internet.](#)

[Bundeskriminalamt, Quellen-TKÜ und Online-Durchsuchung.](#)

[Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Bundeskriminalamt.](#)

[Datensicherheit.de, BKA: Bundeskriminalamt baut Cybercrimebekämpfung aus.](#)

[Deutscher Bundestag \(Drucksache 19/2645\), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.](#)

[European Union Agency for Cybersecurity, 2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries.](#)

¹⁶⁰ [Bundespolizei, GSG 9: Aufgaben im Inland.](#)

[Bundespolizei, Startseite.](#)

[Bundespolizei, Unterstützung anderer Bundesbehörden.](#)

[Bundespolizei kompakt, 04/2015.](#)

[Deutscher Bundestag \(Drucksache 18/13555\), Antwort der Bundesregierung auf die Kleine Anfrage: Aktuelle Situation und Ausrichtung der Bundespolizei.](#)

[European Union Agency for Cybersecurity, 2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries.](#)

[Hintergrundgespräche, 2019.](#)



zung beider Sektoren für eine effizientere Gewährleistung von Cybersicherheit – insbesondere auch im internationalen Kontext. Als Forum zwischen Bundesbehörden und Wirtschaftsvertreter:innen soll sich in Dialogformaten zu internationalen Cybersicherheitsfragen ausgetauscht werden können. Darüber hinaus hat das Bündnis das Ziel, die digitale Souveränität des Wirtschaftsstandorts Deutschland zu stärken. Gemeinsame Projekte sollen beispielsweise Abhilfe schaffen, wo eine hohe Abhängigkeit von ausländischen Technologien besteht. Es stellt eine in unregelmäßigen Abständen aktualisierte Übersicht zu nationalen Cybersicherheitsinitiativen von Staat und Wirtschaft zur Verfügung.

*Das Bündnis für Cybersicherheit ist Teil des **NPCS** und basiert auf einer Vereinbarung zwischen dem **BMI** und dem Bundesverband der deutschen Industrie e.V.¹⁶¹.*



- **Initiative Wirtschaftsschutz**

Die Initiative Wirtschaftsschutz hat das Ziel, die deutsche Wirtschaft vor Gefahren aus dem Cyberraum zu schützen. Hierzu bietet die Initiative ein umfangreiches Schutzkonzept aus Maßnahmen, Handlungsempfehlungen und Seminaren sowie ein Informationsportal unter dem Leitmotiv „Hilfe zur Selbsthilfe“ an. In letzterem wird beispielsweise auch zu Cyberabwehr und Cyberkriminalität informiert. Im Nutzerbereich können Unternehmen auf behördliche Sicherheitsempfehlungen zugreifen und bei Bedarf direkt mit ihnen Kontakt aufnehmen.

*Von staatlicher Seite sind an der Initiative Wirtschaftsschutz **BND, BfV, BKA** und das **BSI** beteiligt. Dem **BMI** kommt eine koordinierende Rolle in der Zusammenarbeit von staatlichen Stellen und Wirtschaftsverbänden zu¹⁶².*



- **IT-Rat**

Der IT-Rat ist als politisch-strategisches Gremium für übergreifende Themen der Digitalisierung sowie die Steuerung der IT der Bundesverwaltung zuständig.

*Das **BMI** ist für den IT-Rat zuständig. Den Vorsitz des IT-Rates haben der:die Chef:in des **BKAmt** sowie der:die CIO Bund inne. Alle Ressorts der Bundesregierung (u.a. **AA, BMBF, BMDV, BMF, BMG, BMJ, BMVg, BMWK, BMUV** und **BMZ**) sind durch ihre:n jeweils für IT beauftragte:n Staatssekretär:in im IT-Rat vertreten¹⁶³.*

¹⁶¹ [Bundesministerium des Innern, für Bau und Heimat, Industrie und BMI etablieren Bündnis für Cybersicherheit. Bundesverband der deutschen Industrie, Bündnis für Cybersicherheit: Industrie und Innenministerium intensivieren Kooperation.](#)

¹⁶² [Bundesamt für Verfassungsschutz, Initiative Wirtschaftsschutz. Bundesamt für Verfassungsschutz, Initiative Wirtschaftsschutz. Das Informationsportal.](#)

¹⁶³ [Der Beauftragte der Bundesregierung für Informationstechnik, IT-Rat.](#)



- **Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)**

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich entwickelt, forscht, unterstützt und berät die deutschen Sicherheitsbehörden in den Bereichen Digitale Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse. Darüber hinaus arbeitet ZITiS auch zu technischen Fragen im Bereich der Kriminalitätsbekämpfung, Gefahren- und Spionageabwehr. Hierfür entwickelt und testet es technische Werkzeuge und Methoden im Cyberbereich, verfügt aber über keine eigenen Eingriffsbefugnisse. Der Öffentlichkeit bekannte nationale und internationale Projekte mit Beteiligung von ZITiS untersuchen beispielsweise den Einsatz künstlicher Intelligenz zur Früherkennung von Straftaten (KISTRA), digitale Forensik im Bereich der Beweisanalyse (DIGFORASP) oder haben es sich zum Ziel gesetzt, einen europaweiten Standard für die forensische Untersuchung von Mobilfunktelefonen zu erarbeiten (FORMOBILE). Darüber hinaus beteiligt sich ZITiS auf EU-Ebene an einem Projekt zur Etablierung eines Netzwerks, um hybride Bedrohung effektiver bekämpfen zu können (EU-HYBNET).

ZITiS wurde vom BMI gegründet, welchem auch die Dienst- und Fachaufsicht zukommt. Sie versorgt Behörden des Bundes mit Sicherheitsaufgaben (BOS), darunter BKA, BfV, BPol, BND, ZKA sowie das BAMAD, mit ihrer Expertise. Das ZITiS-Jahresprogramm wird gemeinsam mit dem BKA, BfV sowie der BPol erstellt und durch das BMI gebilligt. ZITiS beteiligt sich mit dem BKA am EK-finanzierten Projekt OVERCLOCK. Der:die BfDI verfügt über das Recht zur Einsichtnahme in Akten, um die Einhaltung von Datenschutzvorschriften zu kontrollieren. Das BKA ist am Forschungskonsortium des KISTRA-Projektes beteiligt. KISTRA wird durch das BMBF gefördert. Weitere Projektpartner des EU-HYBNET-Projektes sind unter anderem das Hybrid CoE, GD JRC sowie die UniBw. Sie ist auf dem Campus der UniBwM angesiedelt und befindet sich so auch in geographischer Nähe zu CODE. Gemeinsam mit CODE bildet sie auch eigenes Personal im Bereich „Cyber Network Capabilities“ aus. In diesem Jahr liegt ein Schwerpunkt der Arbeit von ZITiS auf dem Aufbau eines gemeinsamen Entwicklungszentrums zum Zwecke der IT-Überwachung gemeinsam mit dem BKA. ZITiS tauscht sich mit der Cyberagentur aus¹⁶⁴.

¹⁶⁴ Andre Meister, Hacker-Behörde bekommt 66 Millionen Euro.

[Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Zentrale Stelle für Informationstechnik im Sicherheitsbereich.](#)

[EU-HYBNET, Project Partners.](#)

[Florian Flade, Mysterium ZITiS. Was macht eigentlich die "Hackerbehörde"?](#)

[Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Aufgaben & Ziele.](#)

[Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Gesetzliche Grundlage, Aufsicht und Kontrolle.](#)

[Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Forschungsprojekte.](#)

**Bundesministerium für Bildung und Forschung (BMBF)**

Das Bundesministerium für Bildung und Forschung finanziert als Teil der Digitalen Agenda drei Kompetenzzentren für IT-Sicherheitsforschung. Mit dem CISPA (Saarbrücken), ATHENE (Darmstadt) und KASTEL (Karlsruhe) soll die deutsche Forschungskapazität im Bereich der Cybersicherheit nachhaltig erhöht werden. Darüber hinaus hat das BMBF das Forschungsprogramm „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ zur Förderung multi-sektoraler Cybersicherheitsforschung sowie die Initiative StartUpSecure ins Leben gerufen, die u.a. „Unternehmensgründungen im Bereich der IT-Sicherheit“ unterstützt. Das Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän.“ hat das Forschungsprogramm „Selbstbestimmt und sicher in der digitalen Welt 2015–2020“ ersetzt.

Das BMBF ist im NCSR, dem IT-Rat sowie dem Verwaltungsrat des ITZBund vertreten und fördert die Kompetenzzentren für IT-Sicherheit. Es hat das Forschungsrahmenprogramm IT-Sicherheit „Digital. Sicher. Souverän.“ eingebracht und begleitet es. Das BMBF ist am NKCS beteiligt. Es fördert das KISTRA-Projekt, an dem unter anderem die ZITiS und das BKA beteiligt sind. Es zählt zu den Drittmittelgebern der SWP. Es hat sich an der Förderung des Cybersecurity Navigators beteiligt, der u.a. von der DKE erarbeitet wurde. Beim BMBF besteht eine koordinierende Geschäftsstelle sowie Erstinformationsstelle für Horizon Europe¹⁶⁵.

**Bundesministerium für Digitales und Verkehr (BMDV)**

Das Bundesministerium für Digitales und Verkehr ist für die Verkehrsinfrastruktur, -planung, -sicherheit sowie die digitale Infrastruktur verantwortlich. Aufgrund der sich daraus ergebenden Verantwortung für die zivile Notfallvorsorge bzw. Gefahrenabwehr, entwickelt das BMDV seine Krisenszenarien auch hinsichtlich möglicher Cyberoperationen auf digitale Infrastrukturen weiter. In der Abteilung für Digital- und Datenpolitik sind u.a. auch Zuständigkeiten für europäische und internationale Digitalpolitik angesiedelt. Unter Federführung des BMDV wird die Digitalstrategie der Bundesregierung erarbeitet.

Das BSH gehört zum Geschäftsbereich des BMDV. Ihm kommt die Fachaufsicht über einige Aufgabenbereiche der BNetzA zu. Es ist im NCSR, dem IT-Rat sowie dem Verwaltungsrat des ITZBund vertreten. Das BMDV nimmt an der ACS teil und kooperiert mit DsiN. Ein:e Vertreter:in des BMDV ist im Steering Committee des deutschen IGF (IGF-D) sowie dem Governmental Advisory Committee der ICANN vertreten. Die ITU

¹⁶⁵ [Bundesministerium des Innern, für Bau und Heimat, Online Compendium Cybersicherheit in Deutschland: Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt“ und StartUpSecure. Fraunhofer SIT, Institutsgeschichte. Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.](#)



führt von deutscher Seite das BMDV und die BNetzA als beteiligte mitgliedstaatliche Einrichtungen auf¹⁶⁶.



• **Bundesamt für Seeschifffahrt und Hydrographie (BSH)**

Das BSH verantwortet u.a. die Gefahrenabwehr in maritimen Gewässern sowie relevante Vermessungsaufgaben. Die Abteilung Schifffahrt des BSH befasst sich im Kontext von Navigations- und Kommunikationssystemen auch mit Cyberrisiken und möchte zur Verhinderung von böswilligen Cyberoperationen in seinem Zuständigkeitsbereich beitragen.

Das BSH gehört zum Geschäftsbereich des BMDV und hat mit dem BSI eine Verwaltungsvereinbarung zur Stärkung der Cybersicherheit in der Seeschifffahrt unterzeichnet¹⁶⁷.



• **Bundesministerium für Finanzen (BMF)**

Das Bundesfinanzministerium ist vorrangig für die Steuer-, Haushalts- und Europäische Finanzpolitik zuständig. Es entwickelt zum Beispiel gemeinsam mit nationalen und internationalen Partnern Mindeststandards für die Cybersicherheit in der Finanzdienstleistungsbranche.

Das BMF ist im NCSR und im IT-Rat vertreten. Ihm nachgeordnet ist das ZKA und es hat außerdem die Rechts- und Fachaufsicht über die BaFin inne. Darüber hinaus gehört das ITZBund zu seinem Geschäftsbereich. BMZ und BMF sind Gesellschafter der GIZ. Vertreter:innen des BMF sind im Aufsichtsrat der Cyberagentur, dem Kuratorium der BAKS sowie dem Stiftungsrat der SWP repräsentiert. Die Etablierung eines deutschen Pendantes zu TIBER-EU der EZB, TIBER-DE, geht auf einen gemeinsamen Beschluss der D BBk und dem BMF zurück¹⁶⁸.



• **Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)**

Die Aufgabe der Bundesanstalt für Finanzdienstleistungsaufsicht ist es, ein funktionsfähiges, integriertes und stabiles Finanzsystem in Deutschland zu gewährleisten. Im Bereich der Wirtschaftskriminalität sieht die BaFin für Versicherer, Finanzdienstleister und Banken eine zunehmende Gefahr durch Cyberkriminalität. Im Bereich der Bankenaufsicht befasst sich eine dedizierte Gruppe mit IT-Auf-

¹⁶⁶ [Bundesministerium für Verkehr und digitale Infrastruktur, Krisenmanagement.](#)

[Bundesministerium für Digitales und Verkehr, Organisationsplan des Bundesministerium für Digitales und Verkehr.](#)

¹⁶⁷ [Bundesamt für Seeschifffahrt und Hydrographie, BSH unterzeichnet Vereinbarung zur Verbesserung der Cyber-Sicherheit auf See.](#)

[Bundesamt für Seeschifffahrt und Hydrographie, Leitung und Abteilungen.](#)

[Bundesamt für Seeschifffahrt und Hydrographie, Wir über uns.](#)

[Bundesamt für Sicherheit in der Informationstechnik, Mehr Cyber-Sicherheit auf See: BSI unterzeichnet Verwaltungsvereinbarung.](#)

¹⁶⁸ [Bundesfinanzministerium, Grundelemente zur Cyber-Sicherheit. \(Webseite entfernt\) Bundesfinanzministerium, Themen.](#)



sicht/Cybersicherheit. Cyberrisiken gehören zu den von der BaFin identifizierten Fokusrisiken. Die BaFin kann u.a. bei den von ihr beaufsichtigten Institutionen entsprechende (Über)Prüfungen, beispielsweise hinsichtlich „Aspekte[n] der IT-Sicherheit und d[er] Einhaltung aufsichtlicher IT-Anforderungen“, vornehmen.

Im Falle eines Cybervorfalles besteht Informationsaustausch mit dem BSI. Die BaFin gehört zum Geschäftsbereich des BMF und ist als Partner im Cyber-AZ vertreten. Die Informationen des Cyber-AZ werden von der BaFin täglich analysiert und auf dieser Basis setzt die BaFin die Finanzindustrie über eventuelle Operationsmuster in Kenntnis. Der Umsetzungsrahmen von TIBER-DE der D BBk wurde mit Beteiligung der BaFin erarbeitet¹⁶⁹.



- **Informationstechnikzentrum Bund (ITZBund)**

Das Informationstechnikzentrum Bund ist IT-Dienstleister der Bundesverwaltung. Das ITZBund wurde als Teil einer Gesamtstrategie mit dem Ziel einer konzentrierten Bündelung der IT-Kapazitäten des Bundes aus drei Vorgängerbehörden gegründet: der Bundesstelle für Informationstechnik, der dem BMDV nachgeordneten Bundesanstalt für IT-Dienstleistungen und dem Zentrum für Informationsverarbeitung und Informationstechnik. In das Aufgabenportfolio des ITZBund fällt auch die Gewährleistung und Einhaltung eines höchstmöglichen Grades an IT-Sicherheit. In diesem Kontext stellt das ITZBund der Bundesverwaltung den Zentralen Dienst für Informationssicherheit (ZeDIS) zur Verfügung, der es ihnen ermöglicht, ihre entsprechenden Sicherheitskonzepte nach IT-Grundschutz-Anforderungen umzusetzen. Hierzu stimmt sich das ITZBund auch eng mit dem BSI ab, um beispielsweise die Verbreitung von „Security by Design“, u.a. in durch die Bundesverwaltung genutzter Software, zu stärken. Es ist auch angedacht, im Rahmen der „Bundescloud“ eine Dienstleistung zur verbesserten Entdeckung von Cyberoperationen (Detection as a Service) für die Bundesverwaltung einzurichten.

Das ITZBund gehört zum Geschäftsbereich des BMF. Der Verwaltungsrat des ITZBund setzt sich aus Staatssekretär:innen aller Bundesressorts (u.a. AA, BMBF, BMDV, BMI, BMJ, BMUV, BMVg, BMWK, BMZ und BKAm) unter Vorsitz eines:r BMF-Staatssekretär:in zusammen. Auftraggeber des ITZBund für die Umsetzung von Maßnahmen zur IT-Konsolidierung Bund sind das BMI und BMF. Zusammen mit dem BSI hat das ITZBund einen „Lenkungskreis Informationssicherheit“ etabliert sowie eine Rahmenverwaltungsvereinbarung geschlossen, die eine en-

¹⁶⁹ [Bundesanstalt für Finanzdienstleistungsaufsicht, Aufgaben & Geschichte der BaFin.](#)

[Bundesanstalt für Finanzdienstleistungsaufsicht, BaFinPerspektiven. Ausgabe 1 2020: Cybersicherheit.](#)

[Bundesanstalt für Finanzdienstleistungsaufsicht, Jahresbericht der BaFin 2021.](#)

[Bundesanstalt für Finanzdienstleistungsaufsicht, Organigramm der BaFin.](#)

[Bundesanstalt für Finanzdienstleistungsaufsicht, Risiken im Fokus der BaFin.](#)

[Bundesanstalt für Finanzdienstleistungsaufsicht, „Risiken im Fokus der Bankenaufsicht: Was tut die BaFin?“.](#)



gere Zusammenarbeit zwischen beiden Institutionen ermöglichen sollen. Es ist zudem am **BSOC**-Verbund beteiligt. Der:die **BfDI** überprüft regelmäßig die Daten- und Informationsverarbeitung des ITZBund. Das ITZBund stellt im Rahmen einer **BMG**-Förderung unter anderem Rechenzentren für den Betrieb von SORMAS (englische Bezeichnung: „Surveillance Outbreak Response Management and Analysis System“), einer IT-Lösung zur Identifikation und Nachverfolgung von Kontaktpersonen im Kontext der SARS-CoV-2-Pandemie, zur Verfügung¹⁷⁰.



- **Zollkriminalamt (ZKA)**

Das Zollkriminalamt ist für die Prävention und Aufklärung von mittlerer, schwerer und organisierter Zollkriminalität verantwortlich. Dabei koordiniert das Zollkriminalamt die Ermittlungen der einzelnen Zollfahndungsämter und kann in besonderen Fällen auch eigene Ermittlungen aufnehmen. Dies erstreckt sich auch auf den Cyberraum.

Das ZKA ist eine Fachdirektion innerhalb der Generalzolldirektion (GZD), die dem **BMF** nachgeordnet ist. Es kann als Sicherheitsbehörde des Bundes auf Dienstleistungen von **ZITIS** zurückgreifen. Ihm steht der Digitalfunk des **BDBOS** zur Verfügung. In der Vergangenheit war das ZKA Teil der deutschen Delegation für ein Treffen der IEG Cybercrime auf UN-Ebene (**UNODC**)¹⁷¹.



- **Bundesministerium für Gesundheit (BMG)**

Das Bundesministerium für Gesundheit ist vor allem für die Leistungsfähigkeit der gesetzlichen Krankenversicherung sowie der Pflegeversicherung verantwortlich. Dies schließt auch die Reform des deutschen Gesundheitssystems mit ein. Durch das E-Health-Gesetz soll eine digitale Infrastruktur mit höchsten Sicherheitsstandards im Gesundheitswesen geschaffen werden. Im Referat „Cybersicherheit und Interoperabilität“ des BMG ist u.a. die Zuständigkeit für das Krankenhauszukunftsgesetz (KHZG) oder weitere gesundheitspezifische IT-Projekte wie beispielsweise SORMAS (IT-Lösung zur Identifikation und Nachverfolgung von Kontaktpersonen im Kontext der SARS-CoV-2-Pandemie) verortet. Im Rahmen des KHZG soll durch den Krankenhauszukunftsfond die digitale Infrastruktur von Krankenhäusern verbessert werden, mindestens 15 Prozent der Fördermittel müssen dabei zur Stärkung der Informationssicherheit eingesetzt werden. Zudem fördert das BMG Modellprojekte zur Umsetzung von IT-Security–Awareness-Programmen in Einrichtungen der medizinischen Versorgung.

170 [Informationstechnikzentrum Bund, ITZBund und BSI intensivieren Zusammenarbeit für mehr IT-Sicherheit.](#)
[Informationstechnikzentrum Bund, IT-Sicherheit.](#)
[Informationstechnikzentrum Bund, Organisation und Verwaltungsrat.](#)
[Informationstechnikzentrum Bund, Über uns.](#)
[Informationstechnikzentrum Bund, Unsere Kunden.](#)
[Informationstechnikzentrum Bund, Zentraler Dienst für Informationssicherheit \(ZeDIS\).](#)

171 [Anna Loll, Datensicherheit oder Abwehr von Cyberkriminalität. Politik und Gesellschaft müssen sich mal entscheiden.](#)
[Der Zoll, Die Aufgaben des Zolls.](#)



Es ist im *NCSR* sowie dem *IT-Rat* vertreten. Das *BMG* hat die *gematik* mit dem Aufbau einer Telematikinfrastruktur beauftragt, welche die Voraussetzung für eine sichere Vernetzung des Gesundheitswesens bildet. Im Rahmen einer *BMG*-Förderung stellt das *ITZBund* unter anderem Rechenzentren für den Betrieb von *SORMAS* zur Verfügung¹⁷².



Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)

Innerhalb der Bundesregierung ist das *BMUV* auch für den Verbraucherschutz zuständig, was auch den digitalen Verbraucherschutz umfasst. In der entsprechenden Abteilung befasst sich ein Referat vor diesem Hintergrund auch mit Cybersicherheitsfragen und „vertrauenswürdiger Künstlicher Intelligenz“. Digitaler Verbraucherschutz umfasst u. a. auch Themen wie der Schutz von Verbraucher:innen vor gefälschten Verkaufsplattformen oder Dark Patterns im Internet sowie der Verbraucherdatenschutz.

Das *BMUV* ist im *NCSR*, dem *IT-Rat* sowie dem Verwaltungsrat des *ITZBund* vertreten¹⁷³.



Bundesministerium für Wirtschaft und Klimaschutz (BMWK)

Das Bundesministerium für Wirtschaft und Klimaschutz hat es sich zum Ziel gesetzt für Wirtschaft, Gesellschaft und Staat den Zugang zu einer sicheren und vertrauenswürdigen IT zu schaffen, damit diese von der Digitalisierung bestmöglich profitieren können. Das *BMWK* setzt sich dabei vor allem für IT-Sicherheit in der Industrie 4.0 und mittelständische Cybersicherheit ein.

Das *BMWK* ist im *NCSR*, dem *IT-Rat* sowie dem Verwaltungsrat des *ITZBund* vertreten und an dem *NKCS* beteiligt. Die *BNetzA* ist eine selbständige Bundesoberbehörde im Geschäftsbereich des *BMWK*. Es hat die *Initiative IT-Sicherheit in der Wirtschaft* ins Leben gerufen und nimmt an der *ACS* teil. Es ist im Beirat von *DsiN* vertreten und das *BKartA* gehören zu seinem Geschäftsbereich. Vertreter:innen des *BMWK* gehören dem Beirat der *gematik*, dem Beirat der *ITSMIG*, dem Kuratorium der *BAKS* sowie dem Stiftungsrat der *SWP* an. Es vertritt die Bundesrepublik Deutschland als Gesellschafter der *DAkkS*. Dem *BMWK* obliegt der Vorsitz im *BSIKT*, es stellt auch

172 [Bundesministerium für Gesundheit, Aufgaben und Organisation.](#)

[Bundesministerium für Gesundheit, E-Health-Gesetz.](#)

[Bundesministerium der Gesundheit, Öffentliche Bekanntmachung des Bundesministeriums für Gesundheit \(BMG\) zum Thema „Förderung von Vorhaben zur Umsetzung von IT-Security-Awareness-Programmen in Einrichtungen der medizinischen Versorgung“.](#)

[Wegweiser, Thomas Süptitz \(BMG\).](#)

173 [Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, Die digitale Souveränität von Verbraucher:innen und Verbrauchern stärken.](#)

[Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, Digitaler Verbraucherschutz.](#)

[Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, Organigramm.](#)



seine Geschäftsstelle. Der BSIKT kann gegenüber dem BMWK beratend tätig werden. Die KITS des DIN wird durch das BMWK gefördert. Das BMWK kann sich an Treffen der MAG des IGF beteiligen und unterstützt den IGF Trust Fund finanziell. Es ist zudem im Steering Committee des deutschen IGF (IGF-D) vertreten. Ein:e Vertreter:in der Physikalisch-Technischen Bundesanstalt, die zum Geschäftsbereich des BMWK gehört, hat den Vorsitz der Arbeitsgruppe 6 der UNECE (ECOSOC) inne¹⁷⁴.



- **Beirat für Standardisierung in der Informations- und Kommunikationstechnologie (BSIKT)**

Der BSIKT setzt sich aus akkreditierten Expert:innen aus Behörden, Wissenschaft, Wirtschaft sowie Verbänden zusammen. Er verfolgt das Ziel, „gemeinsame Standpunkte zu grundsätzlichen und strategischen Fragen der Normung und Standardisierung in Informations- und Kommunikationstechnologien zu erarbeiten“.

Der BSIKT kann gegenüber dem BMWK und der BNetzA beratend tätig werden. Er befasst sich mit Entwicklungen in nationalen, europäischen und internationalen Standardisierungsorganisationen/-gremien, u.a. DIN, DKE, ETSI, CEN, CENELEC, ITU, ISO, IEC, ISO/IEC JTC 1 oder der IETF. Der Vorsitz im BSIKT obliegt dem BMWK, dort ist auch die BSIKT-Geschäftsstelle angesiedelt¹⁷⁵.



- **Bundeskartellamt (BKartA)**

Dem Bundeskartellamt obliegt der Schutz des Wettbewerbs innerhalb der deutschen Wirtschaft. Unter das Mandat des BKartA fällt zudem im Rahmen der Untersuchung digitaler Märkte auch der Schutz von Verbraucherrechten, unter anderem in Bezug auf persönliche Datenverarbeitung. In der Vergangenheit hat das BKartA hierzu beispielsweise Sektoruntersuchungen zu Messenger-Diensten sowie der Authentizität von Nutzerbewertungen im Internet eingeleitet.

Das BKartA gehört zum Geschäftsbereich des BMWK. BKartA und BSI arbeiten im Bereich des digitalen Verbraucherschutzes zusammen. Es ist darüber hinaus Mitglied der ACS¹⁷⁶.

174 [Bundesministerium für Wirtschaft und Klimaschutz, Cybersicherheit im Mittelstand. Bundesministerium für Wirtschaft und Energie, IT-Sicherheit. Bundesministerium für Wirtschaft und Energie, IT-Sicherheit für die Industrie 4.0.](#)

175 [Bundesministerium für Wirtschaft und Klimaschutz, Standards und Wettbewerb. Bundesministerium für Wirtschaft und Klimaschutz, Geschäftsordnung des Beirates für Standardisierung in der Informations- und Kommunikationstechnologie \(BSIKT\). Deutscher Bundestag \(Drucksache 20/1667\), Antwort der Bundesregierung auf die Kleine Anfrage: Einführung des Mobilfunkstandards neuer Generation \(6G\).](#)

176 [Bundeskartellamt, Bundeskartellamt und BSI: Partner im Dienst der Verbraucherinnen und Verbraucher. Bundeskartellamt, Bundeskartellamt leitet Sektoruntersuchung zu Messenger-Diensten ein. Bundeskartellamt, Gefälschte und manipulierte Nutzerbewertungen beim Online-Kauf – Bundeskartellamt zeigt Hintergründe und Lösungsansätze.](#)



- **Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)**

Die Bundesnetzagentur ist vorrangig für Regulierungs- und Wettbewerbsfragen in den Bereichen Elektrizität, Gas, Telekommunikation, Post und Eisenbahn zuständig. Im Strom- und Gasbereich veröffentlicht die BNetzA Sicherheitsvorgaben für alle Netzbetreiber sowie Betreiber von Energieanlagen, die gemäß BSI-KritisV als kritische Infrastrukturen bestimmt wurden. Die Erstellung der Vorgaben erfolgt gemäß §11 Abs.1a und 1b EnWG. Ferner überprüft die BNetzA die Einhaltung der Vorgaben.

Die BNetzA gehört als selbstständige Bundesoberbehörde zum Geschäftsbereich des BMWK. Dem BMDV kommt die Fachaufsicht über einige Aufgabenbereiche der BNetzA zu. Die Erstellung der Vorgaben gemäß §11 Abs.1a und 1b EnWG erfolgt im Benehmen mit dem BSI. Der BSIKT kann u.a. gegenüber der BNetzA beratend tätig werden. Die ITU führt die BNetzA und das BMWK als beteiligte mitgliedstaatliche Einrichtungen von deutscher Seite auf¹⁷⁷.



- **Initiative IT-Sicherheit in der Wirtschaft**

Die Initiative IT-Sicherheit in der Wirtschaft ist eine Initiative des Bundesministeriums für Wirtschaft und Klimaschutz für kleine und mittlere Unternehmen, welche eine Vielzahl von Aktivitäten bündelt, um deren IT-Sicherheitsniveau zu erhöhen. Die Initiative wird durch einen Steuerungskreis bei der Umsetzung ihrer Projekte beraten.

Mitglieder des Steuerungskreises sind unter anderem Vertreter:innen des BMWK, des BSI und dem DsiN. Letzterer wurde im Rahmen der Initiative ins Leben gerufen¹⁷⁸.



- **Transferstelle IT-Sicherheit im Mittelstand (TISiM)**

Die Transferstelle wurde im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie (BMWK) eingerichtet. Die Transferstelle soll kleinen und mittelständischen Unternehmen und dem Handwerk bei Fragen der IT-Sicherheit mit Informationsangeboten, Handlungsanleitungen, konkreten Maßnahmen, Handlungsempfehlungen und Best Practices als Anlaufstelle dienen und dadurch die Umsetzungsbereitschaft von IT-Sicherheitsmaßnahmen erhöhen. Dafür stehen Expert:innen aus Wirtschaft, Wissenschaft und Verwaltung bereit. Die Transferstelle wird

¹⁷⁷ [Bundesnetzagentur, Aufgaben und Struktur.](#)

[Bundesnetzagentur, IT-Sicherheit im Energiesektor.](#)

¹⁷⁸ [Bundesministerium für Wirtschaft und Energie, Erste Berufsschulen in Niedersachsen setzen auf Bottom-Up für mehr IT-Sicherheit im Mittelstand.](#)

[Bundesministerium für Wirtschaft und Energie, Steuerkreis.](#)



mit rund 5 Millionen Euro im Jahr bezuschusst. Perspektivisch soll die Transferstelle Cybersicherheit, gefördert durch das Bundesministerium für Wirtschaft und Klimaschutz, auf der TISiM aufbauen und damit in den Mittelpunkt der Initiative IT-Sicherheit in der Wirtschaft rücken.

Die TISiM ist im DsiN-Forum in Berlin angesiedelt. Geführt wird das Konsortium der TISiM durch DsiN. Die Transferstelle tauscht sich mit seinen Projektträgern zudem im Rahmen der ACS aus¹⁷⁹.



Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)

Das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung ist für die Entwicklungszusammenarbeit der Bundesregierung verantwortlich. Dabei entwickelt das BMZ auch gesicherte IT-Lösungen für Partnerländer.

