April 2021 · Dr. Sven Herpig & Christina Rupp

Deutschlands staatliche Cybersicherheits-architektur

6. Auflage

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Inhalt

1. Hintergrund **8**

2. Visualisierung der Cybersicherheitsarchitektur **10**

3. Akteure und Abkürzungen **11**

4. Erläuterung – Akteure auf EU-Ebene **21**

Agentur der Europäischen Union für Cybersicherheit (ENISA) 21
Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) 22
Computer Emergency Response Team der Europäischen Kommission (CERT-EU) 22
Contractual Public Private Partnership on Cybersecurity (cPPP) 23
Computer Security Incident Response Teams Netzwerk (CSIRTs Netzwerk) 23
Cyber Crisis Liaison Organisation Network (CyCLONe) 23
Cyber and Information Domain Coordination Centre (CIDCC) 24
Direktion Krisenbewältigung und Planung (CMPD) 24
ENISA-Beratungsgruppe (ENISA AG) 25
EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell) 25
Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA) 26
Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG) 26
Europäische Kommission (EK) 27
Europäische Kooperation für Akkreditierung (EA) 27
Europäische Polizeiakademie (CEPOL) 27
Europäische Verteidigungsagentur (EVA) 28
Europäischer Auswärtiger Dienst (EAD) 28
Europäische:r Datenschutzbeauftragte:r (EDSB) 29
Europäischer Rat (ER) 29
Europäisches Amt für Betrugsbekämpfung (OLAF) 30
Europäisches Polizeiamt (Europol) 30
Europäisches Sicherheits- und Verteidigungskolleg (ESVK) 30
Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) 31
Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität (EC3) 31
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) 32
European Cybercrime Training and Education Group (ECTEG) 32
European Cyber Security Organisation (ECSO) 33
European Government CERTs group (EGC group) 33
European Judicial Network (EJN) 34
European Judicial Cybercrime Network (EJCN) 34

European Judicial Training Network (EJTN) 34
European Union Cybercrime Task Force (EUCTF) 35
Gemeinsame Forschungsstelle (GD JRC) 35
Generaldirektion Forschung und Innovation (GD RTD) 35
Generaldirektion Informatik (GD DIGIT) 35
Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD CONNECT) 36
Generaldirektion Migration und Inneres (GD HOME) 36
Gruppe der Interessenträger für die Cybersicherheitszertifizierung 37
Horizon 2020 37
Horizontal Working Party on Cyber Issues (HWP) 37
Institut der Europäischen Union für Sicherheitsstudien (EUISS) 38
Intelligence Directorate des EU-Militärstabs (EUMS INT) 38
Inter-Service Group „Community Capacity in Crisis-Management“ (ISG C3M) 39
Inter-Service Group „Countering Hybrid Threats“ (ISG CHT) 39
Kontaktgruppe zum Schutz Kritischer Infrastrukturen (SKI-Kontaktgruppe) 39
Kooperationsgruppe unter der NIS-Richtlinie (NIS Cooperation Group) 39
MeliCERTes 40
Militärausschuss der Europäischen Union (EUMC) 40
NIS Public-Private Platform (NIS Platform) 41
Politisches und Sicherheitspolitisches Komitee (PSK) 41
Rat der Europäischen Union (Council) 42
Reference Incident Classification Taxonomy Task Force (TF-CSIRT) 43
Senior Officials Group Information Systems Security (SOG-IS) 43
Ständige Strukturierte Zusammenarbeit (PESCO) 43
Taxonomy Governance Group (TGG) 43
Zentrum für die Koordination von Notfallmaßnahmen (ERCC) 44
Zentrum für Informationsgewinnung und -analyse (INTCEN) 44

5. Erläuterung – Akteure auf NATO-Ebene 46
Allied Command Operations (ACO) 46
Allied Command Transformation (ACT) 46
Cyber Defence Committee (CDC) 47
Emerging Security Challenges Division (ESCD) 47
Joint Intelligence and Security Division (JISD) 48
NATO Communications and Information Agency (NCIA) 48
NCI Academy 49
NATO Computer Incident Response Capability (NCIRC) 49
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 50
NATO Consultation, Control and Command Board (C3B) 51
NATO Cyber Defence Management Board (CDMB) 51
NATO Cyber Security Centre (NCSC) 51

NATO Cyberspace Operations Centre (CyOC) 52
NATO-Militärauschuss (MC) 52
NATO School Oberammergau (NS-O) 53
NATO Security Committee (SC) 53
Nordatlantikrat (NAC) 53

6. Erläuterung – Akteure auf Bundesebene 55
Agentur für Innovation in der Cybersicherheit (Cyberagentur) 55
Agentur für Sprunginnovationen (SprinD) 55
Allianz für Cyber-Sicherheit (ACS) 56
Auswärtiges Amt (AA) 56
Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) 57
Bundesakademie für Sicherheitspolitik (BAKS) 57
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) 57
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) 57
Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) 58
Bundesamt für den Militärischen Abschirmdienst (BAMAD) 58
Bundesamt für Sicherheit in der Informationstechnik (BSI) 59
Bundesamt für Verfassungsschutz (BfV) 60
Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit (BfDI) 60
Bundeskanzleramt (BKAmt) 60
Bundeskartellamt (BKartA) 61
Bundeskriminalamt (BKA) 61
Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 62
Bundesministerium der Verteidigung (BMVg) 62
Bundesministerium des Innern, für Bau und Heimat (BMI) 62
Bundesministerium für Bildung und Forschung (BMBF) 63
Bundesministerium für Finanzen (BMF) 63
Bundesministerium für Gesundheit (BMG) 63
Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) 64
Bundesministerium für Wirtschaft und Energie (BMWi) 64
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) 64
Bundesnachrichtendienst (BND) 64
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) 65
Bundesverband der Verbraucherzentralen und Verbraucherverbände (vzbv) 65
Bundespolizei (BPol) 66
Bundeswehr (Bw) 66
Bundesweite IT-Systemhaus GmbH (BWI) 66

Bündnis für Cybersicherheit 67
Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) 67
Cyber Innovation Hub (CIHBw) 67
Cyber-Reserve 68
Cyber Security Cluster Bonn e. V. 68
Deutsche Akkreditierungsstelle (DAkkS) 69
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 69
Deutschland sicher im Netz e. V. (DsiN) 69
Forschungsinstitut Cyber Defence (CODE) 70
Föderale IT-Kooperation (FITKO) 70
gematik 70
Gemeinsames Lagezentrum Cyber- und Informationsraum (GLZ CIR) 71
Gemeinsames Melde- und Lagezentrum (GMLZ) 71
German Competence Centre against Cyber Crime (G4C) 71
Informationstechnikzentrum Bund (ITZBund) 72
Initiative IT-Sicherheit in der Wirtschaft 72
Initiative Wirtschaftsschutz 72
Innenministerkonferenz (IMK) 73
IT-Planungsrat (IT-PLR) 73
IT-Rat 74
IT Security made in Germany (ITSMIG) 74
Kommando Cyber- und Informationsraum (KdoCIR) 74
Kommando Informationstechnik (KdoITBw) 75
Kommando Strategische Aufklärung (KdoStratAufkl) 75
Nationaler Cyber-Sicherheitsrat (Cyber-SR) 76
Nationaler CERT-Verbund 76
Nationaler Pakt Cybersicherheit 77
Nationales Cyber-Abwehrzentrum (Cyber-AZ) 77
Nationales IT-Lagezentrum (LZ) 78
Organisationsbereich Cyber- und Informationsraum (CIR) 78
Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen (UP KRITIS) 78
Stiftung Wissenschaft und Politik (SWP) 79
Transferstelle IT-Sicherheit im Mittelstand (TISiM) 79
Universitäten der Bundeswehr (UniBw) 80
Verwaltungs-CERT-Verbund (VCV) 80
Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) 80
Zollkriminalamt (ZKA) 81

7. Erläuterung – Akteure auf Landesebene 82
Computer Emergency Response Teams der Bundesländer (Länder-CERTs) 82
Cyberabwehr Bayern 83