Das BMZ ist im NCSR, dem IT-Rat sowie dem Verwaltungsrat des ITZBund vertreten. Es ist der wichtigste Auftraggeber der GIZ und neben dem BMF einer der beiden Gesellschafter. Es ist im Kuratorium der BAKS vertreten und gehört zu den Drittmittelgebern der SWP. Der deutsche Beitrag an das UNDP stammt aus dem Haushalt des BMZ¹⁸⁰.



Bundesverband der Verbraucherzentralen und Verbraucherverbände (vzbv)

Der gemeinnützige Verbraucherzentrale Bundesverband e.V. (vzbv) stellt eine Dachorganisation der 16 Verbraucherzentralen und 25 zugehörigen Mitgliedsverbände in Deutschland dar, deren Arbeit er koordiniert. Er vertritt zudem die Interessen der Verbraucher:innen beispielsweise gegenüber Politik und Wirtschaft. Eine weitere Aufgabe des vzbv ist die Erfassung aktueller Marktentwicklungen für Verbraucher:innen. Der vzbv beschäftigt sich u.a. mit digitaler Kommunikation und Diensten, so beispielsweise mit dem Schutz der Privatsphäre im digitalen Raum, Netzneutralität und dem Urheberrecht. Im Bereich der IT-Sicherheit fordert es u.a. eine gesetzliche Verpflichtung für „security by design“ sowie „security by default“ und nimmt Stellung zu geplanten thematischen Gesetzgebungsvorhaben auf nationaler als auch europäischer Ebene.

¹⁷⁹ [Bundesministerium für Wirtschaft und Energie, Altmaier: „Wir stärken die Kompetenzen des Mittelstands im Bereich IT-Sicherheit“.](#)

[Bundesanzeiger \(Bekanntmachung BAnz AT 23.09.2022 B1\), Förderbekanntmachung.](#)

[Bundesministerium für Wirtschaft und Energie, Neue Transferstelle IT-Sicherheit bündelt Hilfestellungen bundesweit.](#)

[Deutschland sicher im Netz, Transferstelle.](#)

¹⁸⁰ [Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Digitalisierung in der Entwicklungszusammenarbeit.](#)

[Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?.](#)



Seine Kernarbeit wird zu einem Anteil von 97 Prozent durch das **BMJ** finanziert. Der vzbv und das **BSI** haben eine Grundsatzvereinbarung über ihre Zusammenarbeit geschlossen¹⁸¹.



Cyber Security Cluster Bonn e.V.

Der Cyber Security Cluster Bonn e. V. ist ein Zusammenschluss von verschiedenen Institutionen, die im Kontext der Cybersicherheit aktiv sind. Der geographische Schwerpunkt des Clusters liegt in der Bonner Region, unter anderem durch das ansässige BSI und dem KdoCIR. Ziel des Vereins ist es, die thematische und geographische Nähe zu nutzen, um die Zusammenarbeit zu intensivieren, Fachkräfte anzuziehen und auch gemeinsam an konkreten Projekten im Bereich der Cybersicherheit zu arbeiten. Neben staatlichen Stellen sind auch Akteure aus Privatsektor und Wissenschaft als Mitglieder im Cluster beteiligt. Darüber hinaus hat das Cluster einen Weisenrat für Cybersicherheit – besetzt mit Vertreter:innen wissenschaftlicher Institutionen – berufen, welcher einen „weiteren Beitrag zur Immunisierung der Gesellschaft gegen Cyber-Attacken“ leisten soll.

Vertreter:innen des **BSI** und des **KdoCIR** der Bw, sowie der:die **BfDI** und das **IM NRW** sind Mitglieder im Beirat des Cyber Security Clusters Bonn e. V. Der Verein ist Multiplikator der **ACS**. Darüber hinaus das Cluster Partner des nordrhein-westfälischen **Kompetenzzentrums für Cybersicherheit in der Wirtschaft**¹⁸².



Deutsche Bundesbank (D BBk)

Die Deutsche Bundesbank ist die Zentralbank Deutschlands, die u.a. in den Bereichen der Geldpolitik, zur Stabilitätssicherung des Finanz- und Währungssystems sowie der Bankenaufsicht tätig ist. Die Bundesbank übernimmt auch Funktionen zur Stärkung der Widerstandsfähigkeit von wichtigen Finanzmarktinfrastrukturen und relevanten weiteren Akteuren gegenüber Bedrohungen aus dem Cyberraum. Zu diesem Zweck hat die Bundesbank u.a. das europäische „Rahmenwerk für bedrohungsgeleitete ethische Penetrationstests“ (TIBER-EU) auf deutscher Ebene

181 [Bundesministerium für Justiz und Verbraucherschutz, Verbraucherzentralen. Bundesamt für Sicherheit in der Informationstechnik, BSI und Verbraucherzentrale stärken digitalen Verbraucherschutz.](#)

[Verbraucherzentrale Bundesverband, Häufige Fragen \(FAQ\). \(Webseite entfernt\)](#)

[Verbraucherzentrale Bundesverband, IT-Sicherheit.](#)

[Verbraucherzentrale Bundesverband, IT-Sicherheit für vernetzte Geräte und digitale Dienste. Vorschläge des Verbraucherzentrale Bundesverbandes zur Konsultation zu einem europäischen Gesetz über Cyberresilienz.](#)

[Verbraucherzentrale Bundesverband, IT-Sicherheit im Verbraucheralltag stärken. Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme \(Zweites IT-Sicherheitsgesetz – IT-SiG 2.0\) in der Fassung vom 16. Dezember 2020.](#)

[Verbraucherzentrale Bundesverband, Über Uns.](#)

182 [Bundesamt für Sicherheit in der Informationstechnik, Liste von Multiplikatoren der Allianz für Cyber-Sicherheit.](#)

[Cyber Security Cluster Bonn, Über uns.](#)

[Cyber Security Cluster Bonn, Wechsel im Beirat des Vereins.](#)

[Cyber Security Cluster Bonn, Weisenrat für Cyber-Sicherheit.](#)

Emailaustausch mit Vertreter:innen des Cyber Security Cluster Bonn e.V. im November 2019.



implementiert (TIBER-DE). Hierfür wurde bei der D BBk ein nationales Kompetenzzentrum (TIBER Cyber Team, TCT) im Bereich Zahlungsverkehr und Abwicklungssysteme des Bundes angesiedelt, welches Unternehmen bei der für sie freiwilligen Durchführung eines TIBER-DE-Tests unterstützt.

Die D BBk wird durch die **EZB** beaufsichtigt, der:die Präsident:in der D BBk ist Mitglied des EZB-Rates. Die Etablierung von TIBER-DE geht auf einen gemeinsamen Beschluss mit dem **BMF** zurück. Der Umsetzungsrahmen von TIBER-DE wurde mit Beteiligung der **BaFin** und des **BSI** erarbeitet. Die D BBk nimmt an Treffen des **ECRB** teil¹⁸³.



Deutsche Akkreditierungsstelle (DAkKS)

Der DAkKS obliegt als nationale Akkreditierungsstelle Deutschlands die „Akkreditierung von Konformitätsbewertungsstellen (Laboratorien, Inspektions- und Zertifizierungsstellen)“. Insbesondere im Rahmen des Sektorkomitees Informationstechnik/Informationssicherheit (SK IT-IS) und seiner Unterausschüsse werden auch Akkreditierungsverfahren im Bereich der Cyber- und IT-Sicherheit vorgenommen.

Gesellschafter der DAkKS sind die Bundesrepublik Deutschland (vertreten durch das **BMWK**) sowie die Länder **Bayern**, **Hamburg** und **Nordrhein-Westfalen**. Die Aufsicht in Cybersicherheitsfragen über die DAkKS obliegt dem **BMI**. Im Aufsichtsrat der DAkKS sind neben Mitgliedern aus der Wirtschaft und Repräsentant:innen der Länder auch Vertreter:innen des **BMWK** und **BSI** vertreten. Im Rahmen einer Verwaltungsvereinbarung haben die DAkKS und das **BSI** zudem eine verstärkte Zusammenarbeit vereinbart, unter anderem mit einem Fokus auf Akkreditierungsverfahren für Cybersicherheitsprüfungen. Die DAkKS ist Mitglied in der **EA**¹⁸⁴.



Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)

Die Deutsche Gesellschaft für Internationale Zusammenarbeit unterstützt die Bundesregierung bei der Realisierung ihrer Ziele zur internationalen Entwicklungszusammenarbeit. Sie unterstützt die Förderung von Informations- und Kommunikationstechnologien und plant in Zukunft auch Cybersicherheit als Element der traditionellen Entwicklungszusammenarbeit aufzunehmen.

¹⁸³ Aufgrund der gleichlautenden Abkürzung mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, wird die offizielle Abkürzung der Deutschen Bundesbank bei Verwendung im Rahmen dieser Publikation und Visualisierung leicht ergänzt um „D BBk“.

[Deutsche Bundesbank, Implementierung von TIBER-DE.](#)

[Deutsche Bundesbank, TIBER-DE macht das deutsche Finanzsystem sicherer.](#)

¹⁸⁴ Deutsche Akkreditierungsstelle, Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443. (Webseite entfernt)

[Deutsche Akkreditierungsstelle, Aufsichtsrat.](#)

[Deutsche Akkreditierungsstelle, Profil.](#)

[Deutsche Akkreditierungsstelle, Sektorkomitee Informationstechnik / Informationssicherheit \(SK IT-IS\).](#)

[Deutsche Akkreditierungsstelle, Welche Aufgabe hat die DAkKS?](#)

[Mastodon: @CIO_Bund@muenster.im \[@cio_bund\], Sichere #Digitalisierung geht mit vertrauenswürdigen Zertifizierungen und verlässlichen Prüfstellen Hand in Hand. Gut, dass @BSI_Bund und Deutsche Akkreditierungsstelle ...\[Tweet\].](#)



BMZ und BMF sind Gesellschafter der GIZ. Ein:e Vertreter:in der GIZ gehört der MAG des IGF an¹⁸⁵.



Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE)

Die DKE arbeitet als „Kompetenzzentrum für elektrotechnische Normung“ auch an der Vereinbarung von Normen im Bereich der Informationstechnik, um u.a. zur verbesserten Interoperabilität sowie der Standardisierung von Systemen und Netzwerken beizutragen. Im Hinblick auf Cyber- und Informationssicherheit sollen diese auch das generelle interne sowie externe Sicherheitsniveau erhöhen und dadurch Gefahrenpotenziale mindern. Die DKE war an der Erarbeitung eines *Cybersecurity Navigator* beteiligt, welcher in der Form einer Datenbank die Suche nach relevanten Rechtsvorschriften sowie entsprechenden Normen und Standards erleichtern soll.

Die DKE ist deutsches Mitglied der IEC, des CENELEC und des ETSI. Mit dem DIN besteht das DIN/DKE Gemeinschaftsgremium „Cybersecurity“. Der Cybersecurity Navigator wird u.a. durch das BMBF gefördert. Mit Entwicklungen innerhalb der DKE wird sich u.a. innerhalb des BSIKT befasst¹⁸⁶.



Deutsches Institut für Normung (DIN)

Als deutsche Normungsorganisation wurde beim DIN auch eine Koordinierungsstelle IT-Sicherheit (KITS) angesiedelt. Diese übernimmt u.a. Koordinierungs- und Beratungsaufgaben und veranstaltet eine jährliche Konferenz. Das DIN hat in der Vergangenheit auch Stellung zu europäischen Gesetzgebungsvorhaben bezogen und beispielsweise ein Statement zum EU Cybersecurity Act oder der NIS 2-Richtlinie veröffentlicht.

Das DIN ist deutsches Mitglied des CEN sowie der ISO. Das Sekretariat der CSCG ist beim DIN angesiedelt, welches zudem auch für Deutschland an der CSCG beteiligt ist. Das DIN stellt zusätzlich das Sekretariat des ISO/IEC JTC 1/SC 27. Mit der DKE besteht auf deutscher Ebene das DIN/DKE Gemeinschaftsgremium „Cybersecurity“. Mit Entwicklungen innerhalb der DKE wird sich u.a. innerhalb des DIN befasst. Es gehört zu den Netzwerkpartnern der DAB. Die KITS wird durch das BMWK gefördert¹⁸⁷.

¹⁸⁵ [Deutsche Gesellschaft für internationale Zusammenarbeit \(GIZ\) GmbH, Bundesregierung.](#)
[Deutsche Gesellschaft für internationale Zusammenarbeit \(GIZ\) GmbH, Startseite.](#)
Hintergrundgespräche, 2018.

¹⁸⁶ [Cybersecurity Navigator, Research.](#)

[Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Cybersecurity Navigator bietet Rechtsvorschriften und Standards für Kritische Infrastrukturen an.](#)

[Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Organisation.](#)

[Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Sichere und innovative Informationssysteme.](#)

[Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Über Uns.](#)

¹⁸⁷ [Deutsches Institut für Normung, Gesetze und Normen zur Cybersicherheit.](#)

[Deutsches Institut für Normung, Koordinierungsstelle IT-Sicherheit.](#)

[Deutsches Institut für Normung, Statement on the Proposal for Directive on measures for a high common level of cybersecurity across the Union, repealing Directive \(EU\) 2016/1148 \(NIS 2\).](#)



Deutschland sicher im Netz e.V. (DsiN)

Deutschland sicher im Netz e. V. soll dazu beitragen, die deutsche Bevölkerung und kleine und mittlere Betriebe über IT-Sicherheit aufzuklären. In Kooperation mit seinen Mitgliedern und Partnern betreibt DsiN verschiedene Initiativen und Projekte, um konkrete Hilfestellungen für IT-Sicherheit zu leisten. Jährlich veröffentlicht DsiN einen Sicherheitsindex, welcher die „digitale Sicherheitslage von deutschen Internetnutzer:innen“ als repräsentative Studie anhand von vier Sicherheitsfaktoren, Bedrohungslage (Sicherheitsvorfälle und Verunsicherungsgefühl) sowie Schutzniveau (Sicherheitswissen und Sicherheitsverhalten), untersucht. Bei DsiN ist u.a. auch das Projekt PolisiN (Politiker:innen sicher im Netz) angesiedelt, welches Vorträge und Workshops für Politiker:innen und Mitarbeiter:innen auf verschiedenen politischen Ebenen durchführt.

Das BMI, BMWK, BMJ, BSI, BKA, BfDI und CODE sind im Beirat des DsiN vertreten. Der/die Bundesinnenminister:in ist Schirmherr:in des DsiN. Gefördert wird DsiN durch das BMI und BMWK. DsiN kooperiert mit der Initiative IT-Sicherheit in der Wirtschaft. Weitere Kooperationen bestehen u.a. mit der ACS, dem BMDV, dem BMJ, dem BKA, dem BSI sowie dem StMD [BY]. Es führt das Konsortium der TISiM¹⁸⁸.



DIN/DKE Gemeinschaftsgremium „Cybersecurity“

Das Gemeinschaftsgremium Cybersecurity bündelt deutsche Aktivitäten im Bereich der Cybersicherheitsnormung und konsolidiert eine deutsche Position für Normungsvorhaben auf europäischer Ebene.

Das Gemeinschaftsgremium des DIN und der DKE koordiniert und steuert als „nationales Spiegelgremium“ beispielsweise die deutsche Beteiligung im CEN/CE-NELEC JTC 13 sowie dem TC Cyber des ETSI¹⁸⁹.



Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän.“

Im Juni 2021 hat die Bundesregierung ein bis 2026 ausgelegtes Forschungsrahmenprogramm zur IT-Sicherheit beschlossen, welches mit insgesamt 350 Millionen Euro unterstützt wird. Es löst das von 2015–2020 bestehende Programm zur IT-Sicherheitsforschung der Bundesregierung „Selbstbestimmt und sicher in der digitalen Welt 2015–2020“ ab und fasst ressortübergreifende Maßnahmen und Aktivitäten in diesem Bereich zusammen. Mit dem Forschungsrahmenprogramm soll „technologische Souveränität auf dem Gebiet der IT-Sicherheitsforschung weiter aus[ge]bau[t] und [...] de[r] Rahmen für die künftige Forschungsförderung für eine sichere digitale Welt“ gesetzt werden. Hierzu wurden sieben strategische Ziele definiert: (1) Daten und Know-how, (2) Digitaler Wandel, (3) Demokratie und Gesellschaft, (4) Privatheit und Datenschutz, (5) Innovation und Transfer, (6) Führende Köpfe und (7) Deutsch-

¹⁸⁸ [Deutschland sicher im Netz, DsiN Sicherheitsindex 2022.](#)
[Deutschland sicher im Netz, Politiker:innen sicher im Netz \(PolisiN\).](#)
[Deutschland sicher im Netz, Presse.](#)
[Deutschland sicher im Netz, Über Uns.](#)

¹⁸⁹ [Deutsches Institut für Normung, Cybersecurity: DIN und DKE gründen Gemeinschaftsgremium.](#)



land und Europa. In seiner Umsetzung soll das Forschungsrahmenprogramm wissenschaftliche Kompetenzen und Exzellenz unterstützen, Innovationsökosysteme und Transfer fortentwickeln, Akteure zusammenbringen, gesellschaftlichen Dialog ermöglichen sowie die Forschung europäisch und international ausrichten.

Das Forschungsrahmenprogramm wurde von **BMBF** eingebracht und wird durch dieses begleitet¹⁹⁰.



Föderale IT-Kooperation (FITKO)

Die FITKO (Föderale IT-Kooperation) wurde als Koordinierungs- und Vernetzungsstelle für Digitalisierungsvorhaben der öffentlichen Verwaltung in Deutschland etabliert. Sie soll Kompetenzen und Ressourcen bündeln, um in Abstimmung mit dem IT-Planungsrat und in Zusammenarbeit mit anderen Akteuren die Digitalisierung der öffentlichen Verwaltung praktisch voranzutreiben – beispielsweise durch die Förderung der Zusammenarbeit aller föderalen Ebenen und die Entwicklung neuer Umsetzungsstrategien. Zu den Aufgaben der FITKO gehören darüber hinaus u.a. die strategische und organisatorische Unterstützung des IT-Planungsrates und seiner Gremien, die Steuerung seiner Projekte und Produkte sowie deren operative Umsetzung und die Bewirtschaftung des gemeinsamen Digitalisierungsbudgets von Bund und Ländern. Die FITKO wurde von dem IT-Planungsrat zudem mit der Erarbeitung und Weiterentwicklung der föderalen IT-Architektur beauftragt, um beispielsweise die Verbreitung von gemeinsamen Standards zu erhöhen.

Die FITKO ist eine eigenständige Anstalt des öffentlichen Rechts in Trägerschaft aller Länder (**BW, BY, BE, BB, HB, HH, HE, MV, NI, NW, RP, SL, SN, ST, SH, TH**) und des Bundes. Sie ist der operative Unterbau des **IT-PLR**. Unter Vorsitz der FITKO wurde ein **Kommunalgremium** eingerichtet. Die FITKO ist Mitglied der AG InfoSic des IT-PLR¹⁹¹.



gematik

Die gematik GmbH ist ein Kompetenzzentrum und Dienstleistungsunternehmen für das deutsche Gesundheitswesen. Für dessen sichere Vernetzung und Digitalisierung stellt die gematik die Telematikinfrastuktur bereit, die den Datenaustausch von Akteuren und Institutionen des Gesundheitssystems gewährleistet. Die gematik kümmert sich dabei insbesondere um die Spezifikation und Zulassung von Diensten und Komponenten der Telematikinfrastuktur sowie die

¹⁹⁰ [Bundesministerium für Bildung und Forschung, Digital.Sicher.Souverän.Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit.](#)

[Bundesministerium für Bildung und Forschung, Digital, sicher und souverän in die Zukunft.](#)

[Bundesministerium für Bildung und Forschung, Karliczek: Mit exzellenter IT-Sicherheitsforschung legen wir den Grundstein für eine sichere digitale Welt. Bundesregierung startet 350-Millionen-Rahmenprogramm zur IT-Sicherheitsforschung.](#)

¹⁹¹ [Lina Rusch, Digitaler Staat: Agenturen in den Startlöchern.](#)

[IT-Planungsrat, FITKO. \(Webseite entfernt\)](#)

[Matthias Punz, Rechtlicher Rahmen für FITKO-Start steht.](#)



Betriebskoordination. Neben der Telematikinfrastruktur ist die gematik auch für die elektronische Gesundheitskarte zuständig, die in Deutschland als ausschließlicher Versicherungsnachweis dient. Die gematik betreibt ein eigenes CERT (gematik CERT).

*Die gematik wird von verschiedenen Gesellschaftern getragen, so hält das **BMG** beispielsweise 51 Prozent der Gesellschafteranteile. Im Beirat sitzen unter anderem jeweils ein:e Vertreter:in der:s **BfDI**, des **BSI** und des **BMWK**. Das CERT der gematik ist bei **TI** als teilnehmendes Team gelistet¹⁹².*



German Competence Centre against Cyber Crime (G4C)

Das German Competence Centre against Cyber Crime (G4C) ist ein Verein, der unterschiedliche Akteure in einer strategischen Allianz gegen Cyberkriminalität zusammenbringt. Durch einen täglichen Informationsaustausch zwischen den behördlichen Kooperationspartnern und den Mitgliedern, können diese geeignete präventive Schutzmaßnahmen entwickeln.

*Das G4C kooperiert mit dem **BKA** und dem **BSI**¹⁹³.*



Innenministerkonferenz (IMK)

Die Innenministerkonferenz ermöglicht eine regelmäßige länderübergreifende Zusammenarbeit zwischen den Innenministern:innen und -senatoren:innen der Länder. Die Innenministerkonferenz hat zwei Gremien etabliert, die sogenannte „Länderoffene Arbeitsgruppe Cybersicherheit“ (LOAG Cybersicherheit, LAG Cybersicherheit) und die für die Polizei etablierte KomSi (AG Kommunikationssicherheit im AK II, UA luK). Diese Arbeitsgruppen sind für die Verwaltung von Handlungsfeldern im Bereich des Katastrophenschutzes oder der Cyberkriminalität zuständig.

*Durch die Teilnahme des:der Bundesinnenministers:in ist die IMK mit dem **BMI** verbunden. Von Länderseite nehmen u.a. die Minister:innen des **IM BW**, des **StMI [BY]**, des **MIK [BB]**, des **MIBD MV**, des **MI [NI]** oder des **IM NRW** sowie der:die Senatorin der **SenInnDS [BE]** teil. Regelmäßig erhält die IMK Berichte des **NCSR**. Der:die **CISO [SN]** ist an einer Länderarbeitsgruppe der IMK vertreten¹⁹⁴.*

¹⁹² [Bundesministerium für Gesundheit, E-Health-Gesetz.](#)

[Gematik, Datensicherheit.](#)

[Gematik, Die elektronische Gesundheitskarte. \(Webseite entfernt\)](#)

[Gematik, Telematikinfrastruktur.](#)

[Gematik, Themen. \(Webseite entfernt\)](#)

[Gematik, Über uns.](#)

¹⁹³ [German Competence Centre against Cyber Crime e. V. \(G4C\), Über uns.](#)

¹⁹⁴ [Bundesrat, Innenministerkonferenz.](#)

[CISO der niedersächsischen Landesverwaltung, Cybersicherheit in der Landesverwaltung. \(Webseite entfernt\)](#)

[Secupedia, Nationales Cyber-Abwehrzentrum.](#)

[Emailaustausch mit Vertreter:innen des BSI im Februar 2020.](#)

[Innenministerkonferenz, 213. Sitzung der Innenministerkonferenz.](#)



IT-Planungsrat (IT-PLR)

Der IT-Planungsrat wurde als politisches Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung der öffentlichen Verwaltung in Deutschland geschaffen. Seine Beschlüsse stellen für Bund und Länder eine verbindliche Grundlage für die gemeinsamen föderalen Digitalisierungsaktivitäten dar. Der IT-Planungsrat legt übergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards fest, steuert ihm zugewiesene E-Government-Projekte und koordiniert das Verbindungsnetz zwischen den IT-Netzen von Bund und Ländern. Im Vorsitz wechseln sich Bund und Länder (in alphabetischer Reihenfolge) jährlich ab. Zu den Gremien des IT-Planungsrats gehört die Arbeitsgruppe Informationssicherheit (AG InfoSic). Diese Arbeitsgruppe ist dafür zuständig, die Umsetzung der Leitlinien für Informationssicherheit in der öffentlichen Verwaltung zu überwachen und die Ziele sowie Strategien zur Informationssicherheit weiterzuentwickeln.

Dem:der CIO der Bundesregierung (BMI) obliegt der Vorsitz des IT-PLR. Der:die BfDI, Vertreter:innen der kommunalen Spitzenverbände sowie der:die Präsident:in der FITKO und ein:e Landedatenschutzbeauftragte:r sind beratende Mitglieder. Von Länderseite sind der:die CIO [BW], CIO [BY], CIO [BE], CIO [HB], CIO [HE], CIO [MV], CIO [NI], CIO [NW], CIO [RP], CIO [SL], CIO [SN], CIO [ST] und CIO [TH] Mitglied. Brandenburg ist durch ein:e Staatssekretär:in des MIK, Hamburg durch den:die Chef:in der SK [HH] und Schleswig-Holstein durch ein:e Staatssekretär:in des MELUND SH vertreten. Weitere Personen, unter anderem jeweilige Ansprechpartner der Fachministerkonferenzen, können ebenfalls hinzugerufen werden, wenn die Entscheidungen des Rates ihr Fachgebiet tangieren. Das BSI ist beratendes Mitglied in der AG InfoSic. Dem IT-Planungsrat untersteht die FITKO. Das Kommunalgremium ist ein Gremium des IT-Planungsrat zum Informationsaustausch mit den Kommunen. Der:die Chef:in des BKAm und die Chef:innen der Staats- und Senatskanzleien nehmen jedes Jahr den Tätigkeitsbericht des IT-Planungsrates zur Kenntnis und informieren sich über die Weiterentwicklung der Nationalen E-Government-Strategie¹⁹⁵.



IT Security made in Germany (ITSMIG)

Das Vertrauenszeichen „IT Security made in Germany“ wurde gemeinsam durch das Bundesministerium des Innern, für Bau und Heimat, das Bundesministerium für Wirtschaft und Energie sowie Vertreter:innen der deutschen IT-Sicherheitswirtschaft ins Leben gerufen und wird in Form der TeleTrusT-Arbeitsgruppe „ITSMIG“ fortgeführt. Ziel ist es, die gemeinsame Außendarstellung der organisierten deutschen IT-Sicherheitswirtschaft zu koordinieren und die Zusammenarbeit zu verbessern.

¹⁹⁵ [IT-Planungsrat, Aufgaben des IT-Planungsrats.](#)

[IT-Planungsrat, Besprechung des Chefs des Bundeskanzleramtes mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder. \(Webseite entfernt\)](#)

[IT-Planungsrat, IT-Planungsrat.](#)

[IT-Planungsrat, Umsetzung Leitlinie InfoSic. \(Webseite entfernt\)](#)

[IT-Planungsrat, Zusammensetzung des IT-Planungsrates.](#)



Bei der Etablierung von ITSMIG haben das **BMI** und das **BMWK** unterstützt. Beide Ministerien sind im Beirat der Arbeitsgruppe vertreten¹⁹⁶.



Kompetenz- und Forschungszentren für IT-Sicherheitsforschung (CISPA, ATHENE, KASTEL)

Die drei Kompetenz- und Forschungszentren für IT-Sicherheit in Saarbrücken (CISPA), Darmstadt (ATHENE) und Karlsruhe (KASTEL) sind Bestandteil der Digitalen Agenda des Bundesministeriums für Bildung und Forschung. Mit der Gründung der drei Forschungszentren hat die Bundesregierung die Forschung und Entwicklung im Bereich Cybersicherheit und Schutz der Privatsphäre ausgeweitet.

Die drei Kompetenz- und Forschungszentren für IT-Sicherheit werden durch das **BMBF** gefördert¹⁹⁷.



Nationaler CERT-Verbund

Der CERT-Verbund ist ein Zusammenschluss deutscher Sicherheits- und Computer-Notfallteams, innerhalb von Unternehmen, Universitäten und Verwaltungen, die sich auf Bund- und Länderebene zusammengeschlossen haben. Durch gegenseitigen Informationsaustausch und Kooperation soll eine schnelle gemeinsame Reaktion auf Cybervorfälle ermöglicht werden.

Im CERT-Verbund sind unter anderem das **CERTBw**, das **BSI** mit dem **CERT-Bund** sowie das CERT der **BWI** vertreten. Von Länderseite sind unter anderem das **Bayern-CERT**, **CERT BWL**, **CERT-NRW** und **CERT-rlp** beteiligt¹⁹⁸.



Nationaler Cyber-Sicherheitsrat (NCSR)

Der Nationale Cyber-Sicherheitsrat soll als strategischer Ratgeber der Bundesregierung langfristige Handlungsnotwendigkeiten und Trends der Cybersicherheit identifizieren und entsprechende Impulse anregen. Konkret sollen durch den NCSR unter anderem „Vorschläge zur Weiterentwicklung der nationalen Regelungen für mehr Cybersicherheit“ gemacht und Räume für öffentlich-private Kooperationen identifiziert werden. Der NCSR wird durch eine ständige wissenschaftliche Arbeitsgruppe unterstützt, der die Beratung in strategischen Fragen sowie die Erarbeitung von Handlungsempfehlungen zukommt. Zudem veröffentlicht die wissenschaftliche Arbeitsgruppe regelmäßig Impulspapiere.

Im NCSR sind **BMI**, **BKAmt**, **AA**, **BMVg**, **BMWK**, **BMJ**, **BMF**, **BMUV**, **BMDV**, **BMG**, **BMZ** und **BMBF** sowie das **BSI** als auch Repräsentant:innen der Länder **Niedersachsen** und

¹⁹⁶ [TeleTrust, IT Security made in Germany.](#)

¹⁹⁷ [Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.](#)

¹⁹⁸ [Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: CERT-Verbund. Deutscher CERT-Verbund, Überblick.](#)



Hessen vertreten. Darüber hinaus sind im NCSR u.a. auch **UP KRITIS** sowie Kommunen (derzeit durch den Deutschen Städtetag, **KSV**) repräsentiert. In Sondersitzungen wurden darüber hinaus in der Vergangenheit auch bereits Vertreter:innen der **ENISA**, des **BfV** und der **SWP** eingeladen. Den Vorsitz des NCSR hat der:die CIO Bund inne. Der wissenschaftlichen Arbeitsgruppe gehört neben wissenschaftlichen Vertreter:innen auch ein:e Repräsentant:in des **BSI** an. Das **Cyber-AZ** sendet seinen Jahresbericht an den NCSR Neben der Bundesregierung soll der NCSR auch Impulse für die **IMK** liefern¹⁹⁹.



Nationales Cyber-Abwehrzentrum (Cyber-AZ)

Das Nationale Cyber-Abwehrzentrum hat die Aufgabe, die operative Zusammenarbeit hinsichtlich verschiedener Gefährdungen im Cyberraum zwischen staatlichen Stellen zu optimieren und entsprechende Schutz- und Abwehrmaßnahmen zu koordinieren. Dafür werden im Cyber-AZ, welches im Bundesamt für Sicherheit in der Informationstechnik angesiedelt ist, alle Informationen zu Cyberoperationen auf IT-Infrastruktur gebündelt. Es finden tägliche Lagebesprechungen und eine wöchentliche „Koordinierte Fallbearbeitung“ statt. Die Arbeitskreise Operativer Informationsaustausch sowie Nachrichtendienstliche Belange des Cyber-AZ kommen monatlich und ein Arbeitskreis Kritische Infrastrukturen alle drei Monate zusammen. Anlassbezogen erstellt das Cyber-AZ eine „Cyber-Lage“.

*Das Cyber-AZ ist eine Kooperationsplattform von **BSI**, **BPol**, **BKA**, **BfV**, **BBK**, **BND**, **KdoCIR** und **BAMAD**. Die **BaFin** ist als Partner beteiligt. Partner des Cyber-AZ auf Länderebene sind die **Cyberabwehr Bayern**, **Hessen3C**, die **Zentralstelle Cybercrime Bayern** und die **Zentral- und Ansprechstelle Cybercrime NRW**. Es schickt seinen Jahresbericht an den **NCSR**. Neben den o.g. Behörden werden die Cyber-Lagen darüber hinaus unter anderem an die **LfV** sowie Mitglieder des **VCV** gesendet. Das **BKA** stellt den:die Koordinator:in des Cyber-AZ, stellvertretend übernehmen diese Funktion das **BfV** und das **KdoCIR** der **Bw**. Alle beteiligten Behörden entsenden Verbindungsbeamte:innen in das Cyber-AZ. Es erhält Situationsanalysen des **KdoCIR** und arbeitet mit dem **LZ** zusammen²⁰⁰.*

199 [Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.](#)

[Bundesministerium des Innern, für Bau und Heimat, Sondersitzung des Nationalen Cyber-Sicherheitsrates.](#)

[Bundesministerium der Verteidigung, Cyber-Sicherheitsrat.](#)

[Der Beauftragte der Bundesregierung für Informationstechnik, Der Nationale Cyber-Sicherheitsrat \(NCSR\).](#)

[Fraunhofer-Institut für Sichere Informationstechnologie, Beratung aus der Forschung. Wissenschaftliche Arbeitsgemeinschaft Nationale Cyber-Sicherheit.](#)

200 Hintergrundgespräche, 2019.

[Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.](#)

[Bundesamt für Sicherheit in der Informationstechnik, BSI Magazin 2020/01: Mit Sicherheit.](#)

[Bundeskriminalamt, Das Nationale Cyber-Abwehrzentrum.](#)

[Deutscher Bundestag \(Drucksache 19/3356\), Antwort der Bundesregierung auf die Kleine Anfrage: Aufgaben und Ausstattung des Nationalen Cyber-Abwehrzentrums.](#)

[Deutscher Bundestag \(Drucksache 19/2645\), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.](#)



Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen (UP KRITIS)

UP KRITIS hat die Aufgabe, die Versorgung durch Kritische Infrastrukturen zu erhalten. Dafür dient UP KRITIS als öffentlich-private Kooperation zwischen staatlichen Stellen, Betreibern Kritischer Infrastrukturen und ihren Verbänden. In eingerichteten Branchen- sowie Themenarbeitskreisen werden Themen mit IT- und Cybersicherheitsbezug diskutiert, gemeinsame Positionen entwickelt sowie durch Vernetzung auch zum Informationsaustausch untereinander beigetragen.

*Im Rahmen des UP KRITIS kooperieren von staatlicher Seite **BMI**, **BSI** und **BBK**, die auch durch Vertreter:innen im Rat von UP KRITIS repräsentiert sind. UP KRITIS erhält den täglichen Lagebericht IT-Sicherheit des **LZ** und ist im **NCSR** vertreten²⁰¹.*



Stiftung Wissenschaft und Politik (SWP)

Die Stiftung Wissenschaft und Politik berät den Bundestag und die Bundesregierung, sowie internationale Organisationen zu außen- und sicherheitspolitischen Fragen und ist dabei politisch unabhängig. Ihre Forschung umfasst auch Digitalisierungs- und Cybersicherheitsthemen.

*Die SWP erhält ihre institutionelle Zuwendung vom **BKAmt**. Unter den Drittmittelgebern sind darüber hinaus das **AA**, **BMBF**, **BMZ** sowie die **EK**. Im Stiftungsrat der SWP sind als Mitglieder unter anderem Vertreter:innen aus **BKAmt**, **BMBF**, **BMZ**, **BMI**, **AA**, **BMF**, **BMWK** und **BMVg** vertreten. In der Vergangenheit wurde eine Vertreterin der SWP zu einer Sondersitzung des **NCSR** eingeladen²⁰².*



Verwaltungs-CERT-Verbund (VCV)

Der Verwaltungs-CERT-Verbund ist eine Plattform zum gegenseitigen Informationsaustausch zwischen dem Computer Emergency Response Team Bund und den Computer Emergency Response Teams der Bundesländer. So soll die IT-Krisenprävention und -reaktion gestärkt und die IT-Sicherheit in der öffentlichen Verwaltung verbessert werden. Alle teilnehmenden CERTs haben sich hierzu zu einem verbindlichen Meldeverfahren verpflichtet, welches einen unverzüglichen Meldeweg bei IT-Sicherheitsvorfällen vorsieht.

²⁰¹ [Bundesamt für Sicherheit in der Informationstechnik. Geschäftsstelle UP KRITIS, UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland.](#)

[Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, UP KRITIS. Organisation.](#)

[Internetplattform zum Schutz Kritischer Infrastrukturen, UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen.](#)

[Internetplattform zum Schutz Kritischer Infrastrukturen, Zusammenarbeit im Rahmen des UP KRITIS.](#)

²⁰² [Stiftung Wissenschaft und Politik, Cyber-Sicherheit.](#)

[Stiftung Wissenschaft und Politik, Cluster „Digitalisierung – Cyber – Internet“.](#)

[Stiftung Wissenschaft und Politik, Organe der Stiftung.](#)

[Stiftung Wissenschaft und Politik, Unterstützerinnen und Unterstützer.](#)

[Stiftung Wissenschaft und Politik, Über uns.](#)

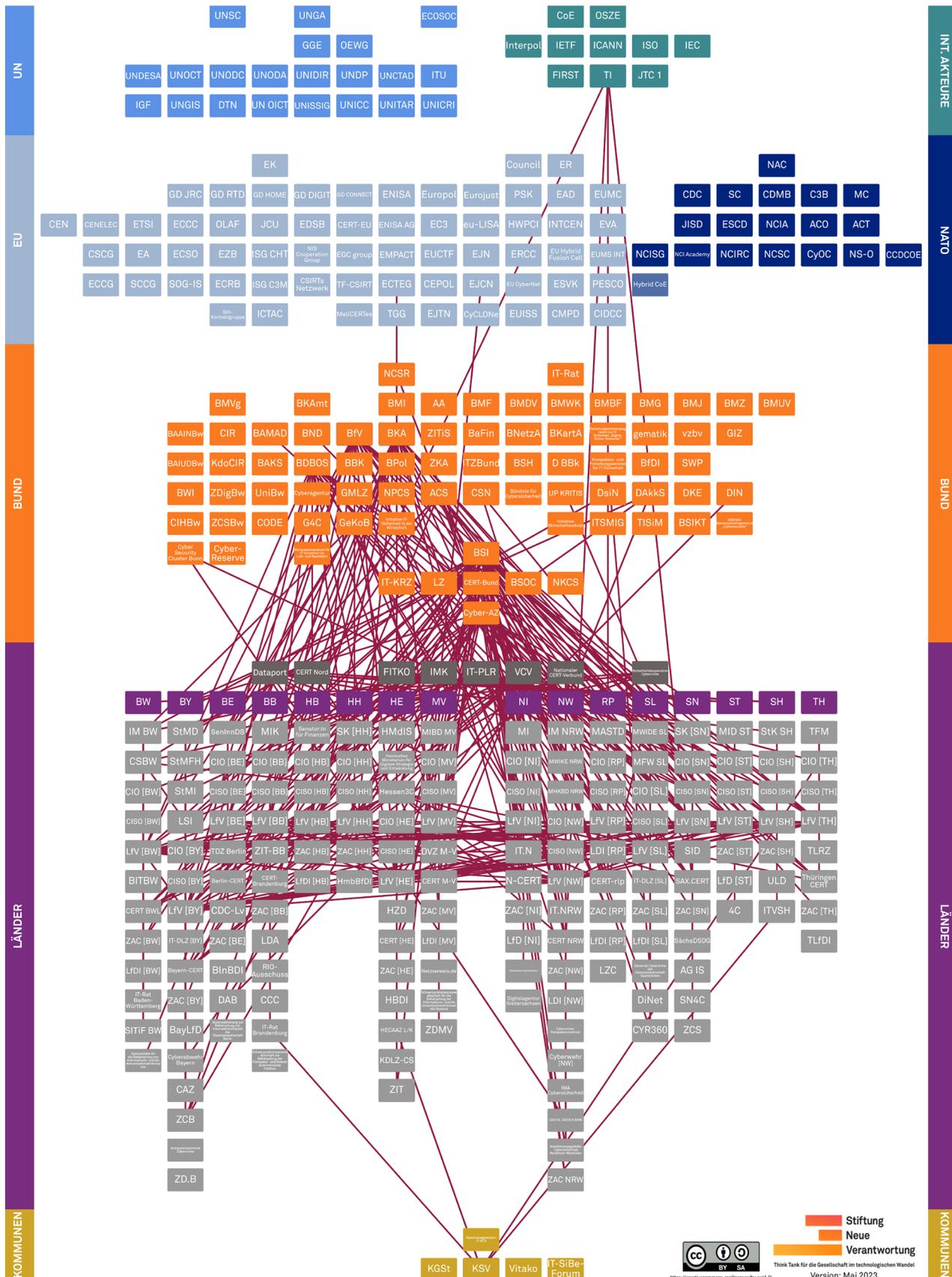


Am VCV beteiligt sind das *BSI* und das *CERT-Bund* sowie *Länder CERTs*, das *CERT Nord* und das *LSI*. Die Mitglieder des VCV erhalten den täglichen Lagebericht *IT-Sicherheit des LZ* sowie die *Cyber-Lagen des Cyber-AZ*. Arbeitsbeziehungen bestehen mit dem *Hessen3C*. Der:die *CISO [MV]* vertritt Mecklenburg-Vorpommern im VCV²⁰³.

203 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheit und IT-Krisenmanagement – Angriffe auf Kritische Infrastrukturen. (Webseite entfernt)
Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTs im Verwaltungs-CERT-Verbund (VCV). (Webseite entfernt)



9. Erläuterung – Akteure auf Landesebene





Policy-Überblick

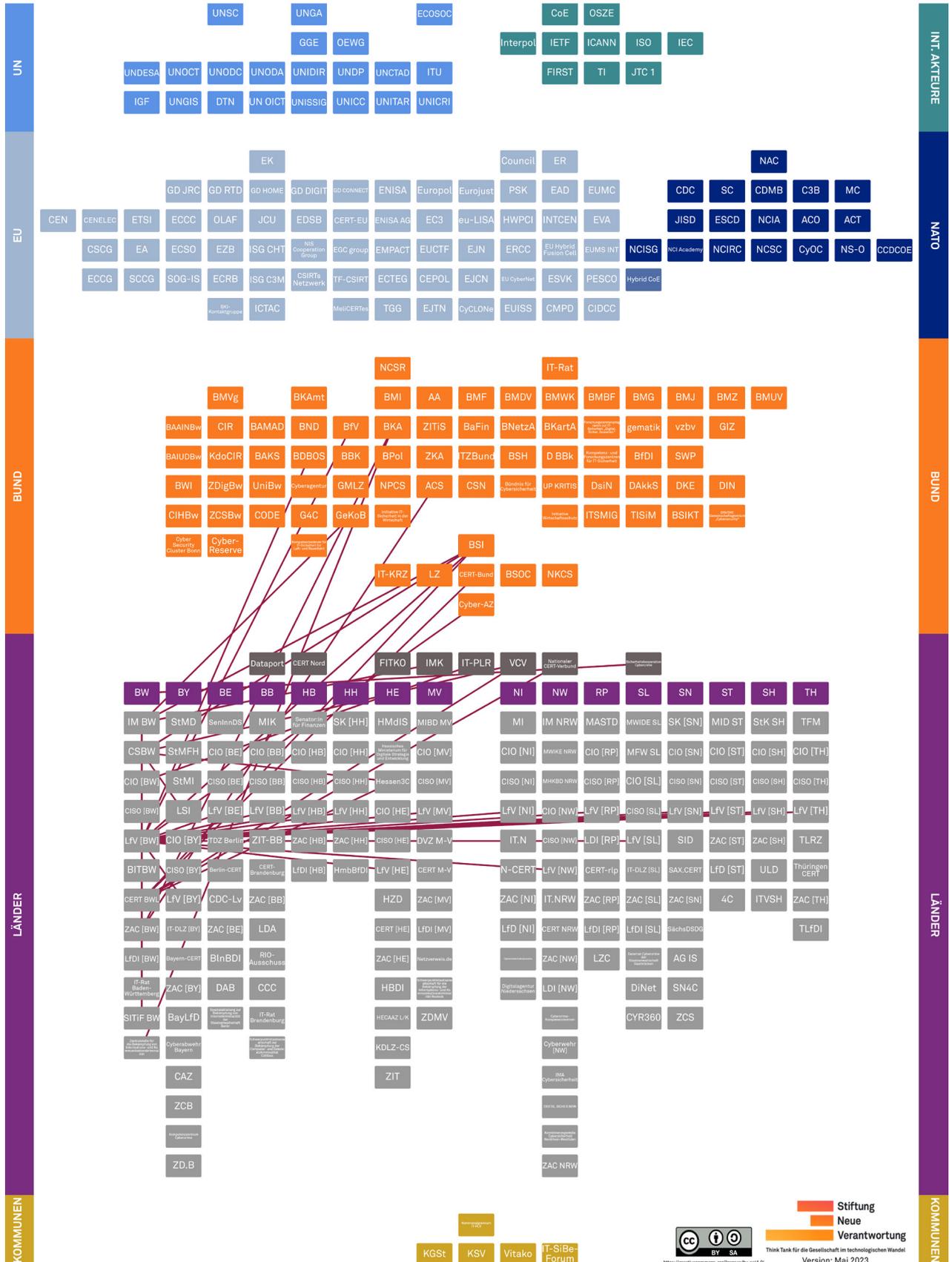
Jahr	Bundesland	Name
2023	HB	<u>Bremische Cybersicherheitsstrategie</u>
2022	BY	<u>Gesetz über die Digitalisierung im Freistaat Bayern</u> (Bayerisches Digitalgesetz – BayDiG)
2022	MV	<u>Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern</u> (Errichtungsgesetz ZDMV – ZDMVG)
2021	BW	Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026
2021	BW	<u>Gesetz für die Cybersicherheit in Baden-Württemberg</u> (Cybersicherheitsgesetz, CSG)
2021	HE	<u>Informationssicherheitsleitlinie für die hessische Landesverwaltung</u>
2021	NW	<u>Cybersicherheitsstrategie des Landes Nordrhein-Westfalen</u>
2020	BB	<u>Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg</u> (E-Government- und IT-Organisationsrichtlinie)
2020	HE	<u>Förderrichtlinie Cybersicherheitsforschung in Hessen</u>
2020	RP	<u>Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz</u> (E-Government-Gesetz Rheinland-Pfalz, EGovGRP)
2019	NI	<u>Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit</u> (NDIG)
2019	SL	<u>Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes</u> (Informationssicherheitsgesetz Saarland, IT-SiG SL)
2019	SN	<u>Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen</u> (Sächsisches Informationssicherheitsgesetz – SächsISiG)
2019	SN	<u>Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen</u> (Sächsisches E-Government-Gesetz, SächsEGovG)
2019	ST	<u>Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt</u> (E-Government-Gesetz Sachsen-Anhalt, EGovG LSA)
2018	Alle	<u>Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung</u>
2018	BB	<u>Gesetz über die elektronische Verwaltung im Land Brandenburg</u> (Brandenburgisches E-Government-Gesetz, BbgEGovG)



Jahr	Bundesland	Name
2018	HB	<u>Gesetz zur Förderung der elektronischen Verwaltung in Bremen</u>
2018	HE	<u>Hessisches Gesetz zur Förderung der elektronischen Verwaltung</u> (Hessisches E-Government-Gesetz, HEGovG)
2018	TH	<u>Thüringer Gesetz zur Förderung der elektronischen Verwaltung</u> (Thüringer E-Government-Gesetz, ThürEGovG)
2017	BW	<u>Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit</u> (VwV Informationssicherheit)
2017	HB	<u>Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL)</u>
2017	SL	<u>Gesetz zur Förderung der elektronischen Verwaltung im Saarland</u> (E-Government-Gesetz Saarland, E-GovG SL)
2016	BE	<u>Gesetz zur Förderung des E-Government (E-Government-Gesetz Berlin (EGovG Bln))</u>
2016	MV	<u>Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern</u> (E-Government-Gesetz Mecklenburg-Vorpommern, EGovG M-V)
2016	NW	<u>Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen</u> (E-Government-Gesetz Nordrhein-Westfalen, EGovG NRW)
2015	BW	<u>Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg</u> (E-Government-Gesetz Baden-Württemberg, EGovG BW)
2015	BY	<u>Gesetz über die elektronische Verwaltung in Bayern</u> (Bayerisches E-Government-Gesetz, BayEGovG)
2014	MV	<u>Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)</u>
2010	Alle	<u>Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag)</u>
2009	SH	<u>Gesetz zur elektronischen Verwaltung für Schleswig-Holstein</u> (E-Government-Gesetz, EGovG)



9.1 Baden-Württemberg (BW)





Das baden-württembergische Landeskriminalamt beteiligt sich an der *Sicherheitskooperation Cybercrime*.

Überblick

- **Relevante Policy-Dokumente**

- 2021: Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026
- 2021: Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz, CSG)
- 2017: Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit)
- 2015: Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (E-Government-Gesetz Baden-Württemberg, EGovG BW)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Ministerium des Inneren, für Digitalisierung und Kommunen (IM BW, Abteilung 7: Digitalisierung, Referat 74: Informations- und Cybersicherheit).

Das *BSI* und Baden-Württemberg haben eine vertiefte Zusammenarbeit vereinbart. Der:die baden-württembergische Innenminister:in nimmt an der *IMK* teil²⁰⁴.



- **Landes-Chief Information Officer (CIO [BW]):** In Baden-Württemberg ist der:die Landesbeauftragte:r für Informationssicherheit unter anderem für die IT-Strategie der Landesverwaltung sowie die E-Government-Strategie zuständig. Der:die CIO fungiert gleichzeitig auch als Chief Digital Officer (CDO) der Landesverwaltung.

Der:die CIO ist dem *IM BW* zugeordnet. Er:sie vertritt Baden-Württemberg im *IT-PLR*²⁰⁵.



- **Landes-Chief Information Security Officer (CISO [BW]):** In Baden-Württemberg wird der:die Informationssicherheitsbeauftragte:r durch das *IM BW* benannt. Ihm:ihr obliegt die Festlegung und Fortschreibung von Richtlinien im Bereich der Informationssicherheit für die Landesverwaltung, die *Beratung des:der Landes-CIO*, sowie die *Erarbeitung eines jährlichen Berichts zur Lage der Umsetzung und Wirksamkeit von vorgenommenen Maßnahmen im Bereich der IT-Sicherheit, welcher wiederum dem:der Landes-CIO vorgelegt wird*²⁰⁶.

204 [Ministerium des Inneren, für Digitalisierung und Kommunen, Organigramm.](#)

Wim Orth, BSI und BaWü kooperieren eng bei Cyber-Sicherheit. (Webseite entfernt)

205 [CIO Baden-Württemberg, Stefan Krebs.](#)

206 [Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit.](#)



- **Behördlicher IT-Dienstleister:** Landesoberbehörde IT Baden-Württemberg (BITBW), die in den Geschäftsbereich des **IM BW** fällt²⁰⁷.



- **Computer Emergency Response Team (CERT):** Das CERT BWL ist bei der **CSBW** angesiedelt. Es arbeitet mit der **ZAC [BW]** zusammen und ist im **CERT-Verbund** vertreten²⁰⁸.



- **Landesbehörde²⁰⁹ für Verfassungsschutz (LfV [BW]):** Innerhalb der Landesbehörde Verfassungsschutz Baden-Württemberg befasst sich vor allen Dingen die Abteilung 4 mit cybersicherheitsrelevanten Arbeitsfeldern. Dort sind unter anderem Zuständigkeiten für Spionage- und Cyberabwehr sowie Geheim- und Sabotageschutz angesiedelt. Zukünftig soll der Bereich der Cyberabwehr verstärkt werden.

*LfV und LKA arbeiten unter anderem im Rahmen der Gemeinsamen Informations- und Analysestelle LKA BW und LfV BW (GIAS) zusammen. Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das **BSI** unterstützt werden²¹⁰.*



- **Institutionelle Ansässigkeit der Zentralen Ansprechstelle Cybercrime für die Wirtschaft²¹¹ (ZAC [BW]):** Landeskriminalamt Baden-Württemberg (LKA BW). Die ZAC verfügt zudem bei Bedarf über eine interne Task Force „Digitale Spuren“, die sich aus Expert:innen aller Spezialisierungsbereiche zusammensetzt.

*Das LKA BW ist Multiplikator der **ACS**²¹².*



- **Landesdatenschutzbehörde:** Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI)²¹³

207 [Landesoberbehörde IT Baden-Württemberg, Über BITBW.](#)

208 [Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten. Natalie Zibolz, Baden-Württemberg bündelt Cybersicherheits-Angebote. Staatsministerium Baden-Württemberg, Systeme des Landesamtes für Geoinformation wieder in Betrieb.](#)

209 [Der Einheitlichkeit halber werden alle LfV als Landesbehörden bezeichnet. In BW, BY, HB, HH, HE und SN sind die LfV's als Landesamt organisiert.](#)

210 [Landesamt für Verfassungsschutz Baden-Württemberg, Aufbau und Organisation. Landesamt für Verfassungsschutz Baden-Württemberg, Cyberspionage.](#)

211 [Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten. Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Berichterstattung zur Cybersicherheitsagentur.](#)

212 [Landespolizeipräsidium Baden-Württemberg, Zentrale Ansprechstelle Cybercrime für Unternehmen und Behörden. Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten.](#)

213 [Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Aufgaben und Zuständigkeiten.](#)



Weitere Akteure in Baden-Württemberg:



Cybersicherheitsagentur Baden-Württemberg (CSBW)

Im Februar 2021 wurde mit dem Aufbau der Cybersicherheitsagentur Baden-Württemberg mit Sitz in Stuttgart begonnen. In ihre Aufgabenbeschreibung fallen unter anderem die Abwehr von Gefahren für die Cybersicherheit sowie der Schutz gesellschaftlicher Prozesse vor Operationen im Cyberraum. Weiterhin soll die CSBW Informationen bereitstellen, Beratung tätigen, vorhandene Akteure vernetzen sowie als Kompetenzzentrum, beispielsweise für Schulungen, zur Cybersicherheit fungieren. Zudem operiert die CSBW als zentrale Koordinierungs- und Meldestelle in Baden-Württemberg für die öffentliche Verwaltung in sämtlichen cybersicherheitsrelevanten Kontexten. Als diese hat sich die CSBW unter anderem der strukturierten Sammlung und Auswertung „alle[r] für die Abwehr von Gefahren für die Cybersicherheit erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Operationen auf die Cybersicherheit und der dabei beobachteten Vorgehensweise“ sowie der landesweiten Maßnahmenkoordination verschrieben. Diese Erkenntnisse sollen unter anderem in ein landesweites aktuelles Lagebild einfließen, welches mit anderen Behörden geteilt wird. Die CSBW kann zudem Warnungen, Hinweise und Empfehlungen aussprechen sowie bei Bedarf und mit Einvernehmen der jeweiligen Landesstelle die informationstechnische Sicherheit von deren Infrastruktur untersuchen. Darüber hinaus bietet die CSBW die Cyber-Ersthilfe BW an, eine telefonische Beratung für IT-Sicherheitsvorfälle.

Dem IM BW kommt die Dienst- und Fachaufsicht über die CSBW zu, dem sie nachgeordnet ist. Die Fachaufsicht über die CSBW hat das zuständige Fachreferat des IM BW – sie kommt derzeit der Person zu, die gleichzeitig auch als Landes-CISO [BW] agiert. Auf operativer Ebene arbeitet die CSBW mit der SITiF, der ZAC [BW], der BITBW und dem LfV [BW] zusammen. Sie berichtet an den Landes-CIO [BW] sowie einmal jährlich an den LfDI [BW]. Die CSBW hat das CERT BWL operativ übernommen und wird dann Mitglied des VCV. Sie arbeitet auch bisher schon mit dem VCV und dem BSI zusammen. Die CSBW berichtet an das IM BW sowie den IT-Rat Baden-Württemberg mindestens einmal jährlich in Form eines Berichtes. Sie kann – unter der Bedingung der Erforderlichkeit und auf explizites Ersuchen – unter anderem das LfV [BW] und Strafverfolgungsbehörden durch technische Expertise, bspw. im Kontext von Durchsuchungen, unterstützen. LKA und LfV [BW] waren an der Erarbeitung des Cybersicherheitsgesetzes, durch das die CSBW errichtet wurde, beteiligt. Die CSBW soll für Themen der Cybersicherheit als zentrale baden-württembergische Ansprechpartnerin für weitere Akteure auf Länder- (unter anderem Hessen 3C und LSI), Bundes-, EU- sowie internationaler Ebene dienen²¹⁴.

²¹⁴ Landesrecht BW Bürgerservice, Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG). [Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Cybersicherheitsagentur Baden-Württemberg.](#)



IT-Rat Baden-Württemberg

Als Gremium entscheidet der IT-Rat über die IT-Standards des Landes, bereitet sowohl die E-Government als auch IT-Strategie Baden-Württembergs vor und berät den Landes-CIO „bei der Abstimmung des ressortübergreifenden Einsatzes des E-Governments und der Informationstechnik“. Seine Beratungen werden durch einen Arbeitskreis Informationstechnik (AK-IT) vorbereitet, der auch die Umsetzung gefasster Beschlüsse beobachtet.

Der Vorsitz obliegt dem [Landes-CIO \[BW\]](#) und die Geschäftsführung des IT-Rates dem [IM BW](#). Der IT-Rat setzt sich aus den Amtschefs:innen der baden-württembergischen Ministerien zusammen. Beratende Mitglieder sind unter anderem die [BITBW](#), die [CSBW](#) sowie der:die [LfDI](#). Vertreter:innen der drei Akteure sind darüber hinaus auch als beratende Mitglieder im AK-IT repräsentiert²¹⁵.



Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg (SITiF BW)

Mit dem SITiF BW wurde die IT-Sicherheit verschiedener Stellen der baden-württembergischen Finanzverwaltung gebündelt. Das SITiF BW, welches seinen Sitz in Karlsruhe hat, betreibt zum Schutz der IT-Infrastruktur permanentes Monitoring sowie regelmäßige Penetrationstests und Audits. Hierdurch sollen Vorfallsszenarien und IT-sicherheitsrelevante Anomalien frühestmöglich identifiziert werden. Zudem sollen Mitarbeiter:innen unter anderem durch Schulungsangebote unterstützt werden. SITiF BW ist beim Landeszentrum für Datenverarbeitung (LZfD) bei der Oberfinanzdirektion (OFD) Karlsruhe angesiedelt²¹⁶.



Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität

Die Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität ist bei der Generalstaatsanwaltschaft Stuttgart angesiedelt. Ihre Aufgabe ist es, Entwicklungen im Bereich der Informations- und Kommunikationstechnologien zu verfolgen, auszuwerten und die Staatsanwaltschaft darüber zu informieren. Außerdem plant sie Fortbildungsveranstaltungen und führt diese durch. Die Zentralstelle prüft neue Instrumente zur Ermittlung aus dem Bereich der Informations- und Kommunikationstechnologien nach ihrer Nutzbarkeit in der Strafverfolgung.

Sie soll außerdem die Zusammenarbeit mit weiteren Dienststellen, die in diesem Bereich tätig sind, stärken und kooperiert dazu mit dem [BKA](#) und dem [LKA \[BW\]](#)²¹⁷.

²¹⁵ [CIO Baden-Württemberg, Aufgaben des CIO/CDO.](#)

[Landesrecht BW Bürgerservice, Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg \(E-Government-Gesetz Baden-Württemberg – EGovG BW\).](#)

²¹⁶ [Staatsministerium Baden-Württemberg, Sicherheitszentrum IT in der Finanzverwaltung vorgestellt.](#)

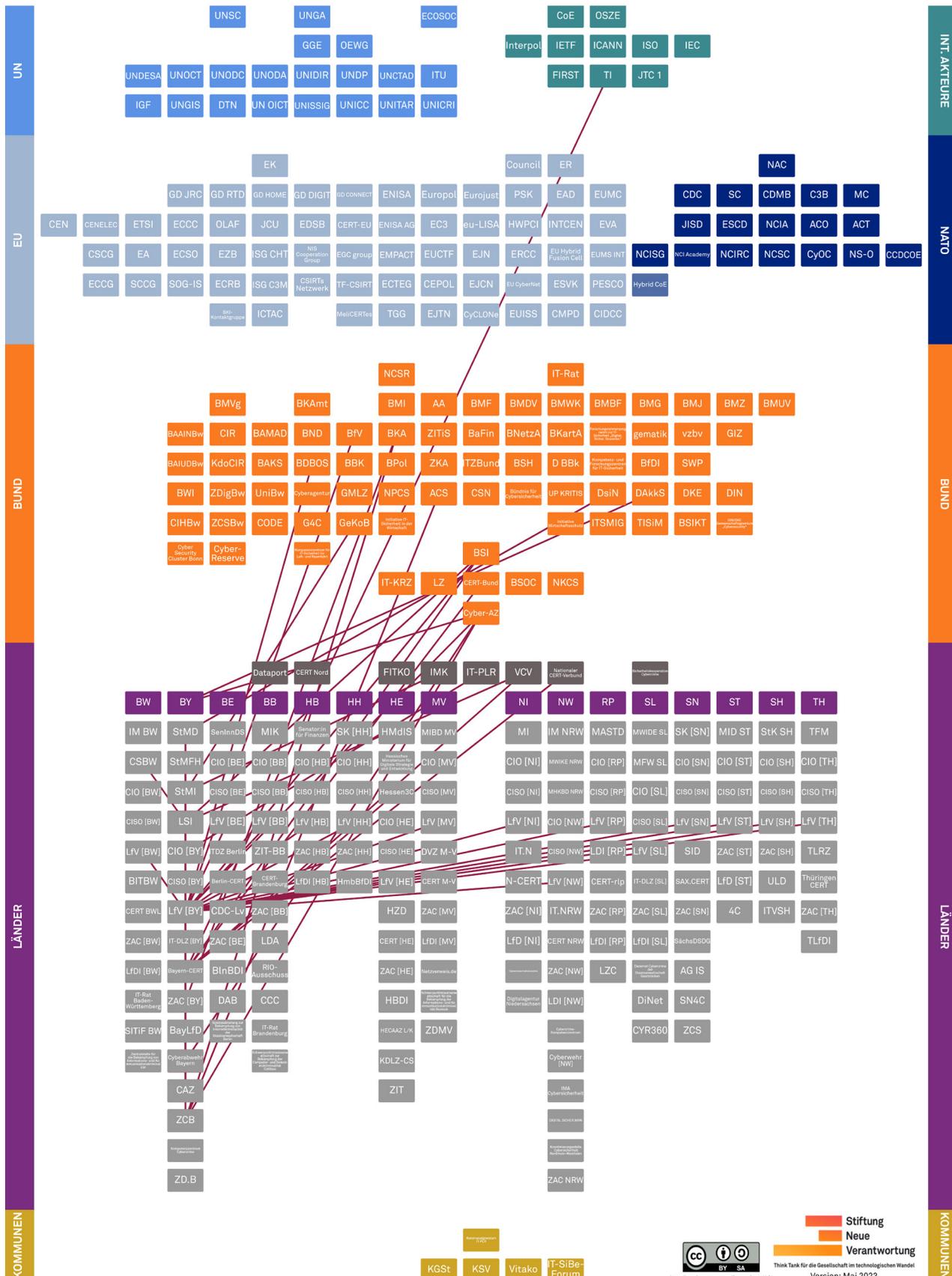
²¹⁷ [Ministerium der Justiz und für Europa Baden-Württemberg, Zentralstelle für die Bekämpfung von informations- und Kommunikationskriminalität eingerichtet. \(Webseite entfernt\)](#)



Impuls
Mai 2023

Deutschlands staatliche Cybersicherheitsarchitektur

9.2 Bayern (BY)





Das Land Bayern ist durch die Cyberabwehr Bayern sowie die Bamberger Schwerpunktstaatsanwaltschaft Cyber im *Cyber-AZ* vertreten. Es ist zudem einer der Gesellschafter der *DAkKS*.