Cyber-Allianz-Zentrum (CAZ) – Bayern 83
Cyber-Competence-Center (CCC) – Brandenburg 83
Cyber Crime Competence Center Sachsen (SN4C) 84
Cyber Defense Center der Landesverwaltung Berlin (CDC-Lv) 84
Cybercrime Competence Center (4C) – Sachsen-Anhalt 84
Cybercrime-Kompetenzzentrum – Nordrhein-Westfalen 85
Cyberwehr – Baden-Württemberg 85
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken 85
Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern 86
Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz 86
Dezernat Cybercrime des Landeskriminalamtes Thüringen 86
Dezernat LPP 222 Cybercrime – Saarland 86
EMERGE IoT – Mecklenburg-Vorpommern 87
Fachkommissariat Cybercrime (LKA 54) – Hamburg 87
Hessen Cyber Competence Center (Hessen3C) 87
Informationssicherheitsbeauftragte:r der Landesverwaltung (Länder-CISO) 88
Kompetenz- und Forschungszentren für IT-Sicherheit (CISPA, ATHENE, KASTEL) 90
Kompetenzzentrum Cybercrime – Bayern 90
Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen 91
Landesamt für Sicherheit in der Informationstechnik Bayern (LSI) 91
Landesbeauftragte:r für Informationstechnologie (Länder-CIO) 91
Landesbehörden für Verfassungsschutz (LfV) 93
Netzverweis.de – Mecklenburg-Vorpommern 95
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock 95
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus 95
Sicherheitskooperation Cybercrime 96
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin 96
Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC) 96
Zentralstelle Cybercrime Bayern (ZCB) 96
Zentralstelle Cybercrime Sachsen (ZCS) 97
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität – Baden-Württemberg 97
Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) – Hessen 97
Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) 97

8. Erläuterung – Akteure auf Kommunalebene 99
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (Vitako) 99

IT-SiBe-Forum 99
Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt) 100
Kommunale Spitzenverbände (KSV) 100
Kommunalgremium des IT-Planungsrates 101

9. Gut zu wissen 102

1. Hintergrund

Der erste Grundstein für die deutsche Cybersicherheitsarchitektur wurde bereits 1986 gelegt. In diesem Jahr wurde in der Vorgängerorganisation des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Zentralstelle für das Chiffrierwesen (ZfCh), „[...] eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte“[1]. Am 1. Januar 1991 nahm das BSI nach Ausgründung aus dem Bundesnachrichtendienst (BND) seine Arbeit auf. In den öffentlichen Fokus geriet die staatliche Sicherheitsarchitektur dann insbesondere im Jahr 2011 durch die Veröffentlichung der ersten Cyber-Sicherheitsstrategie für Deutschland[2].

Seitdem hat sich einiges getan: Cybersicherheit ist für die Sicherheits- und Verteidigungspolitik in Deutschland ein elementarer Bestandteil geworden, weswegen viele neue nationale und internationale Akteure hinzugekommen, und Verknüpfungen zwischen ihnen entstanden, sind. Dennoch beinhaltete auch die aktualisierte Version der Cyber-Sicherheitsstrategie für Deutschland 2016[3] keine grafische oder anderweitige Übersicht über die immer komplexer werdende Architektur deutscher Behörden mit Aufgaben und Kompetenzen im Cyberraum. Von staatlicher Seite wurde erstmals im November 2020 durch das Bundesministerium des Innern, für Bau und Heimat (BMI) im Rahmen des Nationalen Pakts Cybersicherheit eine Auflistung von Akteuren und Initiativen im Bereich der Cybersicherheit aus Staat, Zivilgesellschaft, Wissenschaft und Wirtschaft als Online-Kompendium vorgelegt[4]. Wir hoffen mit unserer seit 2018 bestehenden Veröffentlichungsreihe dazu beigetragen zu haben, dass sich das BMI zu diesem Schritt entschlossen hat.

Für eine effektive und effiziente deutsche Aufstellung im Cyberraum bleibt, gerade auch vor dem Hintergrund begrenzter Ressourcen[5], eine strukturierte politische Herangehensweise unverzichtbar. Aus diesem Grund möchten wir im Rahmen unserer Arbeit zu Cybersicherheitspolitik[6] an der Stiftung Neue Verantwortung hierzu einen Beitrag leisten. In dieser Publikation stellen wir eine grafische Abbildung der staatlichen Cybersicherheitsarchitektur inklusive ihrer internationalen Schnittstellen, ein Abkürzungs- und Akteursverzeichnis, sowie eine Erklärung der Verbindungen einzelner Akteure vor. In der aktuellen Version wurden mit Aufnahme der kommunalen und NATO-Akteure zwei neue Bereiche eingezogen. Darüber hinaus wurden auf EU-, Bund- und Länderebene Aktualisierungen und Anpassungen vorgenommen und zusätzliche Akteure hinzugefügt.

1 Bundesamt für Sicherheit in der Informationstechnik, Jahresbericht 2003.
2 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2011.
3 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
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.

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. Weitere internationale Akteure wie die Vereinten Nationen (UN), rein legislative und judikative Akteure auf allen Ebenen, sowie Akteure aus Privatwirtschaft, Wissenschaft und Zivilgesellschaft wurden bisher nicht berücksichtigt. Am Ende dieser Veröffentlichung findet sich zusätzlich eine Seite mit wissenswerten Informationen rund im Cyber- und IT-Sicherheit in Deutschland.

Basis dieser Veröffentlichung bilden fast ausschließlich öffentlich verfügbare Informationen. Wir freuen uns daher über jeden Hinweis. Änderungs- und Ergänzungsvorschläge nimmt Christina Rupp gerne entgegen. Das Dokument wird auch künftig periodisch aktualisiert, um den neuesten Entwicklungsstand abzubilden und zusätzliche Erweiterungen vorzunehmen.

Für weitere Einblicke in die institutionelle deutsche Cybersicherheitslandschaft möchten wir in der nächsten Auflage (Veröffentlichung im September/Oktober 2021) einen Überblick über die Entwicklung der Cybersicherheitsarchitektur im Laufe der Zeit geben, sowie neue Möglichkeiten der Visualisierung nutzen.

Versionshistorie

Auflage	Datum	Co-Autor	Co-Autorin	Veröffentlichung
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	Vorliegende Version