Überblick

- **Relevante Policy-Dokumente:**

- 2022: Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG)
- 2015: Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz, BayEGovG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:**

- Bayerisches Staatsministerium für Digitales (StMD, Abteilung B: Digitale Verwaltung, IT-Strategie und IT-Recht, Referat B1: Grundsatzfragen, IT-Strategie und IT-Recht, Unternehmensportal + Referat B2: IT-Planungsrat, Föderale IT-Kooperation (FITKO), Single Digital Gateway).

*Das StMD kooperiert mit *DsiN*²¹⁸.*

- Bayerisches Staatsministerium der Finanzen und für Heimat (StMFH, Abteilung VII: Digitalisierung, Breitband und Vermessung, Referat 77: IT-Strategie, IT-Sicherheit, IT-Infrastruktur)²¹⁹.
- Bayerisches Staatsministerium des Innern, für Sport und Integration (StMI, Abteilung E: Verfassungsschutz, Cybersicherheit)

*Der:die bayerische Innenminister:in nimmt an der *IMK* teil²²⁰.*



- **Landes-CIO [BY]:** Das Land Bayern hat eine:n Beauftragte:n für Informations- und Kommunikationstechnik der Bayerischen Staatsregierung bestimmt. Der:die CIO Bayern übernimmt beispielsweise Verantwortung für die IT- und E-Government-Strategie sowie die Digitalisierung der Verwaltung.

*Aktuell wird die Position von dem:der Bayerischen Staatsminister:in für Digitales (StMD) ausgefüllt. Er:sie vertritt Bayern im *IT-PLR*²²¹.*

²¹⁸ [Bayerisches Staatsministerium für Digitales, Organisationsplan.](#)

²¹⁹ [Bayerisches Staatsministeriums der Finanzen und für Heimat, Organisationsplan.](#)

²²⁰ [Bayerisches Staatsministerium des Innern, für Sport und Integration, Organigramm.](#)

[Bayerisches Staatsministerium des Innern, für Sport und Integration, Schutz vor Cybergefahren.](#)

²²¹ [Bayerisches Staatsministerium für Digitales, IT-Beauftragte der Bayerischen Staatsregierung.](#)



- **Landes-CISO [BY]:** Bayern's IT-Sicherheitsbeauftragte:r verantwortet die Implementierung von IT-Sicherheitsmaßnahmen innerhalb der öffentlichen Verwaltung Bayerns, berichtet an den:die Leiter:in der ministeriellen Abteilung VII für Digitalisierung, Breitband und Vermessung.

*Er:sie ist im **StMFH** angesiedelt und ihm:ihr obliegt die Fachaufsicht über das **bayerische CERT**²²².*



- **Behördlicher IT-Dienstleister:** IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) ist angegliedert an das Bayerische Landesamt für Digitalisierung, Breitband und Vermessung (LDBV), welches sich im Geschäftsbereich des **StMFH** befindet²²³.



- **CERT:** Das Bayern-CERT ist am **LSI** angesiedelt.

*Es beteiligt sich am Nationalen **CERT-Verbund** sowie **TI**²²⁴.*



- **LFV [BY]:** In Bayern befasst sich die dortige Landesbehörde für Verfassungsschutz in ihrer Abteilung 5 unter anderem mit Wirtschaftsschutz und Spionageabwehr. Dort ist ebenfalls das **CAZ** und die ihm unterstellte **Cyberabwehr** angesiedelt. Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das **BSI** unterstützt werden²²⁵.



- **Institutionelle Ansässigkeit der ZAC [BY]:** Bayerisches Landeskriminalamt. Die bayerische ZAC bietet ebenso präventive Beratung an und steht neben Unternehmen auch Bürger:innen zur Verfügung²²⁶.



- **Landesdatenschutzbehörde:** Bayerische:r Landesbeauftragte:r für den Datenschutz (BayLfD).

*Er:sie ist an der **Cyberabwehr Bayern** beteiligt²²⁷.*

222 [IT-Beauftragter der Bayerischen Staatsregierung, IT-Sicherheitsstrukturen in Bayern.](#)

[Landesamt für Sicherheit in der Informationstechnik Bayern, IT-Sicherheitskonferenz für niederbayerische Kommunen am 20.02.2019 in Deggendorf.](#)

223 [Bayerisches Staatsministerium der Finanzen und für Heimat, Behörden und Staatsbetriebe im Ressort.](#)

[Landesamt für Digitalisierung, Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern.](#)

224 [Landesamt für Sicherheit in der Informationstechnik, Staatsverwaltung.](#)

225 [Landesamt für Verfassungsschutz Bayern, Organisation.](#)

[Landesamt für Verfassungsschutz Bayern, Spionageabwehr / Wirtschaftsschutz.](#)

226 [Bayerische Polizei, Zentrale Ansprechstelle Cybercrime – Kontakt für Unternehmen.](#)

[Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Initiativen der Landespolizeien.](#)

[Cyberabwehr Bayern, Cybersicherheit für bayerische Unternehmen und Behörden.](#)

227 [Der Bayerische Landesbeauftragte für den Datenschutz, Cybersicherheit.](#)



Weitere Akteure in Bayern:



Cyberabwehr Bayern

Die Cyberabwehr ist eine Informations- und Koordinierungsplattform und garantiert einen schnellen Austausch zwischen staatlichen Institutionen im Bereich der Cybersicherheit. Die an der Cyberabwehr teilnehmenden Behörden werden durch die Cyberabwehr Bayern über IT-Vorfälle informiert und können entsprechende Maßnahmen einleiten. Neben dieser Akuthilfe durch eine Erfassung, Bewertung und Weitergabe von Informationen zu Vorfällen auf die IT-Sicherheitsstruktur soll durch die Cyberabwehr Bayern auch ein Überblick über die Gefährdungslage im Cyberraum gegeben und ein bayerisches Lagebild geschaffen werden. Eine weitere Aufgabe ist der krisensichere Ausbau des Digitalfunks, der u.a. von der bayerischen Polizei und Feuerwehr genutzt wird.

Die Cyberabwehr Bayern ist im CAZ im LfV [BY] verortet. Teil der Cyberabwehr sind das LKA [BY], das LSI, die ZCB, das Bayerische Landesamt für Datenschutzaufsicht und der BayLfD sowie das CAZ. Es ist als Partner im Cyber-AZ vertreten²²⁸.



Cyber-Allianz-Zentrum (CAZ)

Das Cyber-Allianz-Zentrum Bayern unterstützt in Bayern ansässige Unternehmen, Hochschulen, Betreiber Kritischer Infrastrukturen im Bereich der Prävention und Abwehr elektronischer Operationen. Das CAZ fungiert als staatliche Steuerungs- und Koordinierungsstelle in Bayern und vertraulicher Ansprechpartner für betroffene Institutionen. Nach einer forensischen Analyse und nachrichtendienstlichen Bewertung erhalten diese eine Antwort mit Handlungsempfehlungen. Außerdem kontaktiert das CAZ möglicherweise von einem ähnlichen Vorfall betroffene Unternehmen oder Einrichtungen mit Informationen zu den Operationsmustern.

Das CAZ war die erste institutionelle Säule der „Initiative Cybersicherheit Bayern“ des StMI und gehört zum LfV [BY]²²⁹.



Kompetenzzentrum Cybercrime

Das Kompetenzzentrum Cybercrime (Dezernat 54) wurde beim Landeskriminalamt Bayern eingerichtet. Eine der Aufgaben des Kompetenzzentrum Cybercrime ist es, den Ernstfall, also beispielsweise einen Cybervorfall, in Krisenstabsübungen mit Unternehmen und Behörden, die für den Erhalt der öffentlichen Ordnung unverzichtbar sind, zu simulieren. Darüber hinaus nimmt es sich solcher Fälle von Cyber-

²²⁸ [Bayernkurier, Bayern stärkt die Cyber-Abwehr.](#)
[StMI Bayern, Bayern stärkt Cyberabwehr und Digitalfunk.](#)
[Tagesspiegel, Cyberabwehr: Neues Lagezentrum in Bayern geplant.](#)
[Verfassungsschutz Bayern, Cyberabwehr Bayern.](#)

²²⁹ [Bayerisches Landesamt für Verfassungsschutz, Cyber-Allianz-Zentrum Bayern \(CAZ\).](#)



kriminalität an, die überregionale Bedeutung haben und von den örtlichen Polizeidienststellen nicht bearbeitet werden können²³⁰.



Landesamt für Sicherheit in der Informationstechnik Bayern (LSI)

Das Landesamt für Sicherheit in der Informationstechnik Bayern hat sich den Schutz bayerischer IT-Infrastrukturen zur Aufgabe gemacht. Es soll Gefahren für informationstechnische Sicherheit abwehren, öffentliche dem Behördennetz angeschlossene Stellen bei der Abwehr entsprechender Bedrohungen unterstützen, Mindeststandards entwickeln und deren Einhaltung überprüfen, sowie Warnungen aussprechen. Auf Anfrage kann das LSI auch beratend und unterstützend gegenüber „staatliche[n] und kommunale[n] Stellen, öffentliche[n] Unternehmen, Betreiber[n] kritischer Infrastrukturen und weitere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen“ tätig werden. Das LSI kann an Kommunen das Siegel „Kommunale IT-Sicherheit“ vergeben.



Zentralstelle Cybercrime Bayern (ZCB)

Die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg verantwortet herausgehobene Ermittlungsverfahren im Bereich der Cyberkriminalität in ganz Bayern. In Abstimmung mit dem Bayerischen Justizministerium (StMJ) arbeitet die Zentralstelle auch zu verfahrensunabhängigen Fragestellungen im Bereich der Cyberkriminalität. Der Bereich setzt sich aus auf Cyberkriminalität spezialisierten Staatsanwält:innen und IT-Forensiker:innen zusammen. In der Vergangenheit brachte Bayern aufbauend auf der Arbeit der ZCB einen Antrag zur Nutzung von „Spielräumen“ bei der Speicherung von IP-Adressen im Bundesrat ein. Hierzu kooperiert sie mit den Zentralstellen anderer Bundesländer und beteiligt sich in fachlichen Gremien im In- und Ausland. Sie unterstützt die bayerische Justiz außerdem bei der Aus- und Fortbildung im Bereich Cyberkriminalität. Sie kooperiert außerdem mit den zuständigen Spezialisten:innen der bayerischen Polizei oder des BKA und mit internationalen Partnern, beispielsweise bei Verfahren zu organisierter Cyberkriminalität. Die Zentralstelle ist Mitglied in der ACS²³¹.



Zentrum Digitalisierung Bayern (ZD.B)

Das ZD.B soll als regionenübergreifende Forschungs- und Kooperationsplattform in Bayern dienen und Kooperationen zwischen Wirtschaft und Wissenschaft fördern, gesellschaftlichen Dialog mitprägen sowie die Nachwuchsförderung unterstützen. Als eine von insgesamt 11 Plattformen besteht am ZD.B eine Themenplattform Cybersecurity. Angebote der Themenplattformen stehen der bayerischen Wirtschaft, Wissenschaft sowie Kommunen offen. Die Themenplattform Cybersecurity hat es

²³⁰ Bayerische Staatsregierung, Cyber-Kompetenzzentrum im Landeskriminalamt.

²³¹ Bundesamt für Sicherheit in der Informationstechnik, Teilnehmerliste der Allianz für Cyber-Sicherheit. Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB). Bundesrat (Drucksache 572/22), Antrag des Freistaates Bayern.



sich zum Ziel gesetzt, die Wettbewerbsfähigkeit bayerischer Unternehmen sowie deren Resilienz gegenüber Cyberoperationen zu verbessern, das Bewusstsein für Themen der Cybersicherheit in Wirtschaft und Gesellschaft zu schärfen sowie zu öffentlichem Diskurs in diesem Kontext beizutragen.

Das ZD.B wurde durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi) als Leitprojekt des Maßnahmenpaketes BAYERN DIGITAL etabliert²³².

²³² [Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie, Zentrum Digitalisierung.Bayern.](#)
[Bayerisches Staatsministerium für Wissenschaft und Kunst, Zentrum Digitalisierung.Bayern.](#)
[Zentrum Digitalisierung.Bayern, ZD.B-Themenplattform Cybersecurity. Schutz gegen digitale Bedrohungen.](#)



Überblick

- **Relevante Policy-Dokumente:**

- 2016: [Gesetz zur Förderung des E-Government \(E-Government-Gesetz Berlin \(EGovG Bln\)\)](#)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Senatsverwaltung für Inneres, Digitalisierung und Sport (SenInnDS, Abteilung III: Öffentliche Sicherheit und Ordnung, Referat III E: Ressourcen, IT-Angelegenheiten für Polizei und Feuerwehr, Cybersicherheit). Dort ist auch eine Arbeitsgruppe Cybersicherheit (AG Cybersicherheit) angesiedelt, die vornehmlich zu dem Schutz Kritischer Infrastrukturen sowie Cyberkriminalität als identifizierte fachliche Schwerpunkte arbeitet.

Die SenInnDS und das [BSI](#) haben eine Absichtserklärung zur verstärkten Zusammenarbeit vereinbart. Abteilung III der SenInnDS ist Mitglied der [ACS](#). Der:die Innensenator:in Berlins gehört zu den Teilnehmer:innen der [IMK](#)²³³.



- **Landes-CIO [BE]:** In Berlin übernimmt die:der Staatssekretär:in für Informations- und Kommunikationstechnik in der [SenInnDS](#) die Position des Landes-CIOs, die an den:die Innensenator:in berichtet.

Er:sie vertritt das Land Berlin im [IT-PLR](#)²³⁴.



- **Landes-CISO [BE]:** Der:die Berliner Landesbeauftragte:r für Informationssicherheit (Landes-InfSiBe) ist unmittelbar bei dem:der Staatssekretär:in für Informations- und Kommunikationstechnik angesiedelt. Neben der Ausübung von Aufgaben zur Umsetzung und Steuerung von Prozessen und Standards im Bereich der Informationssicherheit, verfügt der:die Landes-InfSiBe über ein direktes Vortragsrecht gegenüber dem:dem Landes-CIO [BE]. Für den Bereich der IT-Sicherheit obliegt dem:der Landes-InfSiBe die fachliche Steuerung des ITDZ Berlin²³⁵.

²³³ [Bundesamt für Sicherheit in der Informationstechnik und Senatsverwaltung für Inneres und Sport, Absichtserklärung zur vertieften Kooperation zwischen dem Bundesamt für Sicherheit in der Informationstechnik und der Senatsverwaltung für Inneres und Sport des Landes Berlin.](#)

[Senatsverwaltung für Inneres und Sport, Arbeitsgruppe Cybersicherheit: Über uns.](#)

[Senatsverwaltung für Inneres und Sport, Organigramm.](#)

[Senatsverwaltung für Inneres und Sport, Stärkung der Bund-Länder-Zusammenarbeit im Bereich Cyber-Sicherheit.](#)

²³⁴ [CIO, Sabine Smentek wird CIO vom Land Berlin.](#)

²³⁵ [Senatsverwaltung für Inneres und Sport Berlin, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin.](#)



- **Behördlicher IT-Dienstleister:** IT-Dienstleistungszentrum Berlin (ITDZ Berlin).

Die Rechtsaufsicht kommt der SenInnDS zu²³⁶.



- **CERT:** Das Berlin-CERT wird durch das ITDZ Berlin betrieben²³⁷.



- **LfV [BE]:** Die SenInnDS beherbergt zudem die Verfassungsschutzbehörde des Landes Berlin (Abteilung 2). Dort sind Zuständigkeiten für den Wirtschafts- und Geheimschutz (Referat Wi/GSB) sowie die Spionageabwehr (Referat II D) angesiedelt.

In der Vergangenheit wurde der Aufgabenbereich der Cyberabwehr im Rahmen einer Verwaltungsvereinbarung seitens der SenInnDS an das BfV übertragen. Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden²³⁸.



- **Institutionelle Ansässigkeit der ZAC [BE]:** Landeskriminalamt Berlin²³⁹.



- **Landesdatenschutzbehörde:** Berliner Beauftragte:r für Datenschutz und Informationsfreiheit (BlnBDI)²⁴⁰.

Weitere Akteure in Berlin:



Cyber Defense Center der Landesverwaltung Berlin (CDC-Lv)

Das Cyber Defense Center der Berliner Landesverwaltung ist im dortigen ITDZ Berlin angesiedelt. Es besteht aus einem Security Operation Center (SOC), dem Berlin-CERT, einem Bereich für Analyse und Forensik und einem Bereich für IT-Sicherheitskoordination und Consulting. Neben dem Schutz der Daten der Berliner Bürger:innen, kommt dem CDC-Lv auch die Erkennung und Abwehr von Operationen auf das Berliner Landesnetz zu.

Das CDC-Lv berichtet durch das Berlin-CERT an den:die CISO [BE] Auf Arbeitsebene besteht Austausch mit dem Berliner BSI-Verbindungsbüro²⁴¹.

²³⁶ [Berliner Vorschriften- und Rechtsprechungsdatenbank, Gesetz über die Anstalt des öffentlichen Rechts IT-Dienstleistungszentrum Berlin.](#)
[ITDZ Berlin, Profil.](#)

²³⁷ [ITDZ Berlin, Sicherheit.](#)

²³⁸ [Senatsverwaltung für Inneres und Sport Berlin, Organigramm.](#)
[Senatsverwaltung für Inneres und Sport Berlin, Verfassungsschutzbericht 2019.](#)

²³⁹ [Polizei Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.](#)

²⁴⁰ [Berliner Beauftragte für Datenschutz und Informationsfreiheit, Über uns.](#)

²⁴¹ [ITDZ Berlin, Innovationsmanagement im ITDZ Berlin.](#)
Hintergrundgespräch, 2021.



Digitalagentur Berlin (DAB)

Die Berliner Digitalagentur stellt Unterstützungsangebote für Berliner Unternehmen zur Verfügung. Ihr Portfolio umfasst u.a. auch eine „Cyberhotline“ und Webinare zu IT-Sicherheit für diese. Die „Cyberhotline“ fungiert dabei für Berliner Unternehmen als Ansprechpartner im Falle von IT- und cybersicherheitsrelevanten Notfällen mit Ersthelfer:innen am anderen Ende der Leitung. Im Bedarfsfall kann die Cyberhotline auch an private IT-Sicherheitsfirmen aus ihrem Netzwerk weitervermitteln.

Das Land Berlin fördert und finanziert die Digitalagentur. Zu ihren Netzwerkpartnern gehört u.a. das [DIN](#)²⁴².



Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin

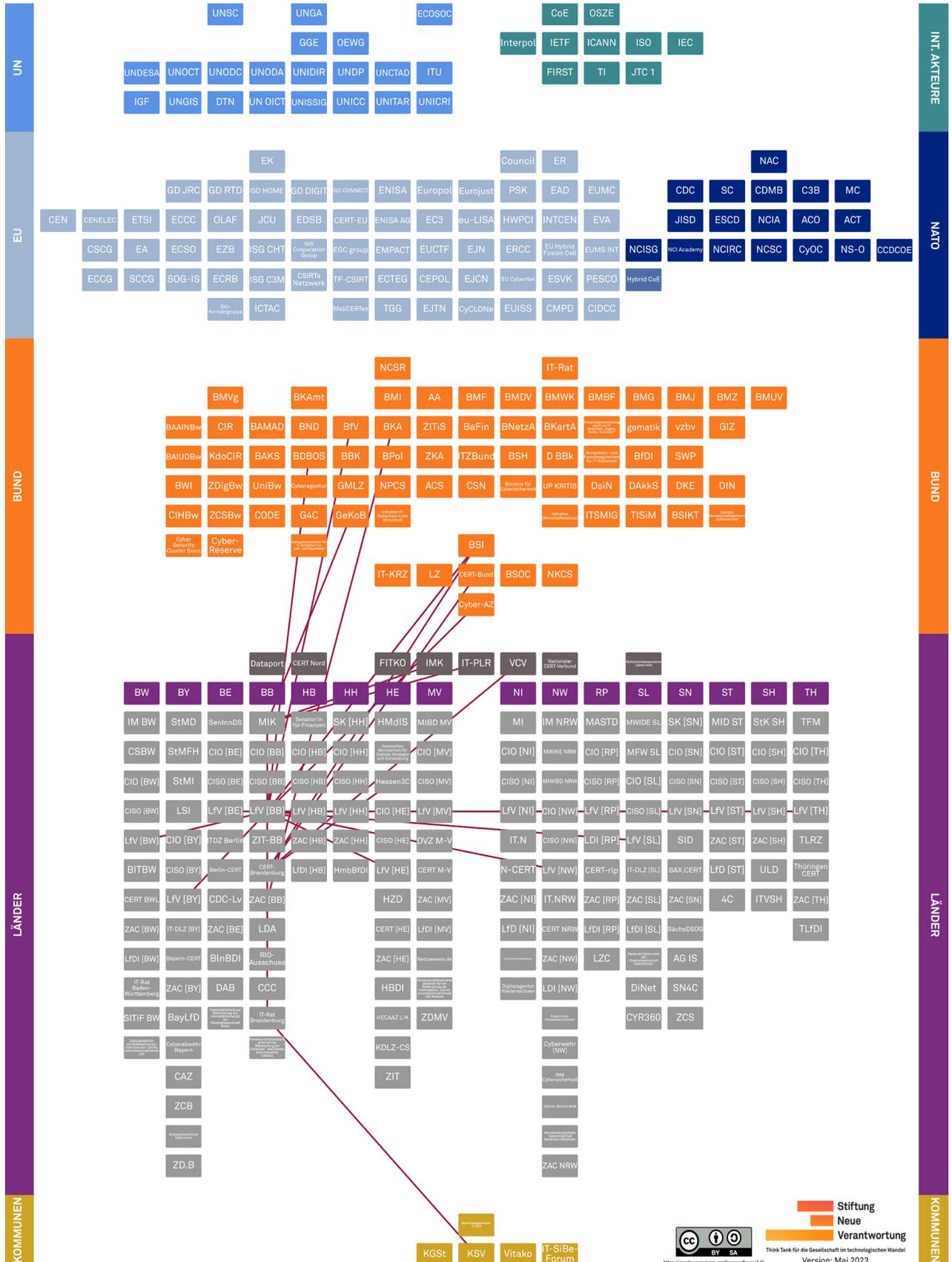
Innerhalb der Staatsanwaltschaft Berlin besteht eine Spezialabteilung zur Cyberkriminalität. Schwerpunkt der Abteilung ist der Waren- und Warenkreditbetrug im Zusammenhang mit Online-Handel²⁴³.

²⁴² [Digitalagentur Berlin, IT-Sicherheit.](#)
[Digitalagentur Berlin, Netzwerk.](#)

²⁴³ [Diana Nadeborn, Berliner Staatsanwaltschaft rüstet auf gegen Cyberkriminalität.](#)



9.4 Brandenburg (BB)





Überblick

- **Relevante Policy-Dokumente:**
 - 2020: Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg (E-Government- und IT-Organisationsrichtlinie)
 - 2018: Gesetz über die elektronische Verwaltung im Land Brandenburg (Brandenburgisches E-Government-Gesetz, BbgEGovG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Ministerium des Innern und für Kommunales (MIK, Abteilung 6: Digitalisierung, E-Government und IT-Leitstelle, Referat 64: IT-Leitstelle, IT-Sicherheit und CERT sowie IT-Infrastruktur des Landes Brandenburg, Koordinierungsstelle für IT- und Cyber-Sicherheit im MIK, Verfahrensverantwortung für die IT-Basiskomponenten gemäß BbgEGovG für Land und Kommune).

*Der:die brandenburgische Innenminister:in nimmt an der **IMK** teil²⁴⁴.*



- **Landes-CIO [BB]:** Das Land Brandenburg hat eine:n Chief Process Innovation Officer bestimmt, der:die sich auch im IT-Angelegenheiten des Landes kümmert.

*Er:sie ist **MIK** angesiedelt²⁴⁵.*



- **Landes-CISO [BB]:** In Brandenburg wird ein:e landesweite:r IT-Sicherheitsmanager:in durch Abteilung 6 (Digitalisierung, E-Government und IT-Leitstelle) innerhalb des **MIK** des Landes Brandenburg eingesetzt. Ihm:ihr kommt unter anderem die Koordinierung des gesamten IT-Sicherheitsmanagements sowie die Erstellung eines jährlichen IT-Sicherheitsberichtes zu.

*Abhängig von ihrer Schwere, wird der:die **IT-Sicherheitsmanager:in** durch das **CERT-Brandenburg** über etwaige Sicherheitsvorfälle informiert²⁴⁶.*



- **Behördlicher IT-Dienstleister:** Brandenburgischer IT-Dienstleister (ZIT-BB), welcher im Geschäftsbereich des MIK angesiedelt ist²⁴⁷.



- **CERT:** Das **CERT-Brandenburg** wird vom ZIT-BB betrieben²⁴⁸.

²⁴⁴ [Ministerium des Innern und für Kommunales Brandenburg, Organigramm.](#)

²⁴⁵ [CIO, Die IT-Chefs der Bundesländer.](#)

²⁴⁶ [Brandenburgisches Vorschriftensystem, Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg.](#)

²⁴⁷ [Brandenburgischer IT-Dienstleister, Start.](#)

²⁴⁸ [Brandenburgischer IT-Dienstleister, CERT-Brandenburg.](#)



- **LfV [BB]:** In Brandenburg ist die Landesverfassungsschutzbehörde im **MIK** angesiedelt (Abteilung 5). Unter ihre Arbeitsfelder fallen unter anderem die Spionageabwehr und der Wirtschaftsschutz. Im letzten Brandenburger Verfassungsschutzbericht wird unter anderem auch auf aktuelle Entwicklungen im sog. „Cyber-Extremismus“ Bezug genommen.

Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden²⁴⁹.



- **Institutionelle Ansässigkeit der ZAC [BB]:** Cyber-Competence-Center (CCC), Akteursbeschreibung s. unten²⁵⁰.



- **Landesdatenschutzbehörde:** Landesbeauftragte:r für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA)²⁵¹.

Weitere Akteure in Brandenburg:



Ausschuss der Ressort Information Officer (RIO-Ausschuss)

In Brandenburg bilden die Ressort Information Officers (RIO) aller Ressorts und der Staatskanzlei gemeinsam mit dem:der ersten Geschäftsführer:in des ZIT-BB sowie einem:r einer Vorsitzenden den RIO-Ausschuss. Der RIO-Ausschuss, der mindestens einmal pro Quartal zusammenkommt und Arbeitsgruppen einsetzen kann, beschließt auf operativer Ebene unter anderem die IT-Standards der Landesverwaltung und „Anforderungen an die landesweite Weiterentwicklung der IT-Infrastruktur“.

*Die:der Vorsitzende:r des RIO-Ausschusses ist ein:e Vertreter:in des **MIK**, der:die gegenüber dem:der **Landes-CIO [BB]** Ansprechperson für den RIO-Ausschuss ist. Unter anderem kann der:die **LDA** beratend an den Sitzungen teilnehmen²⁵².*



Cyber-Competence-Center (CCC)

Das Cyber-Competence-Center bündelt als Fachdienststelle im Landeskriminalamt Brandenburg personelle und fachliche Kompetenzen zur Bekämpfung und Aufklärung jeglicher Kriminalitätsbereiche im Zusammenhang mit dem Internet. Es übernimmt sowohl präventive als auch repressive Aufgaben und unterstützt Ermittlungen der Polizeidirektionen und -inspektionen zur Bekämpfung der Cyberkriminalität.

²⁴⁹ [Ministerium des Innern und für Kommunales, Aufbau und Organisation.](#)

[Ministerium des Innern und für Kommunales Brandenburg, Wirtschaftsschutz.](#)

[Ministerium des Innern und für Kommunales, Verfassungsschutzbericht des Landes Brandenburg 2019.](#)

²⁵⁰ [Polizei Brandenburg, Internetkriminalität.](#)

²⁵¹ [Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Über uns.](#)

²⁵² [Landesregierung Brandenburg, Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg \(E-Government- und IT-Organisationsrichtlinie\).](#)



Am CCC wurde auch die **ZAC [BB]** für Wirtschaftsunternehmen und Behörden eingerichtet²⁵³.



IT-Rat Brandenburg

Der IT-Rat Brandenburg wurde zur „strategischen Abstimmung und gemeinsamen Steuerung informationstechnischer Angelegenheiten der Ebenen übergreifenden Kooperation von Land und Kommunen“ in Brandenburg eingerichtet. Er diskutiert unter anderem aufkommende Themen des IT-PLR, zukünftige Ausgestaltungsmöglichkeiten für die brandenburgische IT- und E-Government-Strategie sowie „IT-Interoperabilitäts- und IT-Sicherheitsstandards für die Ebenen übergreifende Kommunikation“.

*Der IT-Rat setzt sich aus dem:der Chef:in der Staatskanzlei, dem:der **Landes-CIO [BB]**, den Staatssekretär:innen der für Finanzen und Wirtschaft zuständigen Ministerien, und je zwei Vertreter:innen des **Städte- und Gemeindebundes Brandenburg** und des **Landkreistages Brandenburg** zusammen. Dem:der Landes-CIO [BB] kommt der Vorsitz zu. Beratend kann ein:e Vertreter:in des **ZIT-BB** den Sitzungen beiwohnen²⁵⁴.*



Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetz- kriminalität Cottbus

Bei der Staatsanwaltschaft Cottbus ist die brandenburgische Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer und Datennetzkriminalität angesiedelt²⁵⁵.