STAATLICHE CYBERSICHERHEITSARCHITEKTUR

EUROPÄISCHE UNION

BUND

LÄNDER

KOMMUNEN

NATO

EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWP
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
Hybrid CoE
JISD
ESCD
NCIA
ACO
ACT
PESCO
Kooperations-gruppe unter der NIS-Richtlinie
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
CIDCC
CyCLONe
NIS Platform
SOG-IS
EGC Group
Gruppe der Inter-essenträger für die Cybersicherhe-itszertifizierung
SKI-Kontakt-gruppe
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BKA
BfV
BBK
BND
BfDI
BNetzA
ZKA
BaFin
ITZ Bund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
Cyber-agentur
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
Nationaler Pakt Cybersicherheit
Cyber Security Cluster Bonn
gematik
G4C
UP KRITIS
Initiative Wirtschaftsschutz
GMLZ
CODE
Kompetenz- & Forschungszentren für IT-Sicherheit
Initiative "IT-Sicherheit in der Wirtschaft
CERT-Verbund
ITSMIG
Bündnis für Cybersicherheit
ZITiS
Bw
BSI
Cyber-AZ
VCV
IT-PLR
IMK
Sicherheits-kooperation Cybercrime
BADEN-WÜRT-TEMBERG
BAYERN
BERLIN
BRANDEN-BURG
BREMEN
HAMBURG
HESSEN
MECKLEN-BURG-V.
NIEDER-SACHSEN
NRW
RHEIN-LAND-PFALZ
SAARLAND
SACHSEN
SACHSEN-ANHALT
SCHLESWIG-HOLSTEIN
THÜRINGEN
Länder-CIO
Länder-CISO
LfV Baden-Württemberg
ZAC Baden-Württemberg
CERT BWL
BSI-Verbind-ungsbüro Region Süd
Cyberwehr
Zentralstelle für die Bekämpfung von Informations- und Kommunika-tionskriminalität
Länder-CIO
Länder-CISO
LfV Bayern
ZAC Bayern
Bayern CERT
BSI-Verbind-ungsbüro Region Süd
CAZ
Cyberabwehr Bayern
LSI
Kompetenz-zentrum Cybercrime
ZCB
Länder-CIO
Landes-InfSiBe
LfV Berlin
ZAC Berlin
CDC-Lv
Berlin-CERT
BSI-Verbind-ungsbüro Berlin
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin
Länder-CIO
IT-Sicherheits manager
LfV Bran-denburg
ZAC Bran-denburg
CERT Bran-denburg
BSI-Verbind-ungsbüro Berlin
CCC
Schwerpunktstaatsan-waltschaft zur Bekämp-fung der Computer- und Datenrettskriminalität Cottbus
Länder-CIO
Länder-CISO
LfV Bremen
ZAC Bremen
CERT Nord
BSI-Verbind-ungsbüro Region Nord
Länder-CIO
Landes-InSiBe
LfV Hamburg
ZAC Hamburg
CERT Nord
BSI-Verbind-ungsbüro Region Nord
LKA 54
Länder-CIO
Länder-CISO
LfV Hessen
ZAC Hessen
CERT Hessen
BSI-Verbind-ungsbüro Region Rhein-Main
Hessen3C
ZIT
Länder-CIO
BeLVIS
LfV Mecklen-burg-Vorpo-mmern
ZAC Meck-lenburg-Vor-pommern
CERT M-V
BSI-Verbind-ungsbüro Region Nord
Dezernat Cybercrime des Landeskriminalam-tes Mecklen-burg-Vorpommern
Schwerpunktstaatsan-waltschaft für die Bekämpfung der Informa-tions-und Kommunika-tionskriminalität Rostock
EMERGE IoT
Netzver-weis.de
FITKO
Länder-CIO
Länder-CISO
LfV Nieder-sachsen
ZAC Nieder-sachsen
N CERT
BSI-Verbind-ungsbüro Region Nord
Länder-CIO
Länder-CISO
LfV NRW
ZAC Nordrhe-in-Westfalen
CERT NRW
BSI-Standort Region West (Bonn)
Cyber-crime-Kompe-tenzzentrum
ZAC NRW
Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen
Länder-CIO
CISO-rlp
LfV Rhein-land-Pfalz
ZAC Rhein-land-Pfalz
CERT-rlp
BSI-Verbind-ungsbüro Region Rhein-Main
Dezernat Cybercrime des Landeskriminalam-tes Rheinland-Pfalz
Länder-CIO
Länder-CISO
LfV Saarland
ZAC Saarland
CERT Saarland
BSI-Verbind-ungsbüro Region Rhein-Main
Dezernat LPP 222 Cyber-crime
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken
BSI-Drittstandort Saarland
Länder-CIO
BfIS
LfV Sachen
ZAC Sachen
SAX.CERT
BSI-Zweit-standort Region Ost
SN4C
ZCS
Länder-CIO
Landes-InSiBe
LfV Sachsen-Anhalt
ZAC Sachsen-Anhalt
CERT Nord
BSI-Verbind-ungsbüro Region Nord
4C
Länder-CIO
Länder-CISO
LfV Schleswig-Holstein
ZAC Schleswig-Holstein
CERT Nord
BSI-Verbind-ungsbüro Region Nord
Länder-CIO
Länder-CISO
LfV-Thüringen
ZAC Thüringen
Thüringen CERT
BSI-Zweit-standort Region Ost
Dezernat Cybercrime des Landeskriminalam-tes Thüringen
Kommun-algremium IT-PLR
KGSt
Kommunale Spitzenverbände
Vitako
IT-SiBe-Forum

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

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

Version: April 2021

3. Akteure und Abkürzungen

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 Pendants verwendet. Erläuterungen für alle hier genannten Akteure finden sich auf den jeweiligen Ebenen in alphabetischer Reihenfolge. Es ist darauf hinzuweisen, dass sich nicht alle erläuterten Akteure in der Visualisierung wiederfinden, da diese innerhalb der Darstellung anderer Akteure integriert sein können (Beispiel: CERT-Bund im BSI). Kursiv gedruckte Institutionen befinden sich entweder in der Planung oder im Aufbau.

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
4C	Cybercrime Competence Center – Sachsen-Anhalt
AA	Auswärtiges Amt
ACO	Allied Command Operations
ACS	Allianz für Cyber-Sicherheit
ACT	Allied Command Transformation
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKS	Bundesakademie für Sicherheitspolitik
BAMAD	Bundesamt für den Militärischen Abschirmdienst
Bayern CERT	Computer Emergency Response Team Bayern
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BeLVIS	Beauftragte:r für Informationssicherheit Mecklenburg-Vorpommern
Berlin-CERT	Computer Emergency Response Team Berlin
BfDI	Bundesbeauftragte:r für den Datenschutz und die Informationssicherheit
BfIS	Beauftragte:r für Informationssicherheit Sachsen

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BKAmt	Bundeskanzleramt
BKartA	Bundeskartellamt
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium für Finanzen
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bündnis für Cybersicherheit	Bündnis für Cybersicherheit
Bw	Bundeswehr
BWI	Bundesweite IT-Systemhaus GmbH
C3B	NATO Consultation, Control and Command Board
CAZ	Cyber-Allianz-Zentrum – Bayern

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
CCC	Cyber-Competence-Center Brandenburg
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CDC	NATO Cyber Defence Committee
CDC-Lv	Cyber Defense Center der Landesverwaltung Berlin
CDMB	NATO Cyber Defence Management Board
CEPOL	Europäische Polizeiakademie
CERT Brandenburg	Computer Emergency Response Team Brandenburg
CERT BWL	Computer Emergency Response Team Baden-Württemberg
CERT Hessen	Computer Emergency Response Team Hessen
CERT M-V	Computer Emergency Response Team Mecklenburg-Vorpommern
CERT Nord	Computer Emergency Response Team Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt
CERT NRW	Computer Emergency Response Team Nordrhein-Westfalen
CERT Saarland	Computer Emergency Response Team Saarland
CERT-Bund	Computer Emergency Response Team des Bundes
CERT-EU	Computer Emergency Response Team der Europäischen Kommission
CERT-rlp	Computer Emergency Response Team Rheinland-Pfalz
CERT-Verbund	Nationaler Verbund von Computer Emergency Response Teams
CIDCC	Cyber and Information Domain Coordination Centre
CIHBw	Cyber Innovation Hub
CISO-rlp	Informationssicherheitsbeauftragte:r der Landesverwaltung Rheinland-Pfalz
CIR	Organisationsbereich Cyber- und Informationsraum der Bundeswehr
CMPD	Direktion Krisenbewältigung und Planung

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
CODE	Forschungsinstitut Cyber Defence
Council	Rat der Europäischen Union
cPPP	Contractual Public-Private Partnership on Cybersecurity
CSIRTs Netzwerk	Computer Security Incident Response Teams Netzwerk
Cyber Security Cluster Bonn	Cyber Security Cluster Bonn e. V.
Cyberabwehr Bayern	Cyberabwehr Bayern
Cyberagentur	Agentur für Innovation in der Cybersicherheit GmbH
Cyber-AZ	Nationales Cyber-Abwehrzentrum
Cybercrime-Kompetenzzentrum	Cybercrime-Kompetenzzentrum – Nordrhein-Westfalen
Cyber-Reserve	Cyber-Reserve
Cyber-SR	Cyber-Sicherheitsrat
Cyberwehr	Cyberwehr – Baden-Württemberg
CyCLONe	Cyber Crisis Liaison Organisation Network
CyOC	NATO Cyberspace Operations Centre
DAkkS	Deutsche Akkreditierungsstelle
Dezernat Cybercrime der Staats-anwaltschaft Saarbrücken	Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken
Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern	Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern
Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz	Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz
Dezernat Cybercrime des Landeskriminalamtes Thüringen	Dezernat Cybercrime des Landeskriminalamtes Thüringen
Dezernat LPP 222	Dezernat LPP 222 Cybercrime – Saarland