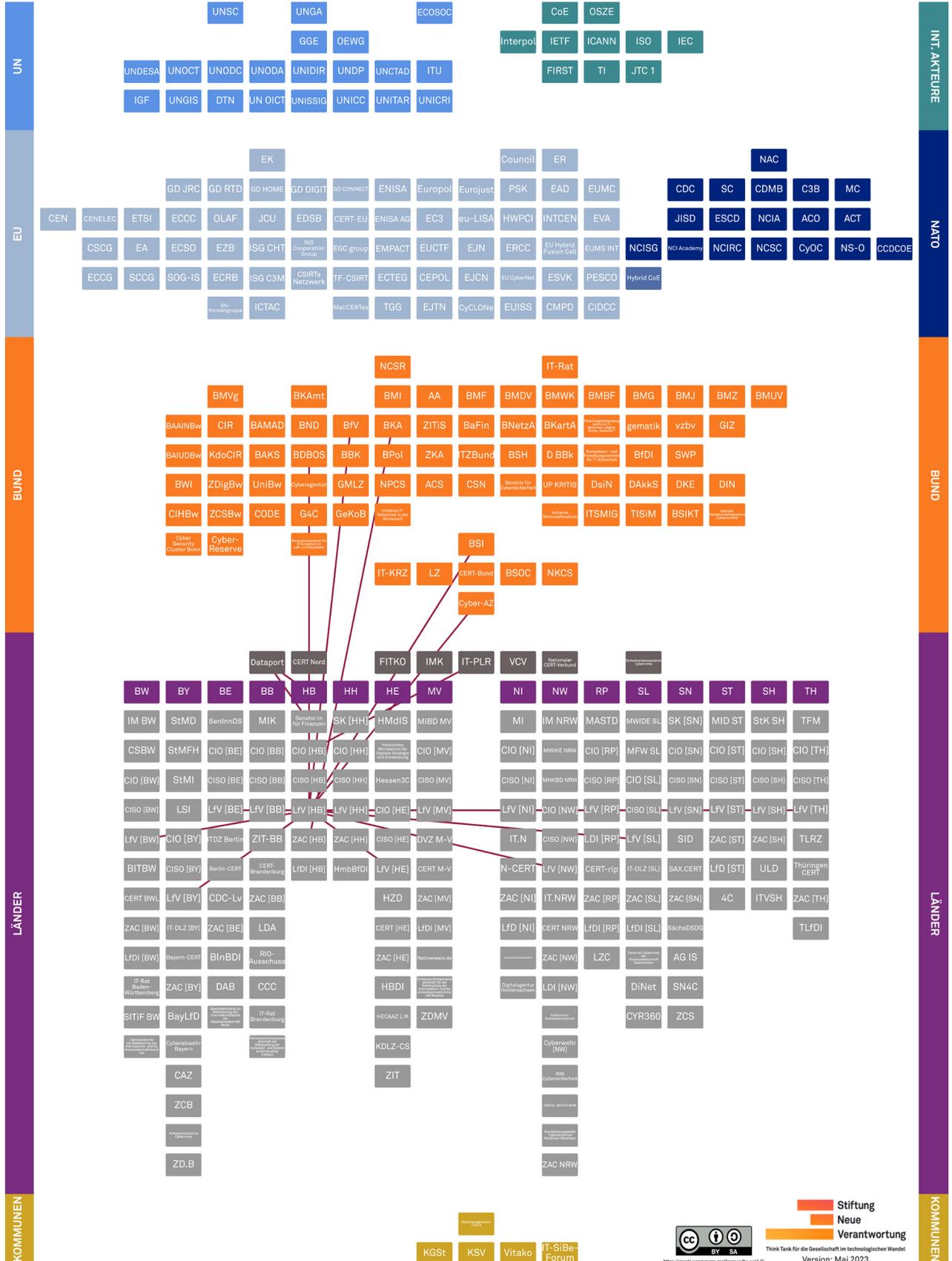
²⁵³ [Polizei Brandenburg, Cyber-Competence-Center im Landeskriminalamt.](#)

²⁵⁴ [Landesregierung Brandenburg, Gesetz über die elektronische Verwaltung im Land Brandenburg \(Brandenburgisches E-Government-Gesetz - BbgEGovG\).
Ministerium des Innern und für Kommunales des Landes Brandenburg, Bericht des IT-Beauftragten der Landesregierung.](#)

²⁵⁵ Staatsanwaltschaft Cottbus, Schwerpunktstaatsanwaltschaft. (Webseite entfernt)



9.5 Bremen (HB)





Das Land Bremen zählt zu den Unterzeichnern des bundesländerübergreifenden Staatsvertrages, durch den **Dataport** eingerichtet wurde.

Überblick

- **Relevante Policy-Dokumente:**

- 2023: [Bremische Cybersicherheitsstrategie](#)
- 2018: [Gesetz zur Förderung der elektronischen Verwaltung in Bremen](#)
- 2017: [Informationssicherheitsleitlinie der Freien Hansestadt Bremen \(IS-LL\)](#)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Der:die Senator:in für Finanzen (Abteilung 4: Zentrales IT-Management, Digitalisierung öffentlicher Dienste).

*Ein:e Vertreter:in der:des Senatoren:in für Finanzen gehört dem Verwaltungsrat **Dataport**'s an²⁵⁶.*



- **Landes-CIO [HB]:** In Bremen ist die CIO-Stelle bei dem:der Staatsrat:ätin des:der Senator:in für Finanzen verortet.

Er:sie vertritt Bremen im IT-PLR²⁵⁷.



- **Landes-CISO [HB]:** Der:die Bremer CISO ist bei der:dem Senator:in für Finanzen der Hansestadt angesiedelt. Er:sie erstellt einen nicht-öffentlichen Jahresbericht zur Informationssicherheit in der bremischen Verwaltung, um Probleme, Lösungen und Alternativen zu adressieren²⁵⁸.



- **Behördlicher IT-Dienstleister:** Dataport, Akteursbeschreibung s. unten (Kapitel 8.17).



- **CERT:** CERT Nord, Akteursbeschreibung s. unten (Kapitel 8.17).



- **LFV [HB]:** In der Eigenbeschreibung der Bremer Landesbehörde für Verfassungsschutz und im letzten Bremer Verfassungsschutzbericht wird auf keine originäre Zuständigkeit für Wirtschaftsschutz oder Cyberabwehr Bezug genommen.

Sofern erforderlich, können die LFV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden²⁵⁹.

²⁵⁶ [Bremische Bürgerschaft, Mitteilung des Senats vom 15. Januar 2019: Cybersicherheit in Bremen.](#)

[Der Senator für Finanzen Bremen, Abteilung 4: Zentrales IT-Management, Digitalisierung öffentlicher Dienste.](#)

²⁵⁷ [Freie Hansestadt Bremen, Staatsrat Dr. Martin Hagen.](#)

²⁵⁸ [CISO Bremen, Vorlage für die Sitzung des Senats am 14.7.2020. Jahresbericht zur Informationssicherheit in der bremischen Verwaltung.](#)

²⁵⁹ [Landesamt für Verfassungsschutz Bremen, Über Uns.](#)

[Freie Hansestadt Bremen, Verfassungsschutzbericht 2019.](#)



- **Institutionelle Ansässigkeit der ZAC [HB]:** Polizei Bremen. Dort befasst sich das Kommissariat K13 mit Cybercrime und Digitalen Spuren²⁶⁰.



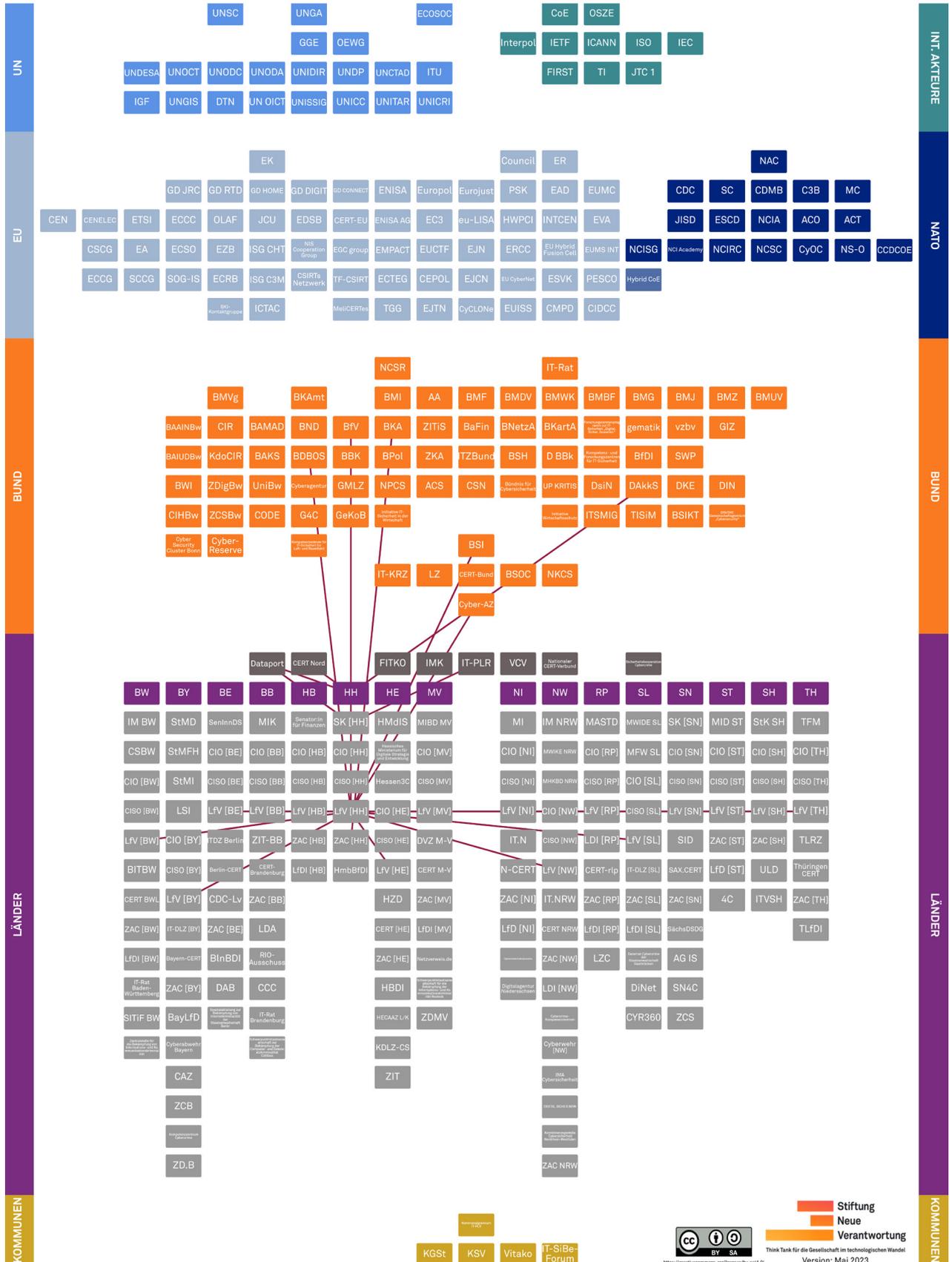
- **Landesdatenschutzbehörde:** Landesbeauftragte:r für Datenschutz und Informationsfreiheit (LfDI)²⁶¹.

²⁶⁰ [Polizei Bremen, Organigramm Direktion Kriminalpolizei / untere Ebene.](#)

²⁶¹ [Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen, Wir über uns.](#)



9.6 Hamburg (HH)





Das Land Hamburg ist einer der Gesellschafter der **DAkKS**. Es zählt zudem zu den Unterzeichnern des bundesländerübergreifenden Staatsvertrages, durch den **Dataport** eingerichtet wurde.

Überblick



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Senatskanzlei Hamburg (SK [HH]), Amt für IT und Digitalisierung (ITD).

*Ein:e Vertreter:in der SK gehört dem Verwaltungsrat **Dataport**'s an²⁶².*



- **Landes-CIO [HH]:** Hamburg bestimmt eine:n Chief Digital Officer (CDO), der:die das ITD (SK) leitet. Darüber hinaus ist im ITD zusätzlich auch der CIO des Landes angesiedelt, die:der das ITD stellvertretend leitet²⁶³.



- **Landes-CISO [HH]:** In der Freien Hansestadt Hamburg wurde ein:e Informationssicherheitsbeauftragte:r (InSiBe) innerhalb des ITD der SK [HH] eingerichtet²⁶⁴.



- **Behördlicher IT-Dienstleister:** Dataport, Akteursbeschreibung s. unten (Kapitel 8.17).



- **CERT:** CERT Nord, Akteursbeschreibung s. unten (Kapitel 8.17).



- **LfV [HH]:** In der Landesbehörde für Verfassungsschutz Hamburg wird in der Abteilung V3 unter anderem zur Spionageabwehr gearbeitet. Das unterstellte Referat V32 verfügt über Kompetenzen und Aufgaben im Bereich des Wirtschaftsschutzes. Sein letzter Verfassungsschutzbericht verweist zudem auf Gefahren durch Cyberspionage, Cybersabotage und Cyberoperationen.

Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden²⁶⁵.



- **Institutionelle Ansässigkeit der ZAC [HH]:** Polizei Hamburg, LKA 54 Fachkommissariat Cybercrime. Mit dem Fachkommissariat wurde eine Dienststelle geschaffen, die die Kompetenzen von kriminalpolizeilicher Ermittlung und angestellten Informatikern bündelt und so polizeiliches und technologisches Wissen

²⁶² Senat der Freien und Hansestadt Hamburg Senatskanzlei, [Arbeitsstrukturen des Amtes für IT und Digitalisierung \(ITD\)](#). (Webseite entfernt)

²⁶³ Senatskanzlei Hamburg, [Senatskanzlei Amt für IT und Digitalisierung](#).

²⁶⁴ [Freie Hansestadt Hamburg, Rahmen-Sicherheitskonzept](#).

²⁶⁵ [Landesamt für Verfassungsschutz Hamburg, Organigramm des Landesamtes für Verfassungsschutz, Behörde für Inneres und Sport Freie Hansestadt Hamburg, Verfassungsschutzbericht 2019](#).



zusammenführt. IT-Sicherheit und Cybercrime stellen zudem ein Handlungsfeld des von der Hamburger Polizei koordinierten „Netzwerk Standortsicherheit Hamburg“ dar²⁶⁶.



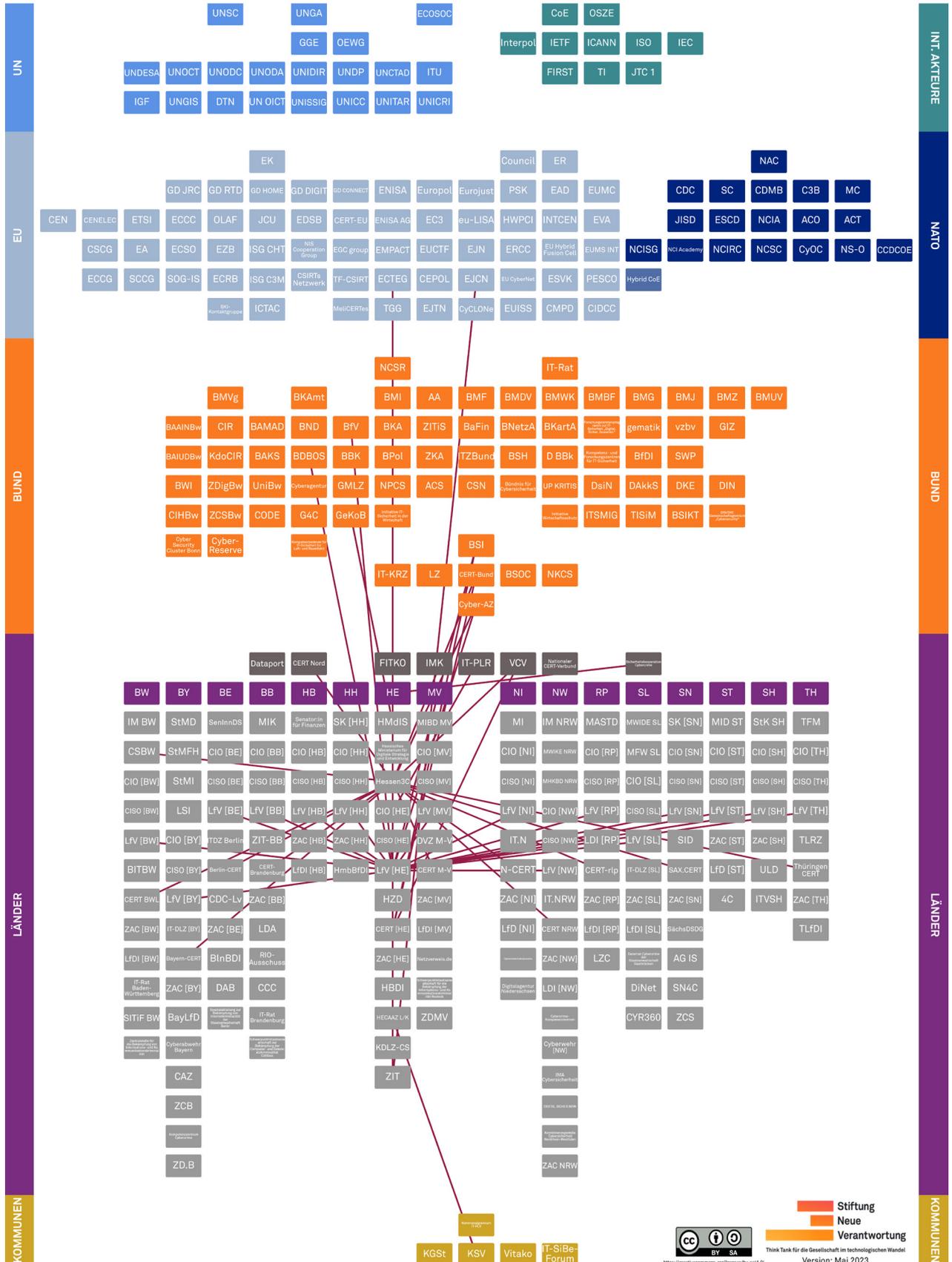
- **Landesdatenschutzbehörde:** Hamburgische:r Beauftragte:r für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg (HmbBfDI)²⁶⁷.

²⁶⁶ [Koordinierungsbüro „Netzwerk Standortsicherheit Hamburg“, IT-Sicherheit und Cybercrime. Polizei Hamburg, Zentrale Ansprechstelle Cybercrime \(ZAC\).](#)

²⁶⁷ [Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg, Tätigkeitsberichte des HmbBfDI.](#)



9.7 Hessen (HE)





Das Land Hessen ist im **NCSR** vertreten und beteiligt sich mit seiner Polizeiakademie an der **ECTEG**. Das hessische Landeskriminalamt beteiligt sich an der **Sicherheitskooperation Cybercrime**.

Überblick

- **Relevante Policy-Dokumente:**

- 2021: Informationssicherheitsleitlinie für die hessische Landesverwaltung
- 2020: Förderrichtlinie Cybersicherheitsforschung in Hessen
- 2018: Hessisches Gesetz zur Förderung der elektronischen Verwaltung (Hessisches E-Government-Gesetz, HEGovG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:**

- Hessisches Ministerium des Innern und für Sport (HMdIS, Abteilung VII: Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung).

*Das **KDLZ-CS** ist ein kommunales Unterstützungsangebot seitens des HMdIS²⁶⁸.*

- Hessisches Ministerium für Digitale Strategie und Entwicklung²⁶⁹.



- **Landes-CIO [HE]:** Der:die CIO des Landes Hessen ist für die Informationstechnologie und E-Government-Themen des Landes zuständig.

*Der:die CIO ist bei dem:der **Hessischen Minister:in für Digitale Strategie und Entwicklung** angesiedelt. Er:sie wird in ihrer:seiner Tätigkeit durch eine:n Co-CIO unterstützt. Der:die Landes-CIO vertritt Hessen im IT-PLR²⁷⁰.*



- **Landes-CISO [HE]:** Derzeit ist in Hessen der:die Leiter:in der Abteilung VII „Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung“ des **HMdIS** in Personalunion der:die Landes-CISO.

*Ein:e Vertreter:in des **Hessen3C** agiert als seine:ihre Stellvertreter:in²⁷¹.*

²⁶⁸ [Hessisches Ministerium des Innern und für Sport, Organisationsplan des Hessischen Ministerium des Innern und für Sport.](#)

²⁶⁹ [Hessische Staatskanzlei: Organisationsplan.](#)

²⁷⁰ [Hessische Ministerin für Digitale Strategie und Entwicklung, CIO.](#)

[Hessische Ministerin für Digitale Strategie und Entwicklung, Drei Fragen an Roland Jabkowski.](#)

²⁷¹ [Ministerium des Innern und für Sport Hessen, Der zentrale Informationssicherheitsbeauftragte der Landesverwaltung.](#)

[Hessischer Landtag \(Drucksache 20/1520\), Antwort auf Kleine Anfrage: Umsetzung Informationssicherheitsrichtlinie.](#)



- **Behörlicher IT-Dienstleister:** Hessische Zentrale für Datenverarbeitung (HZD), die der Dienst- und Fachaufsicht des hessischen Ministeriums der Finanzen (HMdF) untersteht²⁷².



- **CERT:** Das hessische CERT ist bei der Gründung von Hessen3C in dessen Bereich Cybersecurity integriert worden. Dieser nimmt alle Aufgaben des CERTs wahr²⁷³.



- **LfV [HE]:** In der Landesbehörde für Verfassungsschutz Hessen befasst sich das Dezernat 30 mit der Spionageabwehr und Wirtschaftsschutz. Zum Schutz der Wirtschaft wird Cyberspionage als ein expliziter Aufgabenbereich aufgeführt.

*Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das **BSI** unterstützt werden²⁷⁴.*



- **Institutionelle Ansässigkeit der ZAC [HE]:** Landeskriminalamt Hessen²⁷⁵.



- **Landesdatenschutzbehörde:** Hessische:r Beauftragte:r für Datenschutz und Informationsfreiheit (HBDI)²⁷⁶.

Weitere Akteure in Hessen:



Hessisches Cyberabwehrausbildungszentrum Land/Kommunen (HECAAZ L/K)

Im HECAAZ L/K soll u.a. durch Übungen vor Ort die IT- und Cybersicherheit hessischer Kommunen verbessert werden. Dieses Angebot für kommunale Entscheider:innen in Hessen umfasst beispielsweise auch die Entwicklung von entsprechenden Strategien oder Notfallplänen.

*Das HECAAZ L/K wurde von **Hessen3C** in Zusammenarbeit mit einem kommunalen IT-Dienstleister entwickelt, letzterem kommt die operative Durchführung der Ausbildungselemente zu. Die Schulungen finden in Abstimmung mit und Unterstützung der **KSV** statt²⁷⁷.*



Hessen Cyber Competence Center (Hessen3C)

Das Hessen Cyber Competence Center ist eine Kompetenzstelle, die eine interdisziplinäre Zusammenarbeit und institutionalisierte Kooperation staatlicher Behörden in

²⁷² [Hessische Zentrale für Datenverarbeitung, Organisation.](#)

²⁷³ [Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.](#)

²⁷⁴ [Landesamt für Verfassungsschutz Hessen, Organigramm.](#)

[Landesamt für Verfassungsschutz Hessen, Wirtschaftsschutz. Was ist Cyberspionage?](#)

²⁷⁵ [Bundeskriminalamt, Polizei – Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen.](#)

²⁷⁶ [Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Über uns.](#)

²⁷⁷ [Hessisches Ministerium des Innern und für Sport, Innenministerium erweitert Beratungsangebot für Kommunen.](#)



Hessen ermöglicht. Es ging aus der Kompetenzstelle Cybersicherheit, einer Stabsstelle im Hessischen Innenministerium, hervor, die vollständig in Hessen3C aufgegangen ist. Hessen3C's Aufgabe ist es, die Sicherheit der hessischen IT zu verbessern, cyberspezifische Gefahren abzuwehren, eine höhere Effizienz der Bekämpfung von Cyberkriminalität zu schaffen und Synergien zu finden. Das Hessen3C steht für die hessische Landes- und Kommunalverwaltung sowie KMU rund um die Uhr als Ansprechpartner bei Cybersicherheitsvorfällen im Land Hessen bereit. Im Rahmen von Hessen3C's Warn- und Informationsdienst können hessische Kommunen u.a. tägliche Schwachstellenberichte erhalten. Sofern notwendig, steht Kommunen auch ein Mobile Incident Response Team (MIRT) zur Verfügung.

*Hessen3C gehört zum **HMdIS** und tauscht sich mit der Hessischen Polizei und dem **LfV [HE]** zu Cyberthemen aus und erstellt gemeinsam ein Lagebild. Mitarbeiter:innen des Hessen3Cs stammen aus dem **CERT Hessens**, der Polizei und des **LfV [HE]** – so sollen organisationsübergreifende Expertise und Dienstleistungen im Bereich der Cybersicherheit zur Verfügung gestellt werden. Das Hessen3C betreibt das **CERT-Hessen** und leitet das **IT-Krisenmanagement** der Landesverwaltung. Das **HECAAZ L/K** wurde von Hessen3C in Zusammenarbeit mit einem kommunalen IT-Dienstleister entwickelt. Es bestehen Arbeitsbeziehungen mit dem **VCV**, dem **CERT-Bund** sowie den weiteren **Länder-CERTs**. Hessen3C ist zudem im **Cyber-AZ** vertreten²⁷⁸.*



Kommunales Dienstleistungszentrum Cybersicherheit (KDLZ-CS)

Das KDLZ-CS bietet zur Entwicklung und Stärkung kommunaler Cyberresilienz hessischen Kommunen kostenfreie individuelle Analysen ihres IT- und cybersicherheitsrelevanten Status quos sowie eine darauf aufbauende Entwicklung eines entsprechenden Maßnahmenplans. Dadurch soll das KDLZ-CS dazu beitragen, dass die hessischen Kommunen einen dem BSI IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ entsprechenden Sicherheitsstandard erreichen und umsetzen.

*Das KDLZ-CS ist ein kommunales Unterstützungsangebot seitens des **HMdIS**²⁷⁹.*



Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT)

Die Zentralstelle wurde als Außenstelle der Generalstaatsanwaltschaft Frankfurt (a.M.) in Gießen errichtet. Sie ist die operative Zentralstelle bei besonders aufwän-

²⁷⁸ [Hessischer Landtag \(Drucksache 20/8039\), Antwort auf Kleine Anfrage: Interkommunale Zusammenarbeit bei der Digitalisierung.](#)

[Hessisches Ministerium des Innern und für Sport, Cybersecurity: Hessen ist Partner im Nationalen Cyber-Abwehrzentrum.](#)

[Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.](#)

[Hessisches Ministerium des Innern und für Sport, Hessen3C.](#)

[Emailaustausch mit Vertreter:innen des Hessen Cyber Competence Center im November 2019.](#)

²⁷⁹ [Hessischer Landtag \(Drucksache 20/8039\), Antwort auf Kleine Anfrage: Interkommunale Zusammenarbeit bei der Digitalisierung.](#)

[Hessisches Ministerium des Innern und für Sport, Innenministerium erweitert Beratungsangebot für Kommunen.](#)



digen und umfangreichen Ermittlungsverfahren in den Bereichen, Kinderpornographie und sexuellem Missbrauch von Kindern mit Bezug zum Internet, Darknet-Kriminalität und anderer Cyberkriminalität.

Die ZIT ist erster Ansprechpartner des [BKA](#) für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland und bei Massenverfahren gegen mehrere Tatverdächtige deutschlandweit. Sie ist außerdem Gründungsmitglied im [EJCN](#)²⁸⁰.

²⁸⁰ [Staatsanwaltschaften Hessen, Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität \(ZIT\)](#).



Das Land Mecklenburg-Vorpommern zählt zu den Unterzeichnern des bundesländerübergreifenden Staatsvertrages, durch den **Dataport** eingerichtet wurde.

Überblick

- **Relevante Policy-Dokumente:**

- 2022: Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern (Errichtungsgesetz ZDMV – ZDMVG)
- 2016: Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern, EGovG M-V)
- 2014: Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Ministerium für Inneres, Bau und Digitalisierung (MIBD MV, Abteilung 2 Digitale Verwaltung, digitale Infrastruktur und Geoinformation). Für 2023 ist die Etablierung eines dem MIBD MV zugeordneten Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV) geplant, in dem Fähigkeiten gebündelt werden soll, wodurch u.a. auch die Cyber- und IT-Sicherheit des Landes verbessert werden soll²⁸¹.

*MIBD MV kooperiert mit dem **BSI** im Bereich der Cybersicherheit. Der:die Innenminister:in Mecklenburg-Vorpommerns nimmt an der **IMK** teil²⁸².*



- **Landes-CIO [MV]:** In Mecklenburg-Vorpommern ist die Position des:der CIO durch die:den Staatssekretär:in des **MIBD MV** besetzt.

*Er:sie vertritt Mecklenburg-Vorpommern im **IT-PLR** und gehört dem Verwaltungsrat von **Dataport** an²⁸³.*



- **Landes-CISO [MV]:** In Mecklenburg-Vorpommern ist der:die Beauftragte:r für Informationssicherheit (BeLVIS) im **MIBD MV** angesiedelt.

*Er:sie berichtet dem:der **Landes-CIO [MV]** und koordiniert das ressortübergreifende Informationssicherheitsmanagement. Dem:der BeLVIS untersteht das **CERT M-V** und er:sie vertritt Mecklenburg-Vorpommern unter anderem im **VCV**²⁸⁴.*

281 [Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern, Land will Digitalisierung und IT in neuem Landesamt zentralisieren.](#)

282 [Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern, Verstärkte Kooperation zwischen Bund und Land bei IT-Sicherheit. Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern, Organigramm.](#)

283 [Regierung Mecklenburg-Vorpommern, Staatssekretärin Ina-Maria Ulbrich.](#)

284 [DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, DVZ.info 02/14.](#)

[Ministerium für Inneres und Sport Mecklenburg-Vorpommern, Stellenausschreibung Beauftragte/Beauftragter der Landesverwaltung für Informationssicherheit.](#)



- **Behördlicher IT-Dienstleister:** DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ M-V).

*Dem:der Staatssekretär:in im **MIBD MV** kommt die Funktion des:der Aufsichtsratsvorsitzenden zu²⁸⁵.*



- **CERT:** Das CERT M-V ist im **MIBD MV** angesiedelt.



- **LfV [MV]:** In Mecklenburg-Vorpommern ist die Landesverfassungsschutzbehörde im **MIBD MV** angesiedelt (Abteilung 5). Unter das Arbeitsfeld Spionageabwehr und Wirtschaftsschutz fallen unter anderem Bedrohungen durch Cyberoperationen und Wirtschaftsspionage.

*Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das **BSI** unterstützt werden²⁸⁶.*



- **Institutionelle Ansässigkeit der ZAC [MV]:** Dezernat 45 Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern.

*Es nimmt Hinweise, die auf der Plattform **Netzverweis** eingehen, entgegen und geht ihnen nach. Es kooperiert außerdem mit der **Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock** und dem **BKA**²⁸⁷.*



- **Landesdatenschutzbehörde:** Landesbeauftragte:r für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI)²⁸⁸.

Weitere Akteure in Mecklenburg-Vorpommern:



Netzverweis.de

Der Internetauftritt netzverweis.de ist eine gemeinsame Initiative des Landeskriminalamtes Mecklenburg-Vorpommern und des DVZ M-V unter der Schirmherrschaft des MIE MV. Sie fungiert als Online-Meldestelle an die Bürger:innen, wenn gewünscht anonym, Hinweise zum Thema Internetkriminalität angeben können. Diese werden dann an das LKA Mecklenburg-Vorpommerns weitergeleitet und dort von Spezialisten:innen bearbeitet und verfolgt²⁸⁹.

²⁸⁵ [DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern, Über uns.](#)

²⁸⁶ [Verfassungsschutz Mecklenburg-Vorpommern, Spionageabwehr und Wirtschaftsschutz.](#)

²⁸⁷ [Landeskriminalamt Mecklenburg-Vorpommern, Cybercrime in M-V. Aktuelle Aspekte. \(Webseite entfernt\) Landespolizei Mecklenburg-Vorpommern, LKA-MV: Internationaler Ermittlungserfolg gegen Kinderpornografieplattform im Darknet.](#)

²⁸⁸ [Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Behörde.](#)

²⁸⁹ [Netzverweis, Online-Meldestelle. Regierung Mecklenburg-Vorpommern, Landesregierung.](#)



Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock

Mit landesweiter Zuständigkeit ist die Staatsanwaltschaft Rostock gleichzeitig Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität, d.h. sie deckt den Bereich Cybercrime ab²⁹⁰.



Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV)

Das Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV) ist eine obere Landesbehörde. Das Zentrum soll Expertise zu IT und Digitalisierung sowie zum operativen Informationssicherheits- und Datenschutzmanagement zentral in einem Landesamt bündeln und so die Landesbehörden von diesen Aufgaben entlasten. Dafür soll es zukünftig unter anderem die Bereitstellung von einheitlichen und standardisierten IT-Services garantieren.