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
DsiN	Deutschland sicher im Netz e. V.
EA	Europäische Kooperation für Akkreditierung
EAD	Europäischer Auswärtiger Dienst
EC3	Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität
ECCC	Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit
ECCG	Europäische Gruppe für die Cybersicherheitszertifizierung
ECSO	European Cybersecurity Organisation
ECTEG	European Cybercrime Training and Education Group
EDSB	Europäische:r Datenschutzbeauftragte:r
EGC group	European Government CERTs group
EJCN	European Judicial Cybercrime Network
EJN	European Judicial Network
EJTN	European Judicial Training Network
EK	Europäische Kommission
EMERGE IoT	EMERGE IoT – Mecklenburg-Vorpommern
ENISA	Agentur der Europäischen Union für Cybersicherheit
ENISA AG	ENISA-Beratungsgruppe
ER	Europäischer Rat
ERCC	Zentrum für die Koordination von Notfallmaßnahmen
ESCD	Emerging Security Challenges Division
ESVK	Europäisches Sicherheits- und Verteidigungskolleg
EU Hybrid Fusion Cell	EU-Analyseeinheit für hybride Bedrohungen

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
EUCTF	European Union Cybercrime Task Force
EUISS	Institut der Europäischen Union für Sicherheitsstudien
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht
EUMC	Militärausschuss der Europäischen Union
EUMS INT	Intelligence Directorate des EU-Militärstabs
Eurojust	Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen
Europol	Europäisches Polizeiamt
EVA	Europäische Verteidigungsagentur
FITKO	Föderale IT-Kooperation
G4C	G4C German Competence Centre against Cyber Crime e. V.
GD CONNECT	Generaldirektion Kommunikationsnetze, Inhalte und Technologien
GD DIGIT	Generaldirektion Informatik
GD HOME	Generaldirektion Migration und Inneres
GD JRC	Gemeinsame Forschungsstelle
GD RTD	Generaldirektion Forschung und Innovation
gematik	gematik
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
GLZ CIR	Gemeinsames Lagezentrum Cyber und Informationsraum
GMLZ	Gemeinsames Melde- und Lagezentrum
Gruppe der Interessenträger für die Cybersicherheitszertifizierung	*Gruppe der Interessenträger für die Cybersicherheitszertifizierung*
Hessen3C	Hessen Cyber Competence Centre
Horizon 2020	Horizon 2020

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
HWP	Horizontal Working Party on Cyber Issues
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
IMK	Innenministerkonferenz
Initiative IT-Sicherheit in der Wirtschaft	Initiative IT-Sicherheit in der Wirtschaft
Initiative Wirtschaftsschutz	Initiative Wirtschaftsschutz
InSiBe	Informationssicherheitsbeauftragte:r Hamburg
INTCEN	Zentrum für Informationsgewinnung und -analyse
ISG C3M	Inter-Service Group “Community Capacity in Crisis Management”
ISG CHT	Inter-Service Group “Countering Hybrid Threats”
IT-PLR	IT-Planungsrat
IT-Rat	IT-Rat
IT-SiBe-Forum	IT-SiBe-Forum
ITSMIG	IT Security made in Germany
ITZBund	Informationstechnikzentrum Bund
JISD	Joint Intelligence and Security Division
KdoCIR	Kommando Cyber- und Informationsraum
KdoITBw	Kommando Informationstechnik
KdoStratAufkl	Kommando Strategische Aufklärung
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsmanagement
Kommunalgremium IT-PLR	Kommunalgremium des IT-Planungsrates
Kompetenz- und Forschungs-zentren für IT-Sicherheit	Kompetenz- und Forschungszentren für IT-Sicherheit
Kompetenzzentrum Cybercrime	Kompetenzzentrum Cybercrime – Bayern

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
Kooperationsgruppe unter der NIS-Richtlinie NIS Cooperation Group	Kooperationsgruppe unter der NIS-Richtlinie NIS Cooperation Group
Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen	*Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen*
KSV	Kommunale Spitzenverbände
Landes-InfSiBe	Landesbeauftragte:r für Informationssicherheit Berlin
Länder-CERTs	Computer Emergency Response Teams der Bundesländer
Länder-CIO	Landesbeauftragte:r für Informationstechnologie
Länder-CISO	Informationssicherheitsbeauftragte:r der Länder
LfV	Landesbehörden für Verfassungsschutz
LKA 54	Fachkommissariat Cybercrime – Hamburg
LSI	Landesamt für Sicherheit in der Informationstechnik Bayern
LZ	Nationales IT-Lagezentrum
MC	NATO-Militärausschuss
MeliCERTes	MeliCERTes
NAC	Nordatlantikrat
Nationaler Pakt Cybersicherheit	Nationaler Pakt Cybersicherheit
N CERT	Computer Emergency Response Team Niedersachsen
NCI Academy	NCI Academy
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCSC	NATO Cyber Security Centre
Netzverweis.de	Netzverweis.de – Mecklenburg-Vorpommern
NIS Platform	NIS Public-Private Platform

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
NS-O	NATO School Oberammergau
OLAF	Europäisches Amt für Betrugsbekämpfung
PESCO	Ständige Strukturierte Zusammenarbeit
PSK	Politisches und Sicherheitspolitisches Komitee
SAX.CERT	Computer Emergency Response Team Sachsen
SC	NATO Security Committee
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus	Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus
Sicherheitskooperation Cybercrime	Sicherheitskooperation Cybercrime
SKI-Kontaktgruppe	Kontaktgruppe zum Schutz Kritischer Infrastrukturen
SN4C	Cyber Crime Competence Center Sachsen
SOG-IS	Senior Officials Group Information Systems Security
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin
SprinD	Agentur für Sprunginnovationen
SWP	Stiftung Wissenschaft und Politik
TF-CSIRT	Reference Incident Classification Taxonomy Task Force
TGG	Taxonomy Governance Group
Thüringen CERT	Computer Emergency Response Team Thüringen
TISiM	Transferstelle IT-Sicherheit im Mittelstand
UniBw	Universitäten der Bundeswehr

In Visualisierung verwendete Abkürzungen/Bezeichnungen	Name
UP KRITIS	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen
VCV	Verwaltungs-CERT-Verbund
Vitako	Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V.
vzbv	Bundesverband der Verbraucherzentralen und Verbraucherverbände e. V.
ZAC (Bundesland)	Zentrale Ansprechstellen Cybercrime der Polizeien der Länder für die Wirtschaft
ZAC NRW	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen
ZCB	Zentralstelle Cybercrime Bayern
ZCS	Zentralstelle Cybercrime Sachsen
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität
ZIT	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
ZKA	Zollkriminalamt

4. Erläuterung – Akteure auf EU-Ebene

Agentur der Europäischen Union für Cybersicherheit (ENISA)
ENISA 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 ergebenen 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 Cyberangriffen. Jährlich veröffentlicht die ENISA einen Bericht zur Bedrohungslage (ENISA Threat Landscape), der Gefahren aus dem Cyberraum identifiziert und bewertet.

ENISA arbeitet mit relevanten Behörden der Mitgliedstaaten und auf EU-Ebene, insbesondere den Computer Security Incident Response Teams, dem CERT-EU, 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. Auf deutscher Ebene arbeitet ENISA mit dem BSI/CERT-Bund zusammen. Kürzlich wurde ENISA von „European Network and Information Security Agency“ in „European Union Agency for Cybersecurity“ umbenannt. Die Abkürzung des ursprünglichen Namens blieb dabei erhalten[7].

7 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, ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

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 Ermittlungen herstellt, strafrechtliche Strategien entwickelt sowie gemeinsames Handeln, beispielsweise durch eine On-Call Koordination für Notfälle, ermöglicht. Um die Ermittlungsfähigkeiten der Strafverfolgungsbehörden der Mitgliedsstaaten im Bereich Cyberkriminalität, das Verständnis für Cyberkriminalität und Ermittlungsoptionen der Strafverfolger und der Justiz zu stärken, *arbeitet Eurojust mit spezialisierten Beratergruppen des EC3, Netzwerken der Chefs:innen der Cyberkriminalitätseinheiten sowie auf Cyberkriminalität spezialisierten Strafverfolger:innen zusammen. Beziehungen zwischen Eurojust und nationalen Behörden, dem EJN, Europol, Frontex, dem Zentrum für Informationsgewinnung und -analyse und Drittstaaten sollen gefördert werden*[8].

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. Europäische Kommission und Generalsekretariat des Rates). Es arbeitet eng mit anderen Computer Emergency Response Teams (CERTs) in den Mitgliedsstaaten zusammen und ist Mitglied des CSIRTs Netzwerks. Kürzlich wurde eine strukturierte Zusammenarbeit zwischen CERT-EU und der ENISA vereinbart. CERT-EU und die NATO Computer Incident Response Capability (NCIRC) haben in der Vergangenheit eine technische Vereinbarung zur Zusammenarbeit beschlossen[9].

8 Bundesamt für Sicherheit in der Informationstechnik, Avalanche-Botnetz: BSI weitete Schutzmaßnahmen aus. (Webseite entfernt)
Eurojust, Casework at Eurojust.
Eurojust, Eurojust Decision.
Europäische Kommission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

9 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.

Contractual Public Private Partnership on Cybersecurity (cPPP)
Im Rahmen der Cybersicherheitsstrategie der EU wurde eine cPPP zwischen der Europäischen Kommission und der European Cyber Security Organisation unterzeichnet. Das Ziel der cPPP ist es, die Kooperation zwischen öffentlichen und privaten Akteuren in frühen Forschungs- und Innovationsstadien zu fördern, um innovative und vertrauenswürdige europäische Lösungen zu schaffen. Diese Lösungen sollen dabei fundamentale Rechte, insbesondere Privatsphäre, berücksichtigen. Außerdem soll die Cybersicherheitsindustrie gefördert werden.

Die EU wird bis zu 450 Mio. Euro unter dem Schirm des Programms Horizon 2020 investieren[10].

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 setzt sich aus Repräsentanten:innen der ernannten CSIRTs der Mitgliedsstaaten sowie des CERT-EU zusammen. Für Deutschland übernimmt diese Funktion das CERT-Bund. Die Europäische Kommission 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[11].

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 2020 das Cyber Crisis Liasion Organisation Network (CyCLONe) ins Leben gerufen. Durch verstärkte Kooperationsmechanismen und verbesserten Informationsfluss zwischen 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. Derzeit ist CyCLONE noch nicht einsatzbereit und eine Mitgliedschaft beruht für EU-Mitgliedstaaten auf rein freiwilliger Basis.

10 ECSO, About the cPPP.
11 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.
European Union Agency for Cybersecurity, CSIRTs Network.

Die Idee für ein solches Netzwerk, welches von der Europäischen Kommission 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[12].

Cyber and Information Domain Coordination Centre (CIDCC)

Die Initiative für ein Cyber and Information Domain Coordination Centre (CIDCC) wurde von Deutschland als ein Projekt im Rahmen der Ständigen Strukturierten Zusammenarbeit (PESCO) eingebracht. Neben Deutschland, welches durch sein Kommando CIR die Rolle des Koordinators übernimmt, sind die Niederlande, Ungarn und Spanien am Aufbau des CIDCC beteiligt. Auf lange Sicht soll das CIDCC als ständiges multinationales militärisches Element etabliert werden, in dem u. a. 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 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 beim Kommando CIR angesiedelt sein.

In seiner Konzeption des CIDCC hat sich das Kommando CIR mit dem Militärstab der Europäischen Union (EUMS) sowie der Europäischen Verteidigungsagentur (EVA) abgestimmt[13].

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.

Diese Optionen werden in sogenannten Crisis Management Concepts zusammengefasst und den EU-Minister:innen vorgelegt. Sie bilden die Grundlage für operationale Planungen und die Durchführung von Missionen[14].

12 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.
European Union Agency for Cybersecurity, Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe).
Vertretung der Europäischen Kommission in Deutschland, EU-Staaten testen ihre Zusammenarbeit im Falle von Cyber-Angriffen.

13 Bundesministerium der Verteidigung, Cyber and Information Domain Coordination Centre (CIDCCC).
Bundeswehr, Europäisches Verteidigungsprojekt für Cybersicherheit – Das Cyber and Information Domain Coordination Centre.
PESCO, Cyber and Information Domain Coordination Center (CIDCC).

14 European Union External Action Service, The Crisis Management and Planning Directorate (CMPD). (Webseite entfernt)

ENISA-Beratungsgruppe (ENISA AG)
Mit dem Cybersecurity Act wurde eine ENISA-Beratungsgruppe eingesetzt, die sich aus anerkannten Expert:innen 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 Kommission 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. 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[15].

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 ist innerhalb des EU Intelligence and Situation Centre (INTCEN) des Europäischen Auswärtigen Dienstes angesiedelt. Die Analyseeinheit 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 u. a. Best Practices auszutauschen, Resilienz zu stärken sowie Gegeninitiativen zu hybriden Bedrohungen zu formulieren.

Die Analyseeinheit arbeitet eng mit dem Intelligence Directorate des EU-Militärstabes 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

15 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).

Branch innerhalb der JISD sowie dem NATO CCDCOE[16]*.*

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 arbeitet eng mit den Mitgliedstaaten sowie auf EU-Ebene mit dem:der Europäischen Datenschutzbeauftragte:n, der Frontex, dem Rat der EU, der EK, der ENISA, Eurojust und Europol zusammen[17]*.*

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 Gruppe der Interessenträger für die Cybersicherheitszertifizierung 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[18]*.*

16 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.

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

18 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).

Europäische Kommission (EK)
Die Europäische Kommission nimmt eine strategisch-organisatorische Rolle in der EU-Cybersicherheitsarchitektur ein. Sie ist dafür zuständig, Kapazitäten und Kooperation 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), dass ein internes Kommunikationsnetz und ein spezifische Koordinierungsverfahren umfasst. Im Falle einer schweren, EU-weiten Krise, die den Cyberbereich betrifft, erfolgt die Koordinierung bei der Kommission via ARGUS.

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. 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[19].

Europäische Kooperation für Akkreditierung (EA)
Die Europäische Kooperation für Akkreditierung ist der Zusammenschluss von europäischen Akkreditierungsstellen und ist für die Koordination der Akkreditierung in Europa zuständig. Sie ist eine gemeinnützige Vereinigung und besteht aus 50 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 Europäischen Kommission offiziell benannt worden, die EK sitzt zudem im Aufsichtsrat der EA. Die DAkkS ist Mitglied in der EA und repräsentiert deutsche Interessen[20].

Europäische Polizeiakademie (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 da-

19 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”.
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.
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.

20 DAkkS, Europäischer Rechtsrahmen.
European Accreditation, EA Advisory Board.
European Accreditation, Relations with European Commission. European Accreditation, Who are we?.

bei, Trainings zu Prioritäten im Sicherheitsbereich, zu Strafverfolgungskooperation und Informationsaustausch anzubieten. Hierzu wurde u. a. 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, der ECTEG und Interpol erarbeitet und durchgeführt[21].

Europäische Verteidigungsagentur (EVA)
Die Europäische Verteidigungsagentur unterstützt alle EU-Mitgliedstaaten (außer Dänemark) bei der Entwicklung kooperativer europäischer Verteidigungsprojekte. Ein Ziel der EVA ist der Ausbau der Cyberabwehrfähigkeit. Sie unterstützt Mitgliedstaaten bei der Entwicklung eigener Abwehrfähigkeiten – Cyber Defence zählt hierbei dabei zu ihren vier Kernprogrammen.

Für die Ständige Strukturierte Zusammenarbeit (PESCO) führt sie gemeinsam mit dem EAD alle Sekretariatsfunktionen. Mit ENISA, dem EC3 und CERT-EU besteht ein Memorandum of Understanding, mit dem Ziel einen Kooperationsrahmen für die Organisationen zu entwickeln. Der:die Chief Executive der EVA kommt zu regelmäßigen Treffen mit dem:der SACT sowie Assistant SECGEN's der NATO zusammen. Das Steering Board der EVA wird zudem regelmäßig durch letztere gebrieft[22].

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:r 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.

21 CEPOL, About us.
CEPOL, CEPOL Cybercrime Academy Inaugurated.
Emailaustausch mit CEPOL-Verterter:innen im August 2019.

22 Die Europäische Union, Europäische Verteidigungsagentur (EVA).
European Defence Agency, Four EU cybersecurity organisations enhance cooperation.
European Defence Agency, Our current priorities.
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 Councils on 6 December 2016 and 5 December 2017.

Der EAD beherbergt EUMS INT, INTCEN und die dort untergebrachte EU Hybrid Fusion Cell. Zudem ist dort das CMPD angegliedert. Vertreter:innen des EAD haben den Vorsitz im PSK inne. 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[23].