*Das ZDMV operiert unter dem Dach des **MIBD MV** und wird von diesem sowie dem: der **Landes-CIO** gesteuert. Es arbeitet mit dem **DVZ M-V** zusammen. Das Zentrum soll außerdem das **CERT M-V** sowie Informationssicherheits- und Datenschutzbeauftragte für die Landesbehörden bereitstellen²⁹¹.*

²⁹⁰ [Justiz Online in Mecklenburg-Vorpommern, Zuständigkeit.](#)

²⁹¹ [Landtag Mecklenburg-Vorpommern, Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern.](#)
[Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern, Landtag gibt grünes Licht: Zentrum für Digitalisierung kann kommen.](#)



Das Land Niedersachsen ist im **NCSR** vertreten. Mit dem **BSI** hat es eine Kooperationsvereinbarung unterzeichnet. Es zählt zudem zu den Unterzeichnern des bundesländerübergreifenden Staatsvertrages, durch den **Dataport** eingerichtet wurde. Das niedersächsische Landeskriminalamt beteiligt sich an der **Sicherheitskooperation Cybercrime**.

Überblick

- **Relevante Policy-Dokumente:**

- 2019: Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Niedersächsisches Ministerium für Inneres und Sport (MI, Stabsstelle CIO und IT-Bevollmächtigter der Landesregierung, Referat IT2 Informationssicherheit, Cybersicherheit).

Das **BSI** und das **MI** arbeiten in Cybersicherheitsfragen zusammen. Es ist zudem Multiplikator der **ACS**²⁹².



- **Landes-CIO [NI]:** Der:die CIO Niedersachsens leitet die Stabsstelle „Informationstechnik der Landesverwaltung“ des **MI**. Neben der IT-Strategie und E-Government zählt auch die Verwaltungsmodernisierung zu den Aufgaben des:der CIO.

Er:sie vertritt Niedersachsen im **IT-PLR**²⁹³.



- **Landes-CISO [NI]:** Das Informationssicherheitsmanagement der Landesverwaltung in Niedersachsen verantwortet ein:e Informationssicherheitsbeauftragte:r (CISO), der:die im niedersächsischen **MI** angesiedelt ist²⁹⁴.



- **Behördlicher IT-Dienstleister:** IT.Niedersachsen (IT.N). IT.N betreibt unter anderem auch ein Cyber Defense Operations Center (CDOC)²⁹⁵.

292 [Niedersächsisches Ministerium für Inneres und Sport, Land und Bund vertiefen Zusammenarbeit gegen Cyberkriminalität.](#)

[Niedersächsisches Ministerium für Inneres und Sport, Organisationsplan.](#)

[Niedersächsisches Ministerium für Inneres und Sport, Sicherheit in der digitalen Welt.](#)

293 [Niedersächsisches Ministerium für Inneres und Sport, Neuer CIO in Niedersachsen: Dr. Horst Baier ist IT-Bevollmächtigter der Landesregierung.](#)

294 [Ministerium für Inneres und Sport Niedersachsen, Informationssicherheit.](#)

[Ministerium für Inneres und Sport, Informationssicherheit in Niedersachsen.](#)

295 [Landesbetrieb IT.Niedersachsen, Das Organigramm von IT.Niedersachsen.](#)



- **CERT:** Das N-CERT ist beim MI angegliedert. Kürzlich wurde das N-CERT zu einem Cyber-Defense-Center erweitert, um unter anderem ein „umfassendes Echtzeit-lagebild der Cybersicherheit“ zu erstellen. Mehr als 100 niedersächsische Kommunen greifen auf Unterstützungsleistungen des N-CERT zurück²⁹⁶.



- **LFV [NI]:** Die niedersächsische Landesverfassungsschutzbehörde (Abteilung 5), angesiedelt im dortigen MI, befasst sich unter anderem mit den Arbeitsbereichen Wirtschaftsschutz sowie der Cyberabwehr (Referat 55). Ersterer steht Unternehmen als unterstützender Ansprechpartner in Bezug auf die Prävention von Wirtschaftsspionage zur Verfügung und in letzterem werden unter anderem „Daten im Kontext von IT-gestützten Spionage- und Sabotageoperationen fremder Nachrichtendienste erhoben, gesammelt, analysiert und bewertet“.

Sofern erforderlich, können die LFV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden²⁹⁷.



- **Institutionelle Ansässigkeit der ZAC [NI]:** Landeskriminalamt Niedersachsen. Das niedersächsische Landeskriminalamt stellt zudem einen Ratgeber Internetkriminalität zur Verfügung. Die niedersächsische ZAC wird durch 12 Taskforces Cybercrime/Digitale Spuren (TF CC/DS) in lokalen Polizeibehörden unterstützt²⁹⁸.



- **Landesdatenschutzbehörde:** Landesbeauftragte:r für den Datenschutz Niedersachsen (LfD)²⁹⁹.

Weitere Akteure in Niedersachsen:



Cybersicherheitsbündnis

Land und Kommunen haben zur Verbesserung der Informationssicherheit und verstärkten Zusammenarbeit ein Cybersicherheitsbündnis geschlossen. Im Rahmen dieses Bündnisses sollen Beziehungen institutionalisiert und gemeinsame Maßnahmen zur Erhöhung des IT-Sicherheitsniveaus vereinbart und umgesetzt werden.

²⁹⁶ Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV). (Webseite entfernt)

[Niedersächsisches Ministerium für Inneres und Sport, Praxisbeispiel Digitalisierung: Ausbau des N-CERT zum Cyber-Defense-Center \(CDC\).](#)

[Niedersächsisches Ministerium für Inneres und Sport, 100. Kommune nutzt N-CERT-Angebot des Innenministeriums zur Abwehr von Cyberangriffen.](#)

[Niedersächsische Ministerium für Inneres und Sport, Niedersachsen-CERT.](#)

²⁹⁷ [Ministerium für Inneres und Sport Niedersachsen, Die Cyberabwehr beim Verfassungsschutz Niedersachsen.](#)

[Ministerium für Inneres und Sport Niedersachsen, Organisationsplan des Niedersächsischen Ministeriums für Inneres und Sport.](#)

²⁹⁸ [Landeskriminalamt Niedersachsen, Ratgeber Internetkriminalität.](#)

[Landeskriminalamt Niedersachsen, Zentrale Ansprechstelle Cybercrime \(ZAC\).](#)

[Niedersächsischer Landtag, Kleine Anfrage zur schriftlichen Beantwortung mit Antwort der Landesregierung: Wie sicher ist die IT der Ministerien und von Landeseinrichtungen?.](#)

²⁹⁹ [Die Landesbeauftragte für den Datenschutz Niedersachsen, Die Behörde.](#)



*Kommunen sollen darüber hinaus Leistungen des **N-CERT** in Anspruch nehmen können³⁰⁰.*



Digitalagentur Niedersachsen

Als „One-Stop-Shop“ unterstützt die Digitalagentur Niedersachsen „die niedersächsische Wirtschaft bei der Entwicklung von Innovationen um damit Arbeitsplätze zu schaffen und zu sichern“. Ihr Arbeitskreis IT-Sicherheit stellt unter anderem für diese eine zentrale Informationsstelle zur Verfügung, in der beispielsweise Infos zu Anlaufstellen, Beratungs- und Unterstützungsangeboten oder der allgemeinen Gefährdungslage aufbereitet werden.

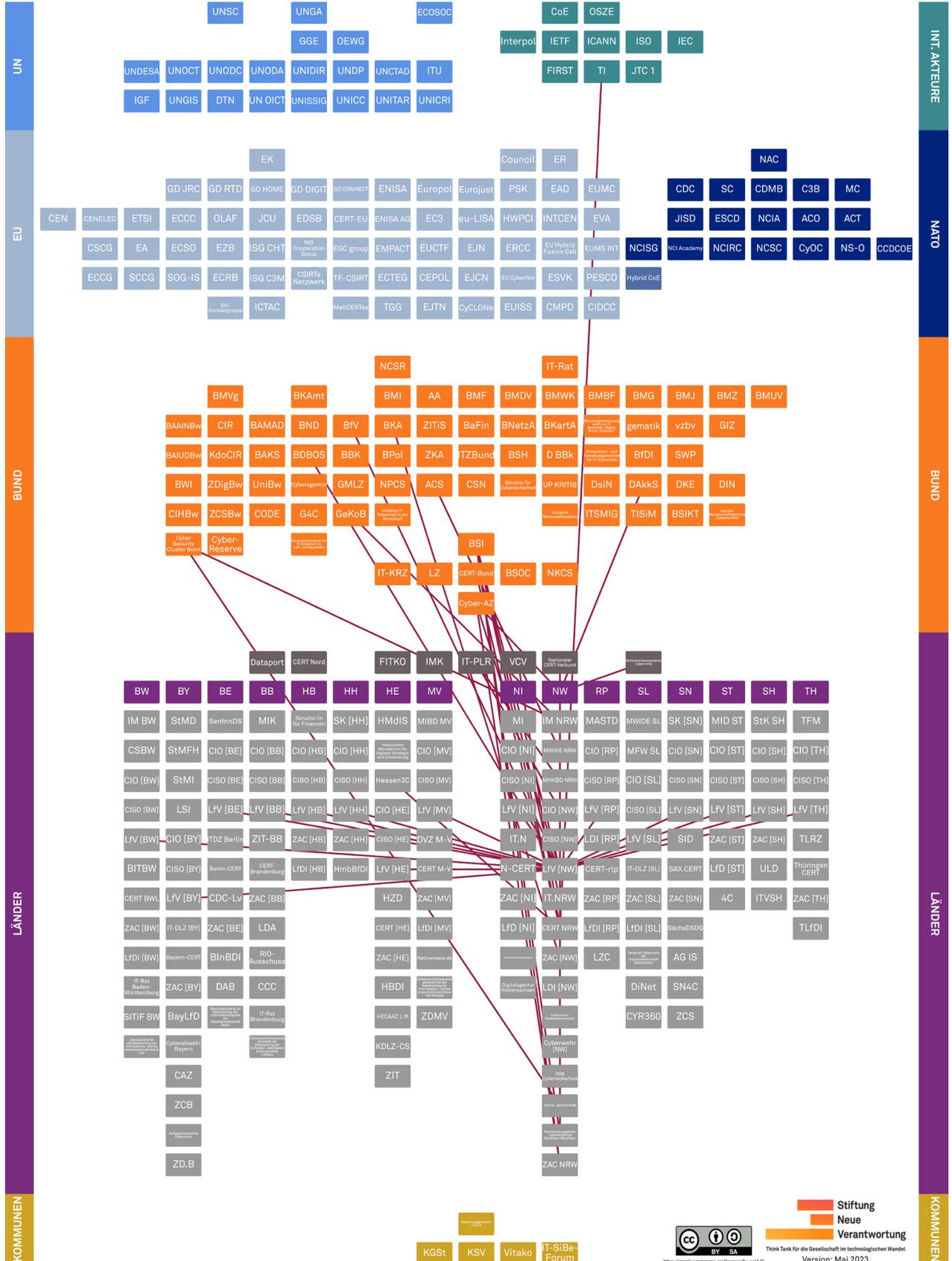
Die Digitalagentur Niedersachsen wird durch das Niedersächsische Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung (MW) getragen³⁰¹.

³⁰⁰ [Niedersächsisches Ministerium des Innern und für Sport, Sicherheit in der digitalen Welt.](#)

³⁰¹ [Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Digitalagentur Niedersachsen.](#)
[Digitalagentur Niedersachsen, IT-Sicherheit für Niedersachsen.](#)
[Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung, Digitalagentur und weitere Angebote zur Unterstützung.](#)



9.10 Nordrhein-Westfalen (NW)





Das Land Nordrhein-Westfalen ist durch seine Kölner Schwerpunktstaatsanwaltschaft Cyber als Partner im **Cyber-AZ** vertreten. Es ist zudem einer der Gesellschafter der **DAkKS**. Das nordrhein-westfälische Landeskriminalamt beteiligt sich an der **Sicherheitskooperation Cybercrime**.

Überblick

- **Relevante Policy-Dokumente:**

- 2021: Cybersicherheitsstrategie des Landes Nordrhein-Westfalen
- 2016: Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (E-Government-Gesetz Nordrhein-Westfalen, EGovG NRW)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:**

- Ministerium des Innern des Landes Nordrhein-Westfalen (IM NRW, Abteilung 3: Gefahrenabwehr, Vermessung Referat 32: Staatliche Krisenvorsorge, Krisenmanagement der Landesregierung, Schutz Kritischer Infrastruktur, Zivile Verteidigung; Abteilung 7: Digitalisierung im IM und im Geschäftsbereich, Referat 73: Koordinierungsstelle für Cybersicherheit NRW, Informationssicherheit im IM und Geschäftsbereich).

*Der/die nordrhein-westfälische Innenminister:in nimmt an der **IMK** teil. Das IM NRW ist im Beirat des **Cyber Security Cluster Bonn** vertreten³⁰².*

- Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen (MHKBD NRW, Abteilung 2: Digitalisierung der Landesverwaltung, Referat 224: Informationssicherheit in der Landesverwaltung).³⁰³
- Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (MWIKE NRW, Abteilung 1: Zentralabteilung, Referat 115: IT, Informationssicherheit, Open.NRW; Abteilung 4: Innovation und Märkte, Referat 414: IKT, Mobilfunk und Cybersicherheit in der Wirtschaft, sowie Abteilung 8: Digitalisierung, Startups und Dienstleistungen, Referat 811: digitale Kompetenzen).

*Das MWIKE NRW ist Teilnehmer der **ACS**. Die **Cyberwehr [NW]** greift auf Fördermittel des MWIKE NRW (Regio Call EFRE.NRW) zurück³⁰⁴.*

³⁰² [Ministerium des Innern des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.](#)

³⁰³ [Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.](#)

³⁰⁴ [Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.](#)



- **Landes-CIO [NW]:** Der:die CIO Nordrhein-Westfalens ist im **MHKBD NRW** als Landesbeauftragte:r für Informationstechnik angesiedelt.

*Er:sie vertritt Nordrhein-Westfalen im **IT-PLR**³⁰⁵.*



- **Landes-CISO [NW]:** Der Posten der:des Informationssicherheitsbeauftragten des Landes Nordrhein-Westfalen fällt dem:der Leiter:in des Referates 224 (Informationssicherheit in der Landesverwaltung) innerhalb des **MHKBD NRW** zu³⁰⁶.



- **Behördlicher IT-Dienstleister:** Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW) im Geschäftsbereich des **MHKBD NRW**.

***BSI** und **IT.NRW** arbeiten zusammen³⁰⁷.*



- **CERT:** Das CERT NRW wird vom **IT.NRW** betrieben. Über das CERT NRW betreibt der IT.NRW einen Kommunalen Warn- und Informationsdienst (KWID), der Kommunen in NRW zur Verfügung steht.

*Es beteiligt sich am **Nationalen CERT-Verbund** und **TI**³⁰⁸.*



- **LfV [NW]:** Das **IM NRW** beherbergt die Verfassungsschutzbehörde des Landes. Dort (Abteilung 6: Gruppe 61 Prävention, Cyberanalysen, Spionageabwehr, ND-IT, Ermittlung) befinden sich Zuständigkeiten für Wirtschaftsschutz (Referat 611), Spionage- und Cyberabwehr (Referat 613) sowie ein IT- und Cyberkompetenzzentrum im Verfassungsschutz (Referat 615).

*Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das **BSI** unterstützt werden³⁰⁹.*

305 [Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.](#)

306 [Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.](#)

307 [Landesbetrieb Information und Technik Nordrhein-Westfalen, Aufbau und Geschäftsverteilung, Landtag Nordrhein-Westfalen, Stellungnahme des Vizepräsidenten des Bundesamtes für Sicherheit in der Informationstechnik \(BSI\), Herr Dr. Gerhard Schabhüser zu den Anträgen der Fraktion der AfD \(17/4803\) „Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern“ und der Fraktion Bündnis 90/DIE GRÜNEN \(17/5056\) „IT-Sicherheit in NRW stärken – Freiheit sichern“ im Rahmen der Anhörung „Lehren aus dem Hackerangriff ziehen – IT-Sicherheit in NRW verbessern“ des Ausschusses für Digitalisierung und Innovation des Landtags Nordrhein-Westfalen am 16. Mai 2019.](#)

308 [Information und Technik Nordrhein-Westfalen, Informationssicherheit für die Landesverwaltung NRW, Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie Nordrhein-Westfalen, Nordrhein-Westfalen stärkt Cybersicherheit in den Kommunen mit neuem Warn- und Informationsdienst.](#)

309 [Ministerium des Innern Nordrhein-Westfalen, Organisationsplan.](#)



- **Institutionelle Ansässigkeit der ZAC [NW]:** Cybercrime-Kompetenzzentrum, Akteursbeschreibung s. unten.



- **Landesdatenschutzbehörde:** Landesbeauftragte:r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI)³¹⁰.

Weitere Akteure in Nordrhein-Westfalen:



Cybercrime-Kompetenzzentrum

Das im Landeskriminalamt Nordrhein-Westfalen eingerichtete Cybercrime-Kompetenzzentrum beherbergt Ermittlungskommissionen für herausragende Verfahren sowie Expert:innen für Computerforensik, Telekommunikationsüberwachung, Auswertung, Analyse und Prävention. Zudem sind dort ein Zentrales Informations- und Servicezentrum Cybercrime (ZISC), ein Cyber-Recherche- und Fahndungszentrum (CRuFz), die TKÜ-Dienststelle sowie die Zentrale Auswertungs- und Sammelstelle Kinderpornografie (ZASt) angesiedelt. Jährlich wird ein Lagebild Cybercrime veröffentlicht.

*Das ZISC beheimatet **ZAC [NW]** für die Wirtschaft³¹¹.*



Cyberwehr (Cyberwehr [NW])

Die Cyberwehr steht als Pilotprojekt KMU in den Städten Bochum, Essen und Gelsenkirchen als Ansprechpartner zur Verfügung. Diese können die Cyberwehr in Notfällen kostenfrei telefonisch kontaktieren. Nach telefonischer Erst-Bestandsaufnahme und je nach Umfang des Vorfalls kann eine Beauftragung eines Cyberwehr-Partners erfolgen, welcher entweder vor Ort oder remote kostenlos „Erste Hilfe“, beispielsweise durch Bestandsaufnahme oder Aussprache von Handlungsempfehlungen, leisten kann. Weitergehender System-Wiederaufbau oder andere Dienstleistungen durch diese oder andere Firmen bleiben dabei für die KMU weiterhin kostenpflichtig. Perspektivisch soll das Pilotprojekt auf ganz Nordrhein-Westfalen ausgeweitet werden.

*Die Cyberwehr greift auf Fördermittel des **MWIKÉ NRW** (Regio Call EFRE.NRW) zurück³¹².*



Interministerieller Ausschuss Cybersicherheit (IMA Cybersicherheit)

Innerhalb des interministeriellen Ausschusses wird sich zu Themen der Cybersicherheit ausgetauscht und Maßnahmen für eine erhöhte Cybersicherheit in Nord-

³¹⁰ [Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Über uns.](#)

³¹¹ [Polizei Nordrhein-Westfalen, Das Cybercrime-Kompetenzzentrum beim LKA NRW.](#)
[Polizei Nordrhein-Westfalen, Lagebild Cybercrime.](#)

³¹² [Cyberwehr, Über Uns.](#)
[eurobits, Pilotprojekt für das Ruhrgebiet: eurobits baut Cyberwehr für den Mittelstand auf.](#)



rhein-Westfalen abgestimmt. Der IMA Cybersicherheit war auch an der Erarbeitung der nordrhein-westfälischen Cybersicherheitsstrategie und dem Landesbericht zur Cybersicherheit beteiligt.

In dem IMA Cybersicherheit sind alle Ressorts der nordrhein-westfälischen Landesregierung, inkl. IM NRW und MWIKE NRW unter Vorsitz der Koordinierungsstelle Cybersicherheit NRW vertreten³¹³.



Kompetenzzentrum für Cybersicherheit in der Wirtschaft (DIGITAL.SICHER.NRW)

Mit Geschäftsstellen in Bonn und Bochum wurde Anfang 2021 das Kompetenzzentrum für Cybersicherheit in der Wirtschaft „DIGITAL.SICHER.NRW“ etabliert. Es soll KMU in NRW in IT- und Cybersicherheitsfragen, beispielsweise durch Bereitstellung von Informationen, als Kontaktstelle oder bei der „Bedarfsermittlung für grundlegenden IT-Schutz“ unterstützen. Zudem sollen Veranstaltungen ausgerichtet und ein Netzwerk von mit Cybersicherheit betrauten Verantwortlichen in der Wirtschaft aufgebaut werden. Angebote des Kompetenzzentrums sind für KMU kostenfrei.

Unter DIGITAL.SICHER.NRW's Partnern ist das MWIKE NRW und das Cyber Security Cluster Bonn³¹⁴.



Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen

Die Koordinierungsstelle Cybersicherheit in Nordrhein-Westfalen hat es sich zur Aufgabe gemacht, zu Transparenz für Bürgerinnen und Bürger, Unternehmen und Kritische Infrastrukturen beizutragen, Informationen zur Cybersicherheit des Bundeslandes für die Landesverwaltung zu bündeln, Vorgänge zwischen Bund und Land sowie in länderübergreifenden Gremien zu koordinieren und effektive Synergien im Land durch Vernetzung und Zusammenarbeit unter anderem mit dem Verfassungsschutz oder dem Cybercrime-Kompetenzzentrum herzustellen. Die Koordinierungsstelle legt dem Landeskabinett jährlich einen Bericht zur Cybersicherheit in NRW vor.

Der IMA Cybersicherheit kommt unter Vorsitz der Koordinierungsstelle zusammen. Die Koordinierungsstelle Cybersicherheit NRW ist im Geschäftsbereich des IM NRW angesiedelt und als zentrale Kontaktstelle des Landes gegenüber dem BSI designiert³¹⁵.

³¹³ [Ministerium des Innern des Landes Nordrhein-Westfalen, Bericht zur Cybersicherheit in Nordrhein-Westfalen. Ministerium des Innern des Landes Nordrhein-Westfalen, Cybersicherheitsstrategie des Landes Nordrhein-Westfalen.](#)

³¹⁴ [DIGITAL.SICHER.NRW, Die Partner des Kompetenzzentrums. Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, DIGITAL.SICHER.NRW: Land startet Kompetenzzentrum für Cybersicherheit in der Wirtschaft.](#)

³¹⁵ [Behörden Spiegel, Neue Koordinierungsstelle für Cyber-Sicherheit in NRW. \(Webseite entfernt\) Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen, Über Uns. Ministerium des Inneren des Landes Nordrhein-Westfalen, Kabinett beschließt Einrichtung von Koordinierungsstelle für Cybersicherheit.](#)



Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)

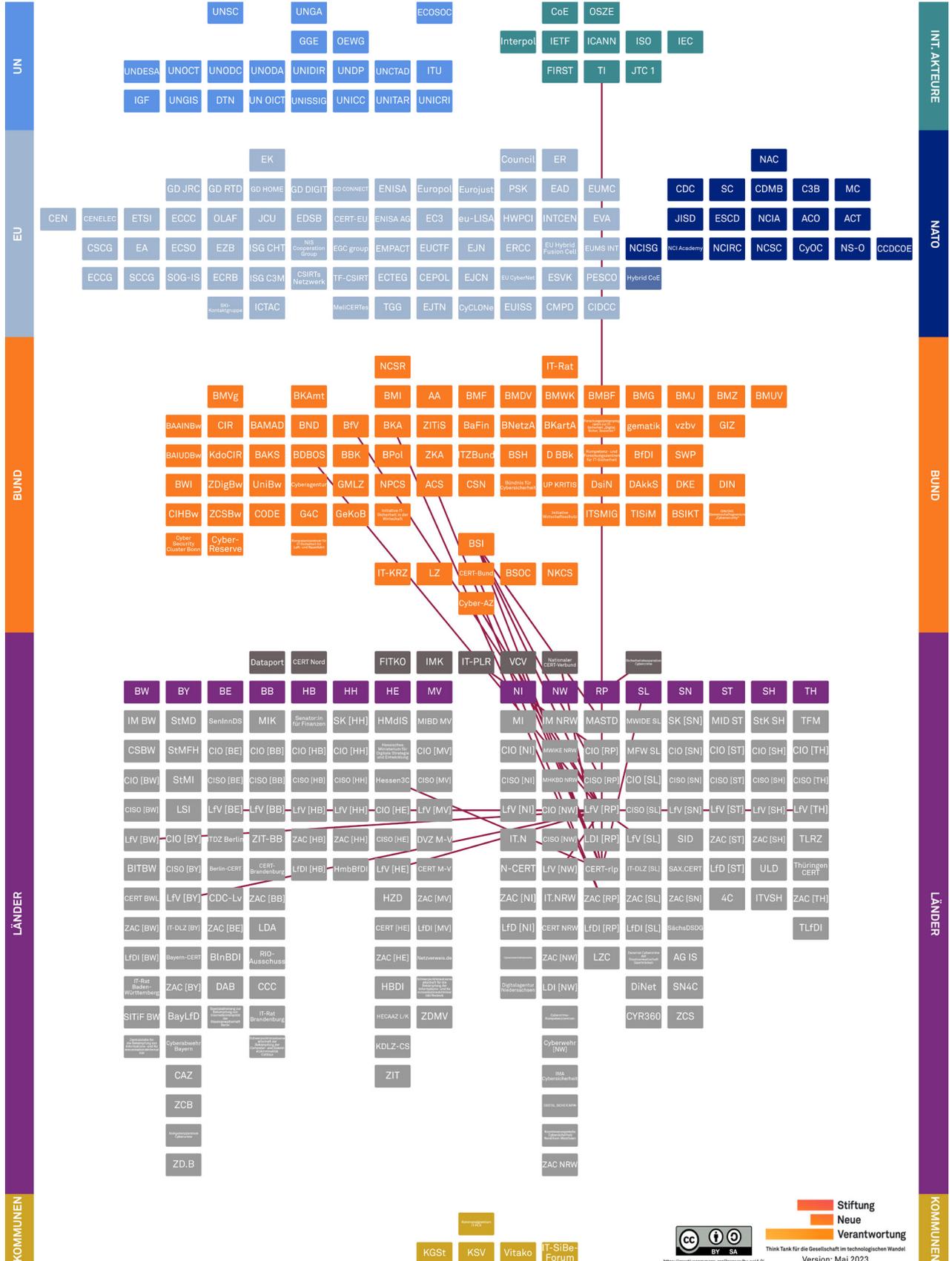
Die Zentral- und Ansprechstelle Cybercrime in NRW (nicht zu verwechseln mit der nordrhein-westfälischen Zentralen Ansprechstelle Cybercrime der Polizei für Wirtschaftsunternehmen, in der Grafik als ZACs, die im Cybercrime-Kompetenzzentrum des nordrhein-westfälischen Landeskriminalamts angesiedelt ist) ist bei der Staatsanwaltschaft Köln die landesweit zuständige justizielle Cybercrime-Einheit. Sie ist bundesweit die größte Cybercrime-Einheit der Justiz, ihr obliegt die Verfahrensführung in herausgehobenen Ermittlungsverfahren der Cyberkriminalität, die Wahrnehmung der Aufgaben einer Ansprechstelle für Cyberkriminalität und die Mitwirkung an Aus- und Fortbildungsmaßnahmen im regionalen und überregionalen Kontext.

Die ZAC NRW steht in engem Austausch mit anderen Zentralstellen für Cybercrime der Bundesländer, den Polizeibehörden, Wirtschaftsunternehmen und dem [BSI](#)³¹⁶.

³¹⁶ [Justiz-ONLINE, Zentral- und Ansprechstelle Cybercrime \(ZAC NRW\)](#).



9.11 Rheinland-Pfalz (RP)





Das rheinland-pfälzische Landeskriminalamt beteiligt sich an der *Sicherheitskooperation Cybercrime*.

Überblick

- **Relevante Policy-Dokumente:**

- 2020: Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (E-Government-Gesetz Rheinland-Pfalz, EGovGRP)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Im Mai 2021 ist die Federführung vom rheinland-pfälzischen Innenministerium an das Ministerium für Arbeit, Soziales, Transformation und Digitalisierung (MASTD, Abteilung 63: Digitalisierung, Referat 633 Ressortübergreifende Informationssicherheit) übergegangen.

*In der Vergangenheit hatten das rheinland-pfälzische Innenministerium und das **BSI** eine Kooperationsvereinbarung zur Zusammenarbeit in Cybersicherheitsfragen unterzeichnet³¹⁷.*



- **Landes-CIO [RP]:** Der:die CIO Rheinland-Pfalz ist unter anderem verantwortlich für die „IT-Infrastrukturen, die IT-Basis- und -Querschnittsdienste der Landesverwaltung sowie die Standardisierungsagenda und koordiniert den IT-Einsatz ressortübergreifend“. Er:sie übernimmt zudem auch die Funktion des:der Chief Digital Officer (CDO).

*Er:sie ist gleichzeitig Staatssekretär:in im **MASTD** und vertritt das Land Rheinland-Pfalz im **IT-PLR**³¹⁸.*



- **Landes-CISO [RP]:** In Rheinland-Pfalz ist der:die Informationssicherheitsbeauftragte:r der Landesverwaltung (CISO-rlp) in Referat 632 der Abteilung 63 des **MASTD** beheimatet.

*Enger Austausch besteht mit dem **BSI**, **CERT-rlp** sowie den Sicherheitsbehörden des Landes³¹⁹.*

³¹⁷ [Ministerium des Innern und für Sport, Kooperationsvereinbarung zur Cybersicherheit abgeschlossen. Ministerium für Arbeit, Soziales, Transformation und Digitalisierung Rheinland-Pfalz, Organigramm.](#)

³¹⁸ [Ministerium des Innern und für Sport Rheinland-Pfalz, Digitale Verwaltung Rheinland-Pfalz. Ministerium für Arbeit, Soziales, Transformation und Digitalisierung, Fedor Ruhose ist neuer Beauftragter der Landesregierung für Informationstechnik und Digitalisierung.](#)

³¹⁹ [Ministerium der Justiz Rheinland-Pfalz, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Rheinland-Pfalz.](#)



- **Behördlicher IT-Dienstleister:** Landesbetrieb Daten und Information (LDI). Die Dienst- und Fachaufsicht obliegt dem rheinland-pfälzischen Ministerium des Innern und für Sport³²⁰.



- **CERT:** Das CERT-rlp gehört zum **LDI**.

*Auf Basis einer Vereinbarung zwischen dem Saarland und Rheinland-Pfalz wird das saarländische (SL) CERT vom CERT-rlp bereitgestellt. Es beteiligt sich am **Nationalen CERT-Verbund** und **TJ**³²¹.*



- **LfV [RP]:** In Rheinland-Pfalz ist die Landesverfassungsschutzbehörde im Ministerium des Innern und für Sport des Landes institutionell angesiedelt. Unter ihre Aufgabenbereiche fallen unter anderem Spionage, Cyberabwehr sowie Wirtschaftsschutz.

*Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das **BSI** unterstützt werden³²².*



- **Institutionelle Ansässigkeit der ZAC [RP]:** Dezernat 47 Cybercrime des Landeskriminalamtes Rheinland-Pfalz. Dieses nimmt eine Zentralstellenfunktion ein und unterstützt die örtlichen Dienststellen. Es übernimmt außerdem herausragende Ermittlungsverfahren der Cyberkriminalität, vor allem Pilot- und Mehrwertverfahren, Verfahren mit besonderer Öffentlichkeitswirkung und Verfahren, „durch die technisches und/oder ermittlungstaktisches Neuland betreten wird sowie Verfahren aus dem Bereich der internationalen, bandenmäßigen oder organisierten Kriminalität“.