Europäische:r Datenschutzbeauftragte:r (EDSB)

Die:der Europäische Datenschutzbeauftragte:r übernimmt diese Funktion innerhalb der Europäischen Union. Er:sie 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 Untersuchung oder die Bearbeitung eingereichter 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 u. a. zur Cybersicherheitsstrategie der EU, sowie 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 des:der BfDI[24].

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.

23 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”.
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/Vice President.
EU-NATO, Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016and 5 December 2017.
IMPETUS, An Integral Element of the EU Comprehensive Approach.

24 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 Europäischen Kommission 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 teil[25].

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 Europäischen Kommission unterstellt, aber in der Ausführung seines Mandates unabhängig. Der Arbeitsgruppe des Rates der Europäischen Union zur Betrugsbekämpfung erstattet OLAF regelmäßig Bericht[26].

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. Dabei arbeitet Europol auch mit Nicht-EU-Mitgliedstaaten und internationalen Organisationen zusammen.

Im Bereich Cyberkriminalität stärkt Europol insbesondere die Strafverfolgung durch das European Cybercrime Centre (EC3). Europol arbeitet eng mit dem BKA zusammen. Das BKA dient Europol als Nationale Stelle und ist somit deutscher Ansprechpartner für Europol[27].

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 Schwerpunktberei-

25 Europäischer Rat, A New Strategic Agenda 2019–2024.
Europäischer Rat, Der Europäische Rat.
26 Europäisches Amt für Betrugsbekämpfung, About Us.
Europäisches Amt für Betrugsbekämpfung, Cooperation with EU institutions.
27 Bundeskriminalamt, Europol.
Europol, About Europol.
Europol, European Cybercrime Centre – EC3.

chen 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. Enger 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 u. a. AA, BAKS und BMVg an diesem Netzwerk[28].

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

Im Dezember 2020 haben die EU-Mitgliedstaaten für die rumänische Hauptstadt Bukarest als Standort des neu zu errichtenden Europäischen Zentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit gestimmt. Das ECCC 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, sollen die vorhandenen Mittel für Cybersicherheit innerhalb der Europäischen Union sowie Investitionen gezielt gebündelt (Förderprogramme Horizont Europa sowie Digitales Europa) und Forschungsvorhaben in der EU im Bereich der Cybersicherheit koordiniert werden. Das Zentrum soll außerdem ein Netzwerk nationaler Koordinierungszentren und die Cybersecurity Competence Community aufbauen und koordinieren.

Das ECCC basiert auf einem Vorschlag der EK und soll die Aufgaben der ENISA ergänzen[29].

Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität (EC3)

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Europol soll die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU

28 ESVK, EAB.Cyber.
ESVK, Education & Training.
ESVK, Institutes.
ESVK, Who We Are.

29 Europäische Kommission, European Cybersecurity Industrial, Technology and Research Competence Centre.
Rat der Europäischen Union, New Cybersecurity Competence Centre and network: informal agreement with the European Parliament.
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.
Rat der Europäischen Union, Bukarest (Rumänien) wird Sitz des neuen Europäischen Kompetenzzentrums für Cybersicherheit.
Rat der Europäischen Union, Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.
Netzpolitik, Neues EU-Kompetenzzentrum für Cybersicherheit bleibt umstritten.

verstärken. Das EC3 ist im Kampf gegen Cyberkriminalität in drei Bereichen tätig: Forensik, Strategie 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.

Partner auf europäischer Ebene sind CERT-EU, CEPOL, Eurojust, ENISA, die Europäische Kommission, sowie die ECTEG. Außerdem stellt das EC3 gemeinsam mit dem CERT-EU forensische Analysen und andere technische Informationen für das CSIRTs Netzwerk bereit[30].

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.

Die Idee der Einrichtung des Hybrid CoE wurde sowohl vom Rat der EU als auch dem NAC befürwortet. Zusammen mit dem JRC der Europäischen Kommission hat Hybrid CoE Ende 2020 einen konzeptionellen Rahmen zu hybriden Bedrohungen vorgestellt. In der Vergangenheit haben Hybrid CoE und die Europäische Verteidigungsagentur eine Zusammenarbeit als Beitrag zur Umsetzung der Prioritäten aus dem Capability Development Plan der EU vereinbart. Deutschland ist als eine der neun Gründungsnationen am Hybrid CoE beteiligt[31].

European Cybercrime Training and Education Group (ECTEG)
Das ECTEG setzt sich aus Strafverfolgungsbehörden der Mitgliedstaaten sowie Mitgliedsstaaten des Europäischen Wirtschaftsraums, internationalen Institutionen,

30 Europol, Cybercrime.
Europol, European Cybercrime Center – EC3.
Europol, EC3 Partners.
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.

31 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.

der Wissenschaft, der privaten Industrie und Experten zusammen. Finanziert wird die Gruppe von der Europäischen Kommission. Ihr Ziel ist es, die globale Strafverfolgung von Cyberkriminalitätsvorfällen vorzubereiten.

Sie arbeitet in enger Abstimmung mit dem EC3 und CEPOL zusammen, um Cyberkriminalitätstrainings grenzübergreifend zu harmonisieren, Wissensaustausch zu ermöglichen, sowie eine Standardisierung von Methoden für Trainingsprogramme voranzubringen. Aus Deutschland sind die Polizeiakademie Hessen und die Albstadt-Sigmaringen Universität beteiligt[32].

European Cyber Security Organisation (ECSO)
Die European Cyber Security Organisation wurde in Belgien als gemeinnützige Organisation 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 sowie Staaten, die mit Horizon 2020 in Verbindung stehen. 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 Vertragspartner der Europäischen Kommission und ist in dieser Funktion für die Implementierung der öffentlich-privaten Partnerschaft für Cybersicherheit (cPPP) zuständig. ECSO unterhält enge 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 Horizontal Working Party on Cyber Issues Bericht zu erstatten. Kontinuierliche Kooperationen bestehen zudem u. a. mit der ENISA, Europol sowie der EVA[33].

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 Entwicklung als auch Wissen in Spezialgebieten zur gemeinsamen Nutzung. Darüber hinaus ist der EGC group die Erleichterung des Informations- und Technologieaustauschs u. a. im Bereich von Schwachstellen ein Anliegen. Dabei verfolgt die Gruppe,

32 ECTEG, European Cybercrime Training and Education Group.
ECTEG, Members.
33 ECS, About ECSO.

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 der CERT-Bund. Darüber hinaus besteht eine enge Kooperation mit der ENISA[34].

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 European Judicial Cybercrime Network[35].

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[36].

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

Es arbeitete im Bereich Cybersicherheit mit CEPOL an den dort angebotenen Trainings[37].

34 Bundesamt für Sicherheit in der Informationstechnik, Europäische CERTs in Bonn. (Webseite entfernt)
EGC Group, Contact.
EGC Group, European Government CERTs (EGC) group.
35 European Judicial Network, About EJN.
European Judicial Network, Network Atlas.
36 Eurojust, European Judicial Cybercrime Network.
37 Emailaustausch mit CEPOL-Verterter:innen im August 2019.
EJTN, About us.

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 Europol, der EK und Eurojust. Gemeinsam mit CEPOL, Eurojust und GD Home werden bei den Treffen Herausforderungen und Aktionen im Kampf gegen Cyberkriminalität identifiziert, diskutiert und priorisiert[38].

Gemeinsame Forschungsstelle (GD JRC)
Die Gemeinsame Forschungsstelle ist der Europäischen Kommission unterstellt und wird durch Horizon 2020 finanziert. Die JRC stellt nationalen Behörden als auch Behörden der EU wissenschaftliche Erkenntnisse, sowie innovative Instrumente während des gesamten Politikzyklus bereit. Dabei möchte es aufkommende Herausforderungen antizipieren, sowie 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[39].

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.

Darüber hinaus ist die GD RTD für das Management von Förderprogrammen wie Horizon 2020 verantwortlich. In der Erfüllung seiner Aufgaben arbeitet GD RTD u. a. eng mit GD CONNECT, GD HOME und GD JRC zusammen[40].

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

38 Europol, EUCTF.
39 EU Science Hub, Information Society.
EU Science Hub, JRC in brief.
EU Science Hub, Organisation.
EU Science Hub, Research Topics.
40 Europäische Kommission, Strategic Plan 2016-2020: Directorate-General for Research and Innovation.

EU-Institutionen bei der täglichen Arbeit unterstützt und 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 DG DIGIT die Europäische Kommission im Management sowie Executive Board der ENISA[41].

Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD CONNECT)
Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien ist verantwortlich für die Entwicklung des digitalen Binnenmarktes. Damit einhergehend arbeitet GD CONNECT auch an der Entwicklung von europäischem Führungspotential im Bereich Netzwerk- und IT-Sicherheit.

GD CONNECT trägt die „parent-DG responsibility" für ENISA, übernimmt die Repräsentation auf Generaldirektions-Ebene im CERT-EU Board und trägt auf dieser Ebene zur Antwort auf Cybervorfälle bei. Für Forschungs- und Innovationsaktivitäten mit IKT-Bezug im Rahmen von Horizon 2020 verantwortet GD CONNECT sämtliche strategischen Belange. Enge Arbeitsbeziehungen bestehen mit GD RTD. Der Vorschlag zur Einrichtung des ECCC seitens der Europäischen Kommission wurde von GD CONNECT vorbereitet[42].

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 (v. a. Europol und Frontex) ausgetauscht. Enge Arbeitsbeziehungen bestehen u. a. mit eu-LISA, Europol sowie CEPOL[43].

41 Europäische Kommission, Annual Activity Report: DG CONNECT.
Europäische Kommission, Informatics.
Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
42 Europäische Kommission, Annual Activity Report: DG CONNECT.
Europäische Kommission, Communication Networks, Content and Technology.
Europäische Kommission, Strategic Plan 2016-2020: Directorate-General for Communications Networks, Content and Technology.
43 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
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 Arbeitsprogramm 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 Kommission und der ENISA gemeinsam inne. Die Sekretariatsfunktionen werden von der ENISA wahrgenommen[44].

Horizon 2020
Horizon 2020 ist ein Forschungs- und Innovationsprogramm der Europäischen Kommission, das knapp 80 Milliarden Euro über sieben Jahre hinweg bereitstellt. Es ist somit das finanzielle Instrument der Initiative 'Innovation Union' und zielt darauf ab, Europas Konkurrenzfähigkeit zu stärken. Unter dem Schirm von Horizon 2020 können auch Projekte im Bereich Cybersicherheit gefördert werden.

Eine koordinierende Geschäftsstelle, sowie eine Erstinformationsstelle stehen Interessierten beim BMBF zur Verfügung. GD RTD verantwortet das gesamte Management von Horizon 2020. GD CONNECT obliegt die strategische Ausgestaltung bei Forschungsaktivitäten mit IKT-Bezug[45].

Horizontal Working Party on Cyber Issues (HWP)
Die Horizontal Working Party on Cyber Issues 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.

44 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).
45 Bundesministerium für Bildung und Forschung, Netzwerk der Nationalen Kontaktstellen.
European Commission, Security.
European Commission, What Is Horizon 2020?.

Die Arbeitsgruppe arbeitet mit der Europäischen Kommission, EAD, Europol, Eurojust, EVA und ENISA zusammen und steht zudem in einem engen Austausch mit anderen Arbeitsgruppen. An der HWP beteiligt sich Deutschland durch Vertreter:innen des federführenden BMI sowie des AA[46].

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 zur Entscheidungsfindung in diesem Bereich 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 Europäischen Union etabliert und arbeitet beispielsweise mit der EK, dem Europäischen Parlament, dem EAD und Regierungen der EU-Mitgliedsstaaten zusammen[47].

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 eingestuften 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.

EUMS INT arbeitet eng 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, dem Eurokorps, sowie dem deutschen militärischen Vertreter bei der Europäischen Union zur Verfügung[48].

46 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheit in Europa gestalten. (Webseite entfernt)
Europäischer Rat, Horizontal Working Party on Cyber Issues (HWP).
The Council of the European Union, Establishment of a Horizontal Working Group on Cyber Issues.

47 EUR-Lex, Document 32001E0554.
EUR-Lex, Institut der Europäischen Union für Sicherheitsstudien.
Europäische Union, Institut der Europäischen Union für Sicherheitsstudien (EUISS).
European Union Institute for Security Studies, Cyber.

48 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.

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 beteiligt[49].

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.

Den Vorsitz der ISG CHT haben sowohl Repräsentant:innen des EAD als auch der Kommission auf Director General- bzw. Deputy Secretary-General-Ebene inne. Die ISG CHT erhält quartalsweise Berichte der EU Hybrid Fusion Cell[50].

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 Schutz Kritischer Infrastrukturen (EPSKI) zuständig. Dieses identifiziert, europäische Kritische Infrastrukturen, sowie 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 koordiniert[51].

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

49 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats “EU Playbook”.
50 Ebd.
Kristine Berzina et al., European Policy Blueprint for Countering Authoritarian Interference In Democracies: Annex A. European Efforts To Counter Disinformation.
51 Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection.

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 u. a. 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 u. a. die Cybersicherheitsübung Blue OLEx (deutsche Beteiligung durch BMI und BSI) sowie das Cyber Crisis Liasion Organisation Network (CyCLONe) zurück[52].

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.

Die ENISA ist verantwortlich für die Durchführung und Bereitstellung zentraler Aspekte der MeliCERTes Anlage[53].

Militärausschuss der Europäischen Union (EUMC)

Der Militärauschuss 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 Ver-

52 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.

53 Europäische Kommission, A call for tender to advance MeliCERTes, the facility used by the CSIRTs in the EU to cooperate and exchange information.
Europäische Kommission, Tools and capacity building for better cyberspace monitoring, analysis and threat detection for Lithuania and EU.

teidigungsfragen 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 Europäischen Union 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 werden[54].

NIS Public-Private Platform (NIS Platform)
Die NIS Plattform wurde mit der Cybersicherheitsstrategie der EU geschaffen und hat das Ziel, die Resilienz von Netzwerken und Informationssystemen, auf denen die Dienstleistungen von Privatunternehmen und öffentlichen Verwaltungen basieren, zu erhöhen. Außerdem gehört es zu ihren Aufgaben, bei der Implementierung der Maßnahmen der Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit zu unterstützen und Best Practices zu identifizieren.

In der Vergangenheit wurden Ergebnisse der NIS Platform von der EK für ihre Empfehlungen zur Cybersicherheit berücksichtigt[55].

Politisches und Sicherheitspolitisches Komitee (PSK)
Das Politische und Sicherheitspolitische Komitee ist für die Gemeinsame Außen- und Sicherheitspolitik der EU (GASP) zuständig. Es setzt sich aus den Botschafter:innen der Mitgliedstaaten in Brüssel bzw. Vertreter:innen der Außenministerien zusammen. 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.

Vertreter:innen des Europäischen Auswärtigen Dienstes haben den Vorsitz im PSK inne. Dem Rat der EU kann das PSK Empfehlungen zu strategischen Konzepten sowie politischen Optionen aussprechen. 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 dem:der SACTEUR[56].

54 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).
55 ENISA, NIS Platform.
56 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.

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 Auswärtigen 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, sowie zur Vorbereitung der Zusammenkünfte der Minister eingerichtet, wozu auch die Horizontale Arbeitsgruppe „Fragen des Cyberraums" (HWP) 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 Europäische Kommission mit der Verhandlung internationaler Abkommen beauftragen, über dessen Abschluss der Rat basierend auf einem Vorschlag der EK entscheidet. Der:die Hohe Vertreter:in der Union für Außen- und Sicherheitspolitik übernimmt den Vorsitz der Ratskonstellation zu Auswärtigen Angelegenheiten (FAC). 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, Frontex, CEPOL oder andere einschlägige Gremien eingeladen werden[57].

57 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.

Reference Incident Classification Taxonomy Task Force (TF-CSIRT)
Die Reference Incident Classification Taxonomy Task Force hat sich die Erstellung eines Referenzdokuments zur Entwicklung eines Mechanismus für Updates und Versionierung, die Verwaltung des Referenzdokuments, sowie die Organisation persönlicher Meetings der Stakeholder zum Ziel gesetzt.

Mitglieder der Taskforce sind Mitglieder europäischer CSIRTs. Darunter befinden sich auch das CERT-Bund sowie die Common Taxonomy Governance Group (inkl. Vertreter:innen der ENISA und EC3)[58].