*Das LKA Rheinland-Pfalz ist Mitglied der **ACS**³²³.*



- **Landesdatenschutzbehörde:** Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI)³²⁴.

³²⁰ [Landesbetrieb Daten und Information, Der LDI: Der IT-Dienstleister der Landesverwaltung Rheinland-Pfalz. Landesbetrieb Daten und Information, Impressum.](#)

³²¹ [Ministerium des Innern und für Sport Rheinland-Pfalz, CERT-rlp.](#)

³²² [Ministerium des Innern und für Sport Rheinland-Pfalz, Spionageabwehr, Wirtschaftsschutz und Cybersicherheit.](#)

³²³ [Polizei Rheinland-Pfalz, Aufgaben des Dezernates Cybercrime.](#)

³²⁴ [Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Über uns.](#)



Weitere Akteure in Rheinland-Pfalz:



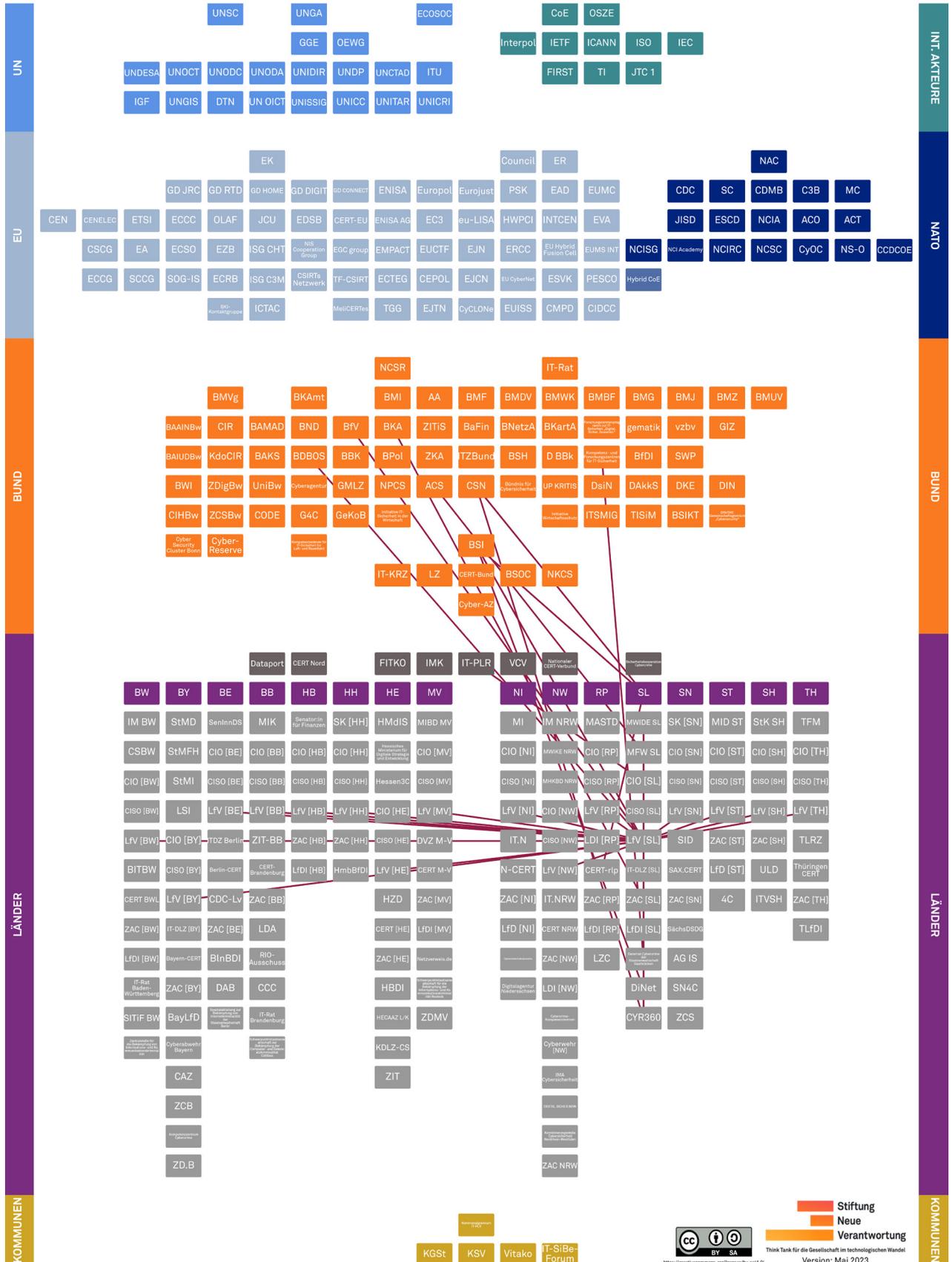
Landeszentralstelle Cybercrime (LZC)

Bei der Generalstaatsanwaltschaft Koblenz befindet sich die Landeszentralstelle Cybercrime, die Koordinierungs-, Unterstützungs- und Ermittlungsaufgaben für das gesamte Land übernimmt. Zu diesen zählen unter anderem die Mitarbeit in Gremien von Bund und Land, die Leitung der landesweiten Arbeitsgruppe Cybercrime unter Beteiligung aller Landesstaatsanwaltschaften sowie die Ermittlung in „Verfahren von besonderer Bedeutung, besonderer Schwierigkeit und/oder besonderen Umfang“. Unter letztere fallen beispielsweise öffentlichkeitswirksame Ermittlungsverfahren oder solche, die in engem Zusammenhang zur organisierten Kriminalität stehen³²⁵.

³²⁵ [Generalstaatsanwaltschaft Koblenz, Landeszentralstelle Cybercrime \(LZC\)](#).



9.12 Saarland (SL)





Das Saarland hat mit dem [BSI](#) eine rechtlich verbindliche Kooperationsvereinbarung zur verstärkten Zusammenarbeit geschlossen. Darüber hinaus ist das Land eine Pilotregion des [CSN](#).

Überblick

- **Relevante Policy-Dokumente:**

- 2019: Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland, IT-SiG SL)
- 2017: Gesetz zur Förderung der elektronischen Verwaltung im Saarland (E-Government-Gesetz Saarland, E-GovG SL)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:**

- Ministerium für Wirtschaft, Innovation, Digitales und Energie (MWIDE SL, Abteilung D: Digitalisierung in Wirtschaft und Verwaltung, Referat D/6 Informationssicherheits- und Datenschutzmanagement, IT-Recht).

Das MWIDE beheimatet die [DiNet](#) sowie [CYBR360](#)³²⁶.

- Ministerium der Finanzen und für Wissenschaft (MFW SL, Stabsstelle Informationssicherheitsmanagement und IT-Recht).

Das MFWv beteiligt sich als Multiplikator an der [ACS](#)³²⁷.



- **Landes-CIO [SL]:** Der:die saarländische CIO ist ein:e Staatssekretär:in des [MWIDE SL](#).

Er:sie vertritt das Saarland im [IT-PLR](#)³²⁸.



- **Landes-CISO [SL]:** Auch der:die CISO des Saarlandes ist im [MWIDE SL](#) angesiedelt.

Er:sie verfügt über ein direktes Vortragsrecht gegenüber dem:der Landes-CIO [SL], berichtet zu Risiken und Stand der Umsetzung von IT-Sicherheitsmaßnahmen und kann ggf. Maßnahmen zur Eindämmung ersterer empfehlen³²⁹.

³²⁶ [Ministerium für Wirtschaft, Innovation, Digitales und Energie Saarland, Organigramm des Ministeriums für Wirtschaft, Innovation, Digitales und Energie.](#)

³²⁷ [Ministerium der Finanzen und für Wissenschaft, Organigramm.](#)

³²⁸ [Ministerium für Wirtschaft, Innovation, Digitales und Energie, Staatssekretärin und CIO Elena Yorgova-Ramanaukas.](#)

³²⁹ [Ministerium für Finanzen und Europa Saarland, Stabsstelle Informationssicherheit und IT-Recht.](#)



- **Behördlicher IT-Dienstleister:** Landesamt für IT-Dienstleistungen (IT-DLZ), welches dem saarländischen MFW SL nachgeordnet ist³³⁰.



- **CERT:** Das CERT Saarland wird durch eine Vereinbarung zwischen dem Saarland und Rheinland-Pfalz vom CERT-rlp bereitgestellt³³¹.



- **LfV [SL]:** Das Ministerium für Inneres, Bauen und Sport des Saarlandes beherbergt die dortige Landesverfassungsschutzbehörde. Dort wird unter anderem zur Spionageabwehr und Wirtschaftsschutz gearbeitet. Der letzte saarländische Verfassungsschutzbericht verweist auf Gefahren durch Cyber- und elektronische Operationen.

Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden³³².



- **Institutionelle Ansässigkeit der ZAC [SL]:** Dezernat Cybercrime der saarländischen Kriminalpolizei. Dieses setzt sich mit besonders schwerwiegenden Fällen auseinander, insbesondere wenn der öffentliche Bereich betroffen, ein sehr hoher Schaden entstanden oder die technischen Anforderungen hoch sind³³³.



- **Landesdatenschutzbehörde:** Unabhängiges Datenschutzzentrum Saarland mit Landesbeauftragter:m für Datenschutz und Informationsfreiheit (LfDI)³³⁴.

Weitere Akteure im Saarland:



Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken

Mit dem bei der Staatsanwaltschaft Saarbrücken angesiedelten Sonderdezernat „Cybercrime“ möchte das saarländische Justizministerium der Kriminalität im Netz entgentreten.

Das Dezernat soll mit dem Institut für Rechtsinformatik und dem CISPA Helmholtz Center for Information Security speziell geschult werden³³⁵.

³³⁰ [Ministerium für Finanzen und Europa Saarland, Themen & Aufgaben.](#)

³³¹ [Kommune 21, CERT für saarländische Kommunen.](#)

³³² [Ministerium des Innern, Bauen und Sport Saarland, Lagebild Verfassungsschutz 2019.](#)

³³³ [sol.de, Saar-Kripo eröffnet neue „Cybercrime“-Dienststelle. \(Website entfernt\)](#)

³³⁴ [Unabhängiges Datenschutzzentrum Saarland, Über Uns.](#)

³³⁵ [Juristisches Internetprojekt Saarbrücken, Neues Dezernat „Cybercrime“ bei der Staatsanwaltschaft Saarbrücken.](#)



Netzwerkstelle Digitalisierung (DiNet)

Die Netzwerkstelle Digitalisierung (DiNet) soll vor allem Unternehmen aus dem saarländischen Mittelstand Unterstützung bei der digitalen Transformation zukommen lassen – und beispielsweise Themen wie die Digitalisierung der Arbeitswelt und Cybersicherheit in den Fokus nehmen. Über das regionale Netzwerk Digitalisierung sollen relevante Akteure miteinander in Kontakt gebracht werden, außerdem sollen unter anderem Innovations-Netzwerke geschaffen und Wissensaustausch gestärkt werden. Dabei gilt der Fokus nicht nur Akteuren aus der Wirtschaft, sondern auch der Vernetzung mit Wissenschaft und Politik. Konkret sollen über das Förderprogramm Digitalstarter Saarland kleine und mittlere Unternehmen dabei unterstützt werden, sich den durch die Digitalisierung entstandenen Anforderungen anzupassen.

*Das DiNet ist Teil des **MWIDE SL** und ist Initiator von **CYBR360**³³⁶.*



Initiative für Cybersicherheit (CYBR360)

CYBR360 ist eine Initiative zur Stärkung der Cybersicherheit kleiner und mittlerer Unternehmen im Saarland. Mit der „Digitalen Rettungskette“ stellt die CYBR360 als akute Reaktion auf IT-Sicherheitsvorfälle eine Anlaufstelle für kleine und mittlere Unternehmen zur Verfügung. Mit Unterstützung des CSN sollen hier, neben erster operativer Unterstützung, früh die, je nach Situation angepassten, technischen und institutionellen Reaktionen, wie Anzeigen und Meldungen eingeleitet werden. Die CYBR360 bündelt Expertise aus Forschung, Beratung und Anwendung und umfasst neben einer Netzwerkplattform verschiedene Formate zur Weiterbildung und Prävention.

*CYBR 360 wurde als Initiative für digitale Sicherheit von der **DiNet** ins Leben gerufen und ist dem **MWIDE SL** angegliedert. Im Rahmen der saarländischen **CSN-Pilotregion** arbeitet es eng mit dem **BSI** und dem **ZAC [SL]** zusammen³³⁷.*

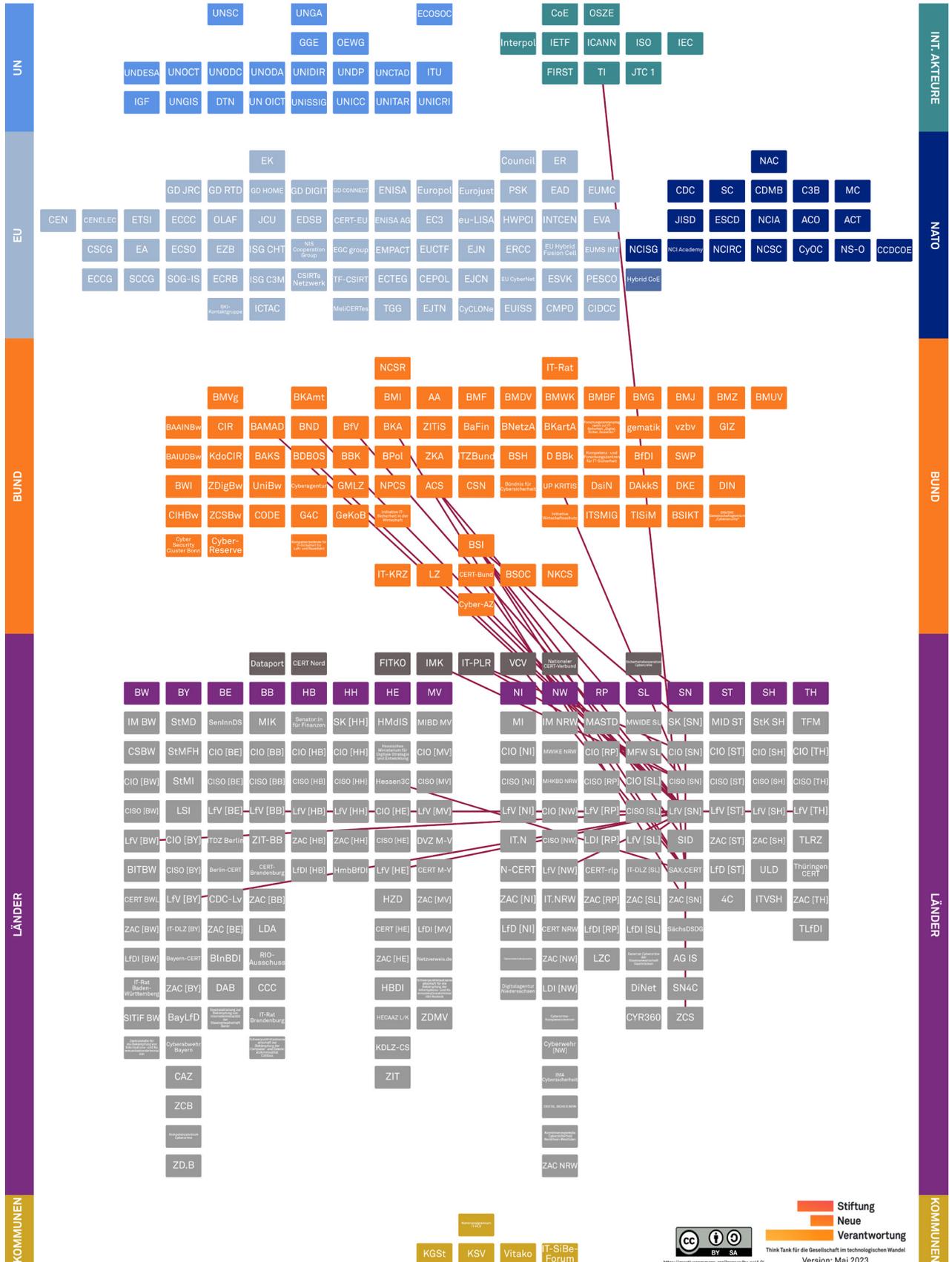
³³⁶ [Ministerium für Wirtschaft, Innovation, Digitales und Energie SL, DiNet.](#)

³³⁷ [CYBR360 Saarland, die Initiative für Cybersicherheit.](#)

[Saarland.innovation&standort, Neu: CYBR360 – Das Netzwerk für digitale Sicherheit im Saarland.](#)



9.13 Sachsen (SN)





Das sächsische Landeskriminalamt beteiligt sich an der *Sicherheitskooperation Cybercrime*.

Überblick

- **Relevante Policy-Dokumente:**

- 2019: Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz – SächsISichG)
- 2019: Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz, SächsEGovG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Sächsische Staatskanzlei (SK [SN], Abteilung 4 Digitale Verwaltung, Referat 45 Informations- und Cybersicherheit, Kritische Infrastrukturen).

Die SK [SN] und das *BSI* haben eine Zusammenarbeit im Bereich der Cybersicherheit vereinbart³³⁸.



- **Landes-CIO [SN]:** Sachsens CIO ist aktuell der:die Amtschef:in der SK [SN], der:die für die Stabsstelle „Landesweite Organisationsplanung, Personalstrategie und Verwaltungsmodernisierung“ zuständig ist.

Er:sie vertritt Sachsen im *IT-PLR*³³⁹.



- **Landes-CISO [SN]:** Der:die sächsische Beauftragte:r für Informationssicherheit des Landes (BfIS) ist zeitgleich Leiter:in des Referats 45 in der SK [SN], das sich mit Informations- und Cybersicherheit sowie kritischen Infrastrukturen befasst.

Er:sie wird durch den:die *Landes-CIO [SN]* benannt und verfügt über ein unmittelbares Vorspracherecht. Er:sie ist Mitglied in der AG Informationssicherheit des *IT-PLR*, einer Länderarbeitsgruppe der *IMK* sowie der *ACS* und *UP KRITIS*³⁴⁰.



- **Behördlicher IT-Dienstleister:** Staatsbetrieb Sächsische Informatik Dienste (SID), der der SK nachgeordnet ist.

Der SID ist Teilnehmer der *ACS*³⁴¹.

³³⁸ [Sächsische Staatskanzlei, Organisation.](#)

[Sächsische Staatskanzlei, Sachsen und Bund kooperieren bei Cyber-Sicherheit.](#)

³³⁹ [Sächsische Staatskanzlei, Staatssekretäre.](#)

³⁴⁰ [Sächsische Staatskanzlei, Beauftragter für Informationssicherheit des Landes \(BfIS\).](#)

³⁴¹ [Sächsische Staatskanzlei, Nachgeordnete Behörden.](#)

[Staatsbetrieb Sächsische Informatik Dienste, Aufgaben, Leistungen.](#)



- CERT: Das SAX.CERT ist an den SID angegliedert. SAX.CERT bietet zudem kostenfreie Sicherheitsdienstleistungen, wie einen Schwachstellenwarndienst oder Identity Leak Checker, für Landesverwaltung und Kommunen an.

Es ist bei TI als teilnehmendes Team gelistet³⁴².



- LfV [SN]: Die sächsische Landebehörde für Verfassungsschutz ist institutionell im dortigen Staatsministerium des Innern (SMI) aufgehängt.

Enge Arbeitsbeziehungen bestehen mit dem BfV, seinen Counterparts in allen Bundesländern (LfV's), dem BND, dem BAMAD, dem BSI sowie dem Cyber-AZ. Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden³⁴³.



- Institutionelle Ansässigkeit ZAC [SN]: SN4C, Akteursbeschreibung s. unten.



- Landesdatenschutzbehörde:
Sächsische:r Datenschutzbeauftragte:r (SächsDSDG)³⁴⁴.

Weitere Akteure in Sachsen:



Arbeitsgruppe Informationssicherheit (AG IS)

Die Arbeitsgruppe Informationssicherheit soll zur ressortübergreifenden Zusammenarbeit in Sachsen beitragen, in dem es im Bereich der Informationssicherheit zum einen den BfIS berät, sowie zum anderen Mindeststandards erarbeitet und anpasst. Letztere werden als Empfehlung beschlossen und daraufhin an den sächsischen Lenkungsausschuss für IT und E-Government (LA ITEG) zur finalen Beschlussfassung übergeben.

Der Vorsitz in der AG IS obliegt dem CISO [SN]. Als Mitglieder gehören der AG IS unter anderem der:die Informationssicherheitsbeauftragte des:der SächsDSDG und des SID sowie (ohne Stimmrecht) der:die Leiter:in des SAX.CERT an³⁴⁵.

³⁴² [Sächsische Staatskanzlei, Jahresbericht Informationssicherheit 2020 des Beauftragten für Informationssicherheit des Landes.](#)

[Staatsbetrieb Sächsische Informatik Dienste, CERT & Informationssicherheit.](#)

³⁴³ [Staatsministerium des Innern Sachsen, Sächsischer Verfassungsschutzbericht 2019.](#)

³⁴⁴ [Sächsischer Datenschutzbeauftragter, Über uns.](#)

³⁴⁵ [Sächsische Staatskanzlei, Arbeitsgruppe Informationssicherheit.](#)

[Sächsische Staatskanzlei, Sächsisches Informationssicherheitsgesetz.](#)



Cyber Crime Competence Center Sachsen (SN4C)

Das Cyber Crime Competence Center im Verantwortungsbereich des Landeskriminalamtes Sachsen fokussiert sich auf die verschiedenen Kriminalitätsfelder, die mit dem Internet in Zusammenhang stehen, wie zum Beispiel rechtswidrige Online-Transaktionen. Dabei verfolgt es einen integrativen Ansatz, indem es entsprechende Spezialisten zusammenzieht und so Synergieeffekte nutzbar macht. Zu seinen Aufgaben gehören außerdem die Beschaffung notwendiger Hard- und Software sowie die Beobachtung aktueller technischer Entwicklungen.

*Das Center übernimmt die Aufgabenbereiche der **ZAC [SN]** und arbeitet mit der **ZCS** zusammen³⁴⁶.*



Zentralstelle Cybercrime Sachsen (ZCS)

Die bei der Generalstaatsanwaltschaft Dresden angesiedelte Zentralstelle ist das justizielle Gegenstück zum SN4C des Landeskriminalamtes Sachsen. Die ZCS ermittelt lediglich selbst in Verfahren, sofern diese beispielsweise „die innere und äußere Sicherheit in Deutschland“ zum Gegenstand haben. Sie agiert primär als Koordinierungs- sowie beratende Stelle für Ermittler:innen und stellt thematische Aus- und Fortbildung sicher.

*ZCS und **SN4C** arbeiten eng zusammen³⁴⁷.*

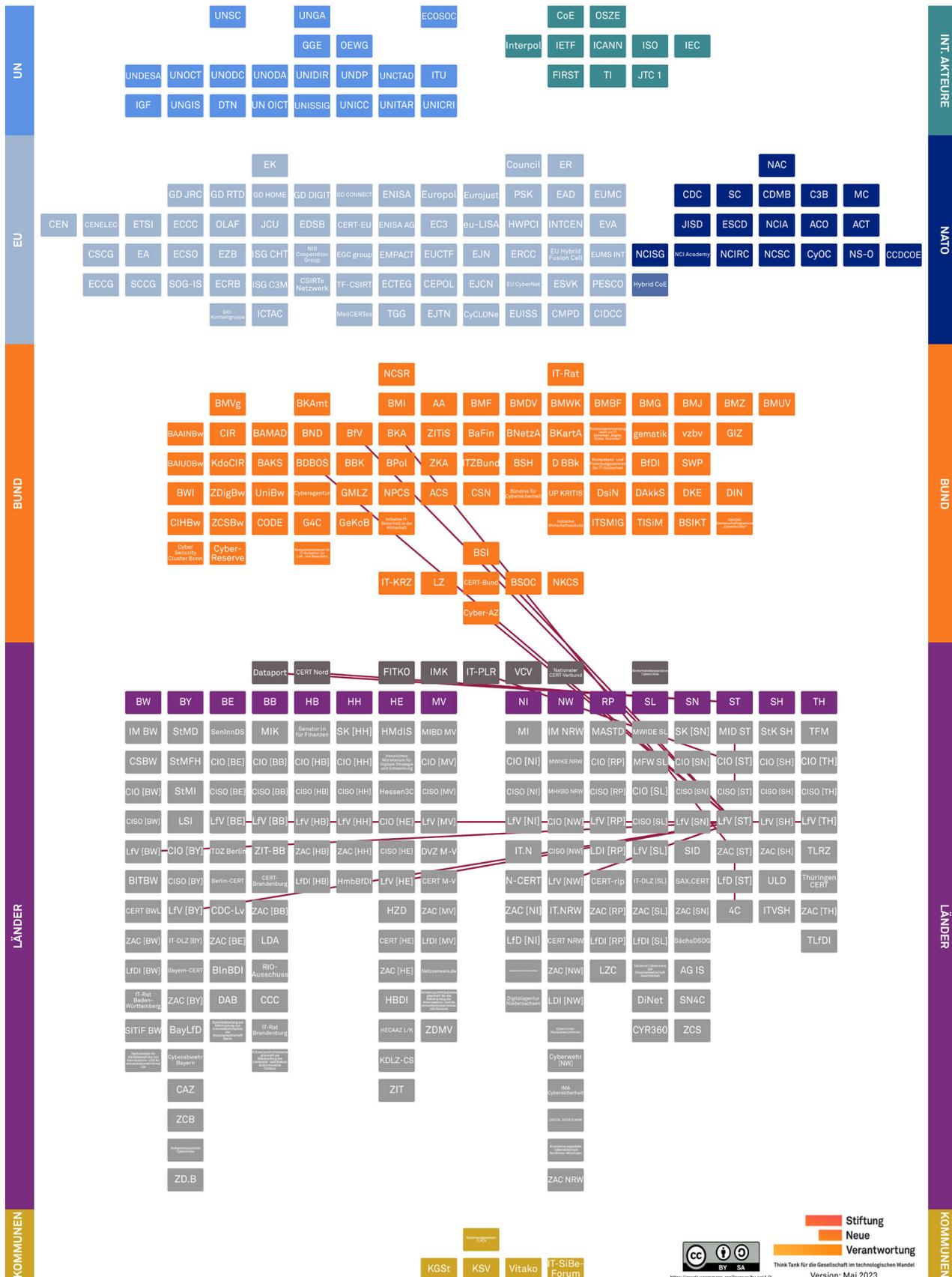
³⁴⁶ [Sächsisches Staatsministerium des Innern, Cybercrime Competence Center Sachsen \(SN4C\).](#)

[Sächsisches Staatsministerium des Innern, Zentrale Ansprechstelle Cybercrime \(ZAC\) für Unternehmen, Behörden und Verbände des Freistaates Sachsen.](#)

³⁴⁷ [Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Spezialisierte Einrichtungen der Justiz.](#)
[Staatsministerium der Justiz, Sächsisches Justizministerialblatt Nr. 5/2018.](#)



9.14 Sachsen-Anhalt (ST)





Das Land Sachsen-Anhalt zählt zu den Unterzeichnern des bundesländerübergreifenden Staatsvertrages, durch den **Dataport eingerichtet wurde**.

Überblick

- **Relevante Policy-Dokumente:**

- 2019: Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt, EGovG LSA)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Ministerium für Infrastruktur und Digitales Sachsen-Anhalt (MID ST, Abteilung 4 Digitale Gesellschaft und Geoinformation sowie Abteilung 5 Digitale Verwaltung).³⁴⁸



- **Landes-CIO [ST]:** Aktuell stellt das MID ST den:die Landes-CIO, der:die Beauftragte:r der Landesregierung für Informationstechnik ist.

Er:sie vertritt Sachsen-Anhalt im IT-PLR³⁴⁹.



- **Landes-CISO [ST]:** Das MID ST beheimatet neben dem:der Landes-CIO auch den:die Informationssicherheitsbeauftragte:r des Landes.

Er:sie unterrichtet den:die Landes-CIO [ST] und verantwortet Prozesse zur Umsetzung und Einhaltung von Informationssicherheitsstandards³⁵⁰.



- **Behördlicher IT-Dienstleister:** Dataport, Akteursbeschreibung s. unten (Kapitel 8.17).



- **CERT:** CERT Nord, Akteursbeschreibung s. unten (Kapitel 8.17).



- **LFV [ST]:** In Sachsen-Anhalt befindet sich die Landesverfassungsschutzbehörde im Ministerium für Inneres und Sport (Abteilung 4). Im Referat 44 ist eine Zuständigkeit für Spionageabwehr und Wirtschaftsschutz verortet. Gemäß sachsen-anhaltischem Verfassungsschutzbericht fallen unter Spionageabwehr auch Cyberoperationen.

Sofern erforderlich, können die LFV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden³⁵¹.

³⁴⁸ [Ministerium für Infrastruktur und Digitales Sachsen-Anhalt, Organigramm.](#)

³⁴⁹ [Sachsen-Anhalt, Der Beauftragte der Landesregierung für Informationstechnik \(CIO\).](#)

³⁵⁰ [Ministerium für Justiz und Gleichstellung Sachsen-Anhalt, Leitlinie zur Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt.](#)

³⁵¹ [Ministerium für Inneres und Sport Sachsen-Anhalt, Organisationsplan.](#)

[Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Verfassungsschutzbericht 2019.](#)



- **Institutionelle Ansässigkeit der ZAC [ST]:** Cybercrime Competence Center, Akteursbeschreibung s. unten.



- **Landesdatenschutzbehörde:**
Landesbeauftragte:r für den Datenschutz Sachsen-Anhalt (LfD)³⁵².

Weitere Akteure in Sachsen-Anhalt:



Cybercrime Competence Center (4C)

Das Competence Center wurde im Landeskriminalamt Sachsen-Anhalt eingerichtet und bündelt Spezialisten:innen verschiedener Dezernate im Bereich der Cyberkriminalität. Die Mitarbeiter:innen des Landeskriminalamtes werden dabei von Wissenschaftler:innen unterstützt, für die neue Stellen geschaffen wurden. Das Kompetenzzentrum soll sich landesweit um komplizierte Fälle kümmern und die Polizei bei einfacheren Betrugsfällen unterstützen.

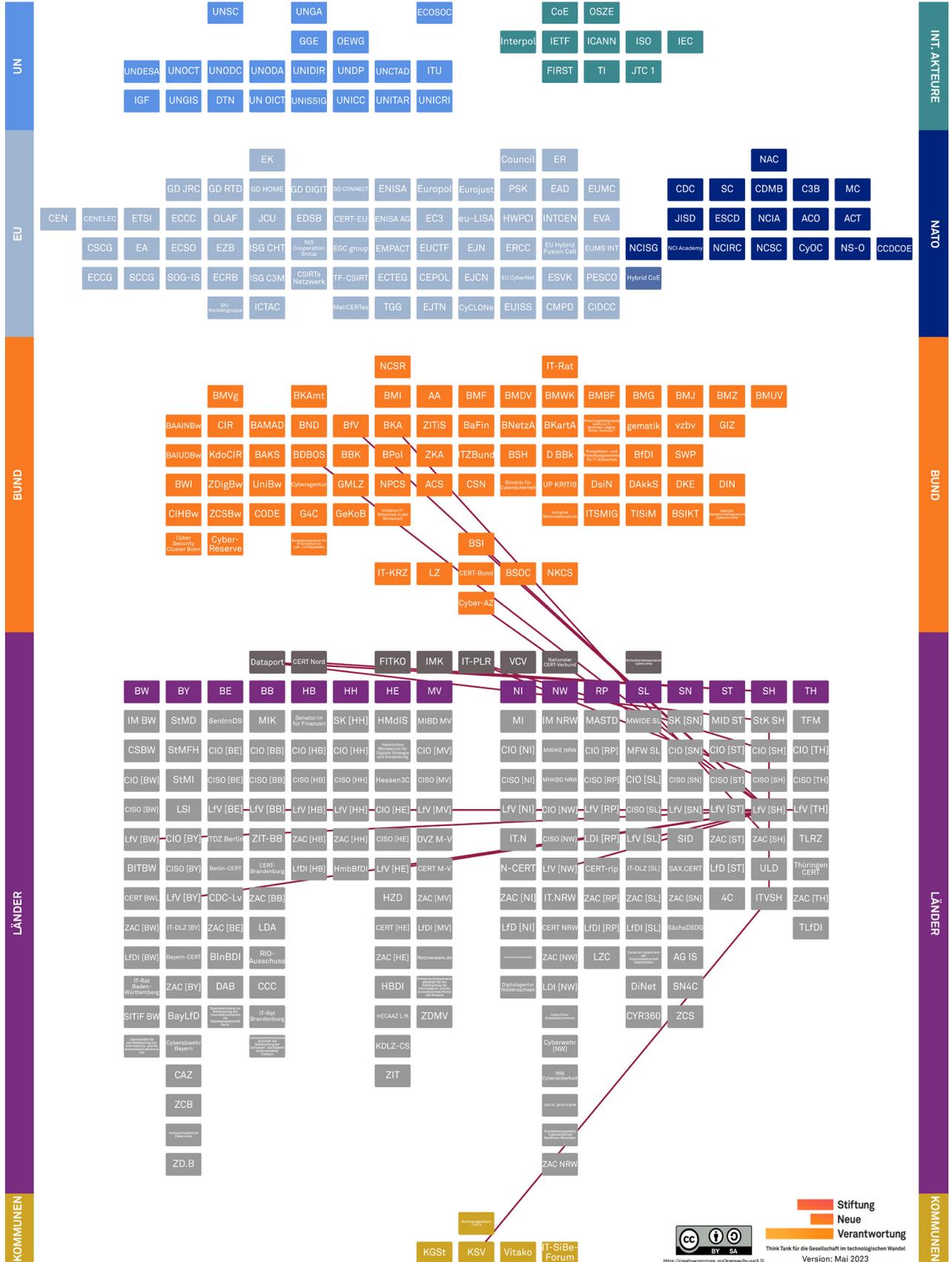
*Das Center ist auch die **ZAC [ST]** angesiedelt³⁵³.*

³⁵² [Landesbeauftragter für den Datenschutz Sachsen-Anhalt, Gesetzliche Aufgaben und Zuständigkeiten.](#)

³⁵³ [Hallelife.de, Sachsen-Anhalt startet Kompetenzzentrum gegen Internetkriminalität.](#)



9.15 Schleswig-Holstein (SH)





Das Land Schleswig-Holstein zählt zu den Unterzeichnern des bundesländerübergreifenden Staatsvertrages, durch den **Dataport eingerichtet wurde**.

Überblick

- **Relevante Policy-Dokumente:**

- 2009: Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (E-Government-Gesetz, EGovG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Staatskanzlei Schleswig-Holstein (StK SH, Abteilung 1: Zentrale Angelegenheiten, Service, Protokoll, Referat StK 10 Personal, Justitiariat und Informationssicherheit und Referat StK 14 Organisation, Digitalisierung und IT)³⁵⁴.



- **Landes-CIO [SH]:** Der:die CIO in Schleswig-Holstein ist zuständig für das Zentrale IT-Management Schleswig-Holstein und ist an die StK SH angebunden³⁵⁵.



- **Landes-CISO [SH]:** In Schleswig-Holstein ist der:die Informationssicherheitsbeauftragte:r für die Landesverwaltung (CISO) innerhalb der **Stk SH** angesiedelt. Der:dem CISO obliegt das ressortübergreifende Informationssicherheitsmanagement.

Er:sie verfügt über ein Vortragsrecht gegenüber dem:der als Landes-CIO [SH] agierenden Staatssekretär:in und ist zudem in der AG InfoSic des IT-PLR für Schleswig-Holstein vertreten³⁵⁶.



- **Behördlicher IT-Dienstleister:** Dataport, Akteursbeschreibung s. unten (Kapitel 8.17).



- **CERT:** CERT Nord, Akteursbeschreibung s. unten (Kapitel 8.17).



- **LfV [SH]:** Die Landesverfassungsschutzbehörde des Landes Schleswig-Holstein ist im dortigen Ministerium für Inneres, Kommunales, Wohnen und Sport (MIKWS SH) angesiedelt (Abteilung IV 7). Unter ihre Arbeitsfelder fällt unter anderem Spionageabwehr und Wirtschaftsschutz. Ein weiteres Referat (IV 76) befasst sich darüber hinaus mit „Digitale[m] Arbeiten, IT, G10 und Geheimschutz“.

³⁵⁴ [Staatskanzlei Schleswig-Holstein, Organisation und Ansprechpartner.](#)

³⁵⁵ [Schleswig-Holstein, E-Government – Steuerung und Zusammenarbeit.](#)

³⁵⁶ [Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung Schleswig-Holstein, Bemerkungen 2017 des Landesrechnungshofs Schleswig-Holstein mit Bericht zur Landeshaushaltsrechnung 2015; Bericht und Beschlussempfehlung des Finanzausschusses vom 01.12.2017, Drucksache 19/364; hier: Aktuelle Nachberichterstattung zu unserem Bericht vom 29.04.2019.](#)



Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden³⁵⁷.



- **Institutionelle Ansässigkeit der ZAC [SH]:** Landeskriminalamt Schleswig-Holstein. Sie koordiniert auch „länderübergreifende Cybercrime-Ermittlungen im Falle von Angriffen gegen Unternehmen und Behörden“³⁵⁸.



- **Landesdatenschutzbehörde:** Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) mit Landesbeauftragter:m für Datenschutz³⁵⁹.

Weitere Akteure in Schleswig-Holstein:



IT-Verbund Schleswig-Holstein (ITVSH)

Der gemeinschaftlich vom Land Schleswig-Holstein und seinen Kommunen finanzierte ITSVH steht Kommunen als Ansprechpartner in Digitalisierungsfragen zur Verfügung und setzt zudem konkrete Projekte um. Das ITVSH-Projekt SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) unterstützt schleswig-holsteinische Kommunen bei der Etablierung eines Informationssicherheitsmanagements sowie der Implementierung von BSI-IT-Grundschutzprofilen.

Dem Verwaltungsrat des ITVSH gehören Vertreter:innen der **KSV** auf Länderebene an³⁶⁰.

³⁵⁷ [Der Ministerpräsident des Landes Schleswig-Holstein, Spionageabwehr und Wirtschaftsschutz. Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung, Organisationsplan.](#)

³⁵⁸ [Landespolizei Cybercrime, Zentrale Ansprechstelle Cybercrime \(ZAC\).](#)

³⁵⁹ [Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Wir über uns.](#)

³⁶⁰ [Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: IT-Verbund Schleswig-Holstein \(ITVSH\).](#)

[IT-Verbund Schleswig-Holstein, SiKoSH.](#)

[Landesregierung Schleswig-Holstein, Gesetz zur Errichtung einer Anstalt öffentlichen Rechts „IT-Verbund Schleswig-Holstein“ \(Errichtungsgesetz ITVSH\).](#)



Überblick

- **Relevante Policy-Dokumente:**

- 2018: Thüringer Gesetz zur Förderung der elektronischen Verwaltung (Thüringer E-Government-Gesetz, ThürEGovG)



- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** Thüringisches Finanzministerium (TFM, Abteilung 5 E-Government und IT, Referat 53 Informationssicherheit, Rechtsfragen von E-Government und IT, Vergabe)³⁶¹.



- **Landes-CIO [TH]:** Der:die CIO von Thüringen (Beauftragte:r des Freistaates Thüringen für E-Government und IT) ist als Staatssekretär:in im **TFM** angesiedelt und für die Vereinheitlichung von IT- und E-Government-Strukturen verantwortlich. Ihm:ihr untersteht eine Koordinierungsstelle für E-Government und IT.

*Er:sie ist Mitglied im **IT-PLR** und ihm:ihr kommt die Fachaufsicht über das Thüringer Landesrechenzentrum (**TLRZ**) zu. Zusätzlich ist er:sie in strategischen Belangen Ansprechpartner für die **KSV**³⁶².*



- **Landes-CISO [TH]:** Der:die thüringische IT-Sicherheitsbeauftragte:r wird durch das **TFM** eingesetzt und ist in dessen Abteilung 5 angesiedelt. Er:sie leitet das unter anderem das aus Informationssicherheitsbeauftragten aller Ressorts bestehende Informationssicherheitsteam (ISM-Team).

*Er:sie ist unmittelbar dem:der **Landes-CIO [TH]** unterstellt³⁶³.*



- **Behördlicher IT-Dienstleister:** TLRZ im Geschäftsbereich des **TFM**³⁶⁴.



- **CERT:** Das ThüringenCERT wird durch das **TLRZ** betrieben³⁶⁵.



- **LfV [TH]:** In Thüringen ist die Landesbehörde für Verfassungsschutz innerhalb des Thüringer Ministerium für Inneres und Kommunales (TMIK) organisatorisch

³⁶¹ [Thüringer Finanzministerium, Geschäftsverteilungsplan. Thüringer Finanzministerium, Informationssicherheit. Thüringer Landtag, Unterrichtung durch die Landesregierung: Aktionsplan 2016 zur Umsetzung der Strategie für E-Government und IT des Freistaats Thüringen.](#)

³⁶² [Freistaat Thüringen, CIO des Freistaats Thüringen. Thüringer Finanzministerium, Verwaltungsvorschrift für die Organisation des E-Government und des IT-Einsatzes in der Landesverwaltung des Freistaats Thüringen vom 12. März 2019.](#)

³⁶³ [Finanzministerium Thüringen, Informationssicherheitsleitlinie der Thüringer Landesverwaltung.](#)

³⁶⁴ [Thüringer Landesrechenzentrum, Über uns.](#)

³⁶⁵ [Bundesamt für Sicherheit in der Informationstechnik, BSI und Thüringen: Engere Zusammenarbeit bei der Cybersicherheit \(Webseite entfernt\). Thüringer Landesrechenzentrum, ThüringenCERT.](#)



angesiedelt. Im Rahmen des Referats 54 wird sich dort mit der Spionageabwehr befasst, welche auch Cyberabwehr sowie Wirtschaftsschutz beinhaltet.

Sofern erforderlich, können die LfV's zur Verhinderung oder Erforschung von Aktivitäten, die die Sicherheit oder Nutzung von Informationstechnik beeinträchtigen, durch das BSI unterstützt werden³⁶⁶.



- **Institutionelle Ansässigkeit der ZAC [TH]:** Dezernat Cybercrime des Landeskriminalamtes Thüringen (TLKA). Dieses beschäftigt sich unter anderem mit Betrug im Internet und Ermittlungen zu Kinder- und Jugendpornografie im Netz³⁶⁷.



- **Landesdatenschutzbehörde:** Thüringische:r Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit (TLfDI)³⁶⁸.

³⁶⁶ [Ministerium für Inneres und Kommunales Thüringen, Organigramm.](#)

[Ministerium für Inneres und Kommunales Thüringen, Wirtschaftsspionage / Wirtschaftsschutz.](#)

³⁶⁷ [Heise Online, Cybercrime: Neue Herausforderungen für Thüringer LKA.](#)

[Ministerium für Inneres und Kommunales Thüringen, Internetkriminellen gemeinsam mit den Unternehmen das Handwerk legen. \(Webseite entfernt\)](#)

³⁶⁸ [Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.](#)



9.17 Bundesländerübergreifende Akteure



CERT Nord

Die Länder Bremen, Schleswig-Holstein, Hamburg und Sachsen-Anhalt haben ein gemeinsames CERT Nord. Informationen zu IT-Sicherheitsvorfällen werden über interne Plattformen geteilt. Sofern notwendig, übernimmt das CERT Nord bei Vorfällen mit ressort- und eventuell länderübergreifenden Auswirkungen die Koordination reaktiver Maßnahmen. Das CERT Nord spricht für seinen Adressatenkreis Empfehlungen für präventive IT-Sicherheitsmaßnahmen und -standards aus.

Das CERT Nord ist bei [Dataport](#) angesiedelt und ist Mitglied im [VCV](#)³⁶⁹.



Dataport

Als Anstalt des öffentlichen Rechts basiert Dataport auf einem Staatsvertrag zwischen den Ländern Bremen, Hamburg, Niedersachsen, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein. Für diese sechs Bundesländer und deren öffentliche Verwaltungen agiert Dataport als zentraler IT-Dienstleister. Zur Identifikation und Abwehr von Cyberoperationen verfügt Dataport auch über ein Security Operations Center (SOC), welches u.a auch kontinuierlich und proaktiv auf der Suche nach Schwachstellen ist.

BSI und Dataport haben eine Vereinbarung über den Informationsaustausch und die Zusammenarbeit in der Informationssicherheit geschlossen. Dataport's Verwaltungsrat gehören Vertreter:innen der [Senator:in](#) für Finanzen [HB], der [SK](#) [HH], dem [Finanzministerium](#) [NI], dem [MIBD MV](#) (die:der [Landes-CIO](#) [MV]), sowie der [Staatskanzlei SH](#) an³⁷⁰.



Sicherheitskooperation Cybercrime

Die Sicherheitskooperation ist eine Initiative, die eine Plattform für Polizei und Digitalwirtschaft bietet, um gemeinsam den Gefahren durch Cybercrime zu begegnen und dazu Wissen und technische Kompetenzen auszutauschen.

Sie ist eine Initiative der [Landeskriminalämter](#) aus [Baden-Württemberg](#), [Hessen](#), [Niedersachsen](#), [Nordrhein-Westfalen](#), [Rheinland-Pfalz](#) und [Sachsen](#) sowie dem [Bitkom](#)³⁷¹.

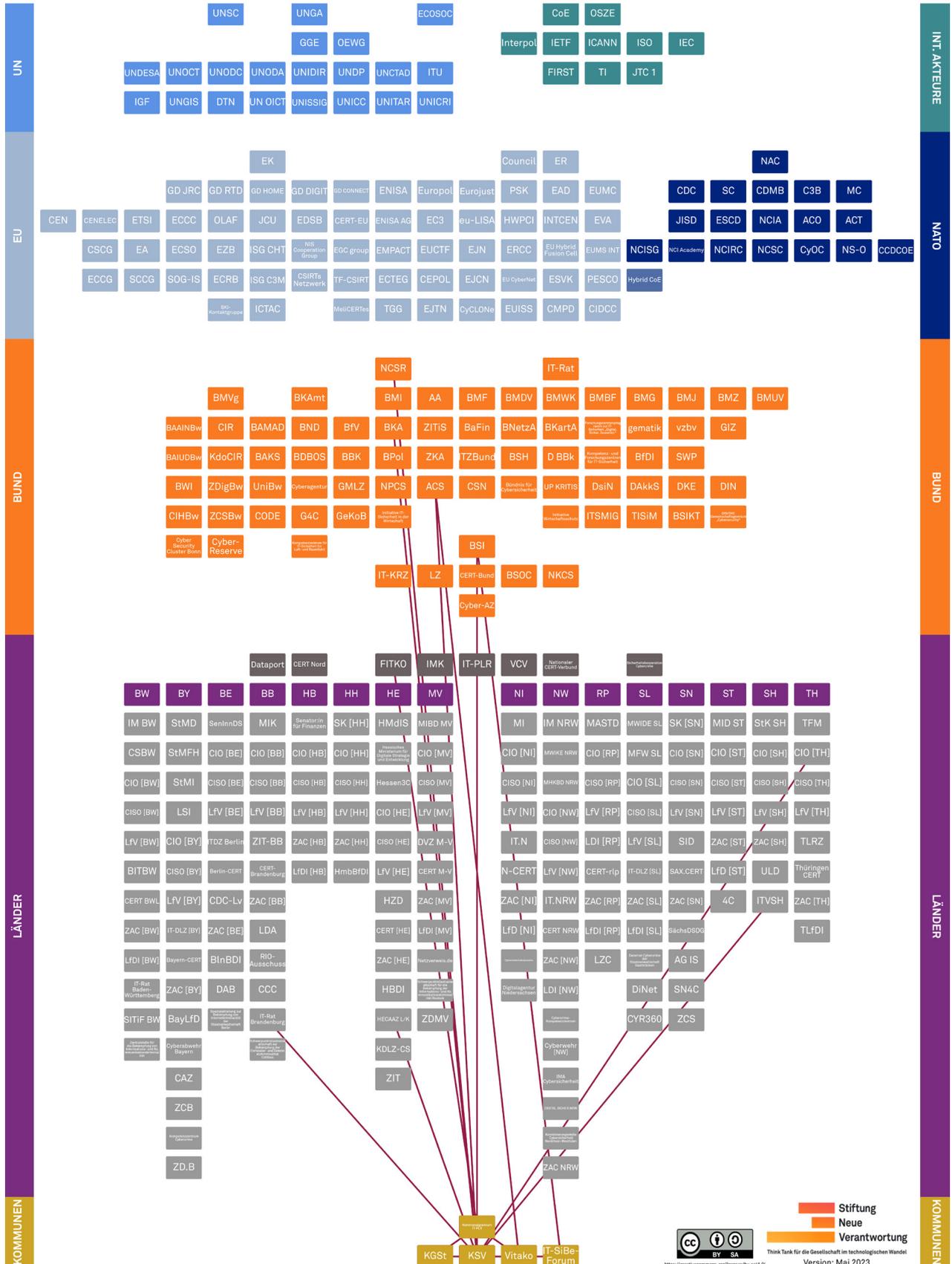
³⁶⁹ [CERT Nord, CERT Nord.](#)

³⁷⁰ [Bundesamt für Sicherheit in der Informationstechnik, BSI und Dataport vereinbaren engere Zusammenarbeit. Dataport, Die Organe von Dataport. Dataport, Dataport, Digitalisierung. Mit Sicherheit. Dataport, Security Operations Center.](#)

³⁷¹ [Sicherheitskooperation Cybercrime, Aktivitäten. Sicherheitskooperation Cybercrime, Die Kooperation.](#)



10. Erläuterung – Akteure auf Kommunalebene





Policy-Überblick

Jahr	Name
2019	IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung (Version 2.0)
2017	Handreichung: Informationssicherheits-Leitlinie in Kommunalverwaltungen Vorgänger-Dokument(e): <ul style="list-style-type: none">• 2015: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen



Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (Vitako)

In der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (Vitako) mit Sitz in Berlin haben sich derzeit 52 Rechenzentren, Software- und IT-Serviceunternehmen zusammengeschlossen, die in über 10.000 Kommunen Deutschlands operieren. Die Vitako hat sich zum Ziel gesetzt, Wissen sowie Know-how zu bündeln und dadurch ihren Mitgliedern hinsichtlich der Nutzung von Informationstechnik im öffentlichen Sektor behilflich zu sein. Zudem vertritt die Vitako als Verband die Interessen und die Perspektive der kommunalen IT-Dienstleister zu „rechtlichen sowie technisch-organisatorischen Rahmenbedingungen“ in politischen Foren und Gremien. Innerhalb der Vitako haben sich Mitglieder zum inhaltlichen Austausch sowie der Erarbeitung von Handlungsleitfäden und Verbandspositionen zu zwölf Facharbeitsgruppen zusammengeschlossen, die bspw. aktuelle Entwicklungen im Bereich E-Government, IT-Sicherheit oder Standardisierung diskutieren.

*Die Vitako entsendet drei Vertreter:innen in das **Kommunalgremium** der **FITKO**. Enge Arbeitsbeziehungen bestehen zu den drei **kommunalen Spitzenverbänden**, die durch die Vitako durch Know-how sowie bei deren Interessenvertretung in IT-Sicherheitsfragen unterstützt werden. Empfehlungen der Vitako selbst werden immer in Abstimmung mit den kommunalen Spitzenverbänden getroffen. Darüber hinaus unterhält die Vitako unter anderem eine Kooperation mit der **KGSt**. Die Vitako ist Multiplikator der **ACS**³⁷².*



IT-SiBe-Forum

Als verwaltungsinternes, nicht-öffentliches Forum von Kommunen und Ländern steht das IT-SiBe-Forum als Plattform allen kommunalen IT-Sicherheitsbeauftragten offen, die als Ansprechpartner in Kommunalverwaltungen und kommunalen Einrichtungen die Umsetzung von IT-Sicherheit und die Einführung von IT-Grund-

³⁷² [Vitako, Gremien.](#)
[Vitako, Satzung.](#)
[Vitako, Verband.](#)
[Vitako, Verein.](#)



schutzstandards verantworten³⁷³. Ihnen bietet das IT-SiBe-Forum Möglichkeiten für Informations- und Erfahrungsaustausch. Grundsätze des IT-SiBe-Forums stellen hierbei unter anderem die Wahrung der kommunalen Selbstverwaltung, gegenseitige Unterstützung sowie eine Bündelungsfunktion für Ebenen übergreifende Zusammenarbeit dar.

Das IT-SiBe-Forum wird durch das BSI unterstützt. Aus dem IT-SiBe-Forum bilden sich zudem Arbeitsgruppen der kommunalen Spitzenverbände mit Praktiker:innen der IT-Sicherheit aus der Kommunalebene. Zuletzt war das IT-SiBe-Forum in diesem Kontext unter anderem an der Überarbeitung des IT-Grundschutz-Profiles „Basis-Ab-sicherung Kommunalverwaltung“ sowie der „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ aktiv beteiligt³⁷⁴.



Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt)

Die KGSt unterstützt als Gemeinschaftsstelle seine Mitglieder – Städte, Kreise, Gemeinden und weiteren Verwaltungsorganisationen aus der gesamten DACH-Region – bei sämtlichen Fragen im Bereich des kommunalen Managements und bietet Hilfe bei der Umsetzung der Verwaltungsmodernisierung an. In der Praxis umfasst dieses Angebot für derzeit mehr als 2.200 Kommunen die Bereitstellung von Information, Handlungsempfehlungen, individueller Beratung und Seminaren im Bereich von kommunaler IT-Steuerung, IT-Strategie sowie IT- und Datensicherheit. Zusätzlich hat die KGSt einen Innovationszirkel „Digitales und IT-Steuerung“ eingerichtet, in welchem regelmäßig ca. 30 kommunale IT-Expert:innen zusammenkommen, Erfahrungen austauschen und bei Bedarf Positionspapiere verfassen.

*Die KGSt unterhält eine Kooperation mit den **kommunalen Spitzenverbänden** und ist durch zwei Vertreter:innen im **Kommunalgremium der FITKO** vertreten³⁷⁵.*



Kommunale Spitzenverbände (KSV)

Kommunale Spitzenverbände als Sammelbegriff umfassen die freiwilligen interkommunalen Zusammenschlüsse und Interessenverbände deutscher Gemeinden und Städte auf Bundesebene: den Deutschen Städtetag, den Deutschen Städte-

³⁷³ Es ist darauf hinzuweisen, dass nicht alle Kommunen Deutschlands über eine:n IT-SiBe verfügen und deren Aufgabenfelder sowie Verantwortlichkeiten aufgrund der kommunalen Heterogenität weit gestreut und sehr unterschiedlich sein können.

³⁷⁴ Heino Sauerbrey, Ziel und Zweck des Internetforums für IT-Sicherheitsbeauftragte der Länder und Kommunen. (Webseite entfernt)
[IT-SiBe-Forum, Grundsätze.](#)
[IT-SiBe-Forum, Kurzinformation.](#)
[IT-SiBe-Forum, Meilensteine.](#)

³⁷⁵ KGSt, [Über Uns.](#)
[KGSt, IT-Strategie, IT-Steuerung und Informationssicherheit.](#)
[KGSt, Organisation, Digitales und IT.](#)
[KGSt, Innovationszirkel: Digitales und IT-Steuerung.](#)



und Gemeindebund sowie den Deutschen Landkreistag. Deren Arbeit wird innerhalb der Bundesvereinigung der kommunalen Spitzenverbände koordiniert, deren Vorsitz jährlich unter den dreien rotiert. Gemeinsam oder einzeln nehmen die kommunalen Interessenverbände zu politischen Entscheidungsprozessen oder Planungen des Bundes mit Kommunalrelevanz Stellung und werden ggf. an diesbezüglichen Gesetzgebungsverfahren beteiligt. Dies schließt auch die Themen IT- und Cybersicherheit mit ein. Die Vertretung der kommunalpolitischen Interessen ihrer Mitglieder soll dabei der Förderung der kommunalen Selbstverwaltung dienen. In diesem Kontext ist es den kommunalen Spitzenverbänden, die auch auf Länderebene organisiert sind, zudem ein Anliegen, den Austausch von Erfahrungen und Informationen zwischen ihren Mitgliedern zu ermöglichen und zu pflegen.

Der KSV (durch den Deutschen Städtetag) vertritt die Kommunen im NCSR. Gemeinsam mit dem BSI haben die KSV ein IT-Grundschutzprofil für Kommunen erarbeitet. Zudem haben die KSV in Zusammenarbeit mit BKA und dem BSI Empfehlungen für IT-Operationen auf kommunale Verwaltungen ausgesprochen. Über die KSV und im Rahmen des IT-SiBe-Forum hat das BSI die Kommunalverwaltungen in die Modernisierung des IT-Grundschutzes eingebunden. Gemeinsam mit der Vitako haben die drei KSV eine Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen publiziert. Die KSV können durch insgesamt drei (jeweils eine:n) entsandte Vertreter:innen an den Sitzungen des IT-Planungsrates in beratender Funktion teilnehmen. An der Benennung der Vertreter:innen für das Kommunalgremium der FITKO sind die kommunalen Spitzenverbände beteiligt und können grundsätzlich auch selber als solche fungieren. So stellt der Städte- und Gemeindebund beispielsweise eine:n von drei Vertreter:in für die Städte und Gemeinden im FITKO-Kommunalgremium. Rein vertretungsweise sind für die Städte und Kreise auch der Deutsche Städtetag sowie der Deutsche Landkreistag vertreten. Der Deutsche Landkreistag ist zudem Mitglied der ACS. Die Schulungen des HECAAZ L/K finden in Abstimmung und Unterstützung der regionalen KSV statt³⁷⁶.



Kommunalgremium des IT-Planungsrates

Unter dem Vorsitz der FITKO wurde ein Kommunalgremium des IT-Planungsrates eingerichtet. Das Gremium soll hauptsächlich Funktionen im Bereich des kommunalen IT-Bedarfsmanagement übernehmen, kommunale IT-Bedarfe abfragen und eine Kommunikations- und Informationsplattform zwischen dem IT-Planungsrat

³⁷⁶ [BSI, Empfehlungen bei IT-Angriffen auf kommunale Verwaltungen.](#)
[BSI, IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung.](#)
[Deutscher Landkreistag, Bundesvereinigung der kommunalen Spitzenverbände.](#)
[Deutscher Landkreistag, Der Verband.](#)
[Deutscher Städtetag, Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen.](#)
[DStGB, Wir über uns.](#)
[IT-Planungsrat, Zusammensetzung des IT-Planungsrats.](#)
[Schubert & Klein, Kommunale Spitzenverbände.](#)



und Kommunen im Bereich föderaler IT aufbauen. Dadurch spielt das Kommunalgremium auch eine Rolle bei der operativen Umsetzung des Onlinezugangsgesetzes (OZG) zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen. Das Gremium tag ca. alle 4 Wochen.

*In dem Kommunalgremium (insgesamt 14 Mitglieder) sind je drei Vertreter:innen der Landkreise, Städte und Gemeinden inklusive ihres Spitzenverbandes (KSV), drei Vertreter:innen der **Vitako** sowie zwei Vertreter:innen der **KGSt** vertreten³⁷⁷.*

³⁷⁷ FITKO, [Wie unterstützt die FITKO die Digitale Transformation?](#).

[Innenministerkonferenz, Bericht zum IT-Planungsrat.](#)

KGSt, OZG-Umsetzung: Die kommunale Stimme stärken. (Webseite entfernt)



Über die Stiftung Neue Verantwortung

Die Stiftung Neue Verantwortung (SNV) ist ein gemeinnütziger Think Tank, der an der Schnittstelle von Technologie und Gesellschaft arbeitet. Die Kernmethode der SNV ist die kollaborative Entwicklung von Politikvorschlägen und -analysen. Die Expert:innen der SNV arbeiten nicht allein, sondern entwickeln und testen Ideen gemeinsam mit Vertreter:innen aus Politik und Verwaltung, Technologieunternehmen, Zivilgesellschaft und Wissenschaft. Unsere Expert:innen arbeiten unabhängig von Interessengruppen und Parteien. Unsere Unabhängigkeit gewährleisten wir durch eine Mischfinanzierung, zu der viele verschiedene Stiftungen, öffentliche Mittel und Unternehmensspenden beitragen.



Über die Autor:innen

Dr. Sven Herpig ist Leiter für Cybersicherheitspolitik und Resilienz. Bei der SNV befasst sich vorrangig mit der deutschen Cybersicherheitspolitik, Staatlichem Hacken (u.a. dem „Bundestrojaner“) und IT-Schwachstellenmanagement, der staatlichen Beantwortung von Cyberoperationen, Angriffen auf Machine-Learning Anwendungen und Aktiver Cyberabwehr.

Christina Rupp ist Projektmanagerin im Themenbereich Cybersicherheitspolitik und Resilienz. Sie arbeitet zu Themen der Cyberdiplomatie und Cyberaußenpolitik, insbesondere internationalen Normen für verantwortliches Staatenverhalten im Cyberraum, sowie Deutschlands staatlicher Cybersicherheitsarchitektur.

Rebecca Beigel ist Projektleiterin (Jr.) für Cybersicherheitspolitik und Resilienz. Ihre Arbeitsschwerpunkte liegen auf Cyber Capacity Building, cybersicherheitspolitischen Übungen im länderspezifischen Kontext und deutscher Cybersicherheitspolitik.

Frederic Dutke unterstützt als studentische Hilfskraft den Themenbereich Cybersicherheitspolitik und Resilienz. Sein Schwerpunkt ist die deutsche Cybersicherheitsarchitektur.

So erreichen Sie die Autor:innen:

Dr. Sven Herpig
Leiter für Cybersicherheitspolitik und Resilienz
sherpig@stiftung-nv.de
+49 (0) 30 81 45 03 78 91

Christina Rupp
Projektmanagerin Cybersicherheitspolitik und Resilienz
crupp@stiftung-nv.de

Rebecca Beigel
Projektleiterin (Jr.) Cybersicherheitspolitik und Resilienz
rbeigel@stiftung-nv.de

Frederic Dutke
Studentische Hilfskraft Cybersicherheitspolitik und Resilienz
fdutke@stiftung-nv.de



Impuls

Mai 2023

Deutschlands staatliche Cybersicherheitsarchitektur

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center

Berliner Freiheit 2

10785 Berlin

T: +49 (0) 30 81 45 03 78 80

F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de

info@stiftung-nv.de

Design:

Make Studio

www.make-studio.net

Layout:

Jan Klöthe



Dieser Beitrag unterliegt einer Creative Commons-Lizenz (CC BY-SA). Die Vervielfältigung, Verbreitung und Veröffentlichung, Veränderung oder Übersetzung von Inhalten der Stiftung Neue Verantwortung, die mit der Lizenz „CC BY-SA“ gekennzeichnet sind, sowie die Erstellung daraus abgeleiteter Produkte sind unter den Bedingungen „Namensnennung“ und „Weiterverwendung unter gleicher Lizenz“ gestattet. Ausführliche Informationen zu den Lizenzbedingungen finden Sie hier: creativecommons.org/licenses/by-sa/4.0/.