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.

Deutsches Mitglied ist das BSI[59].

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.

Der Europäische Auswärtige Dienst (inkl. EUMS) sowie die Europäische Verteidigungsagentur bilden das PESCO-Sekretariat. Als Teil von PESCO-Projektpaketen wurde u. a. das CIDCC geschaffen[60].

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.

58 ENISA, Building a common language to face future incidents – ENISA and European CSIRTs establish a dedicated task force.
ENISA, Reference Incident Classification Taxonomy.
59 SOGIS, Introduction.
60 EEAS, Ständige Strukturierte Zusammenarbeit – SSZ.
PESCO, About PESCO.
PESCO, PESCO Secretariat.
Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018).

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 European Crime Task Force (EUCTF), das CERT-EU sowie ausgewählte CSIRTs durch jeweilige Fachexpert:innen[61].

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".

Es verantwortet das Krisenmanagement der Kommission und bildet den 24/7-verfügbaren Kontaktpunkt für die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR)[62].

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.

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,

61 Europol, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.
Rossella Mattioli und Yonas Leguesse, Reference Incident Classification Taxonomy Task Force Update.
62 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".

das BMVg, das BAMAD, das BMI und den BfV sowie themenbezogen auch an weitere Stellen. INTCENT-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 Intelligence Directorate des EU-Militärstabes bildet INTCEN die Single Intelligence Analysis Capacity (SIAC). 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 wird[63].

63 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.

5. Erläuterung – Akteure auf NATO-Ebene

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 operationeller 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. Gemeinsam mit dem SECGEN hat der SACEUR bereits an Briefings seitens der NATO gegenüber dem PSK der EU teilgenommen[64].

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 u. a. Übungen im Cyberbereich, wie die jährliche NATO Cyber Coalition Exercise, vorbereitet.

An der NATO Cyber Coalition Exercise, die mit Unterstützung des NATO-Militärausschusses durchgeführt wird, nimmt die Bundeswehr teil. In Besuchsfunktion ist auch die ENISA vertreten. 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

64 NATO, Allied Command Operation.
NATO Public Diplomacy Division, Allied Command Operations.
SHAPE, Allied Command Operations overview: An introduction to the organisation and responsibilities.

ACT unterstellten NATO School Oberammergau. Es kommt zu regelmäßigen Treffen zwischen dem SACT und dem Chief Executive der EVA[65].

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 Cyber Defence Management Board (CDMB) hat gegenüber dem CDC eine Berichtspflicht. Beispielsweise im Falle eines schweren Cybersicherheitsvorfalls kann das CDC die Situation zur weiteren Befassung an den Nordatlantikrat verweisen. Der:die deutsche Vertreter:in im CDC erhält eine von AA, BMI und BMVg abgestimmte Weisung, das BSI ist in den Weisungsgebungsprozess beratend eingebunden[66].

Emerging Security Challenges Division (ESCD)
Die Emerging Security Challenges Division ist organisatorisch innerhalb des NATO International Staff (IS) angesiedelt. Die ESCD soll u. a. 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 und verantwortet auch das NATO Science for Peace and Security Programme (SPS), sowie die Strategic Analysis Capability. Neben Abteilungen zu Innovation, Datenpolitik, Terrorismusbekämpfung, sowie hybriden Herausforderungen und Energiesicherheit verfügt die ESCD auch über eine dezidierte Abteilung für Cyberverteidigung/-abwehr. Als ziviler Counterpart zu der Befassung aus militärischer Perspektive innerhalb von SHAPE (ACO), koordiniert die ESCD Anstrengungen zum Schutz der NATO-Netzwerke gegen Cyberangriffe, unterstützt Bündnispartner bei der Stärkung ihrer Resilienz und entwickelt cyberverteidigungspolitische Kooperationen und Partnerschaften. Darüber hinaus verfügt die ESCD über eine Cyber Threat Assesment 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 NATO Cyber Defence Management Board. Ihre Cyber Thre-

65 Allied Command Transformation, Who We Are.
NATO, Cyber defence.
66 Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.
NATO, Cyber defence.
NATO CCDCOE, North Atlantic Treaty Organization.

at Assesment Cell operiert in engem 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 geschlossen[67]*.*

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 Akteure parallel eine koordinierte Bewertung der Sicherheitslandschaft vor, um zu einer einheitlichen Betrachtung der Bedrohungslage beizutragen[68]*.*

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 u. a. 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 beispielsweise 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 ständi-

67 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.

68 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.

gem Austausch mit dem CyOC, an das es Statusupdates zu den NATO-Netzwerken übermittelt und auf dessen operative Anweisungen es bei Cybersicherheitsvorfällen reagiert. 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 statt[69].

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.

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 Cyberbereich[70].

NATO Computer Incident Response Capability (NCIRC)

Die der NCIA unterstellte NATO Computer Incident Response Capability verfügt organisatorisch über ein Technical (NCIRC TC), sowie Coordination Centre (NCIRC CC), die bei SHAPE ansässig sind. Beide sollen sämtliche NATO-eigenen Netzwerke im Alltag und rund um die Uhr vor Angriffen 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 Angriffs 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.

69 Don Lewis, What is NATO Really Doing in Cyberspace?.
NATO, Cyber defence.
NCIA, Who we are.

70 NCIA, About the NCI Academy.
NCIA, Introducing the NCI Academy.
NCIA, 10,000 Cyber Defenders: Cyber education for the NATO-EU workforce.

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 teil[71].

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, sowie 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 International 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, ESVK und dem CODE der Universität der Bundeswehr. Als eine von sieben Gründungsnationen des CCDCOE stellt derzeit Deutschland derzeit den Deputy Director und beteiligt sich durch Bw- und BMVg-Vertreter:innen an Locked Shields[72].

71 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.

72 Hintergrundgespräch, 2021.
NATO CCDCOE, About Us.
NATO CCDCOE, Training.
NATO CCDCOE, Research.
Rat der EU, EU Cyber Defence Policy Framework.

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 Headquarters C3 Staff (NHQC3S), einer gemeinsamen Einheit des Internationalen Militärstabes und International Staff, unterstützt.

An dem C3B nehmen neben nationalen Repräsentant:innen, Vertreter:innen des Militärausschusses, ACT sowie ACO teil. Von deutscher Seite wird diese Funktion federführend vom BMVg wahrgenommen. Im untergeordneten Information Assurance and Cyber Defence Capability Panel sind BMVg und BSI vertreten[73].

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, u. a. ACO, ACT und NCIA, zusammen[74].

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

73 NATO, Consultation, Command and Control Board (C3B).
NATO, Cyber defence.
74 Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.
NATO, Cyber defence.

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.

Dem NCSC untersteht die NCIRC. Informationsaustausch und enge Arbeitsbeziehungen bestehen mit dem CyOC, welche auch durch die gemeinsame Ansässigkeit bei SHAPE gefördert werden[75].

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 u. a. über Verbindungselemente zu regionalen Kommandos des ACO verfügen.

Zur Lageerkennung ist das CyOC auf nachrichtendienstliche Informationen der Bündnisstaaten angewiesen und wird in seiner Aufgabenerfüllung u. a. durch die Cyber Threat Assesment Cell (CTAC) der ESCD im NATO HQ sowie NCIRC unterstützt. CyOC ist dem DCOS Cyberspace im ACO unterstellt und bei SHAPE in Belgien angesiedelt[76].

NATO-Militärauschuss (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 Cyberangriffe 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 Representänt: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.

75 NCIA, Securing the Cloud.
NCIA, What We Do: NATO's Cybersecurity Centre.
NICP, Objectives and Principles.
76 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.

Deutschland wird durch Vertreter:innen der Bw im MC repräsentiert. Der MC kommt regelmäßig zu Treffen mit seinem Counterpart in der EU, dem EUMC, zusammen[77].

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 Angriffe zu schützen. Hierzu hat die NS-O auch (gemeinsam mit der Naval Postgraduate School (NPS)) ein Cyber Security Certificate Programme ins Leben gerufen.

Die Ausbildung an der NS-O im Bereich der Cybersicherheit und Cyberverteidigung wird durch das CCDCOE koordiniert[78].

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, u. a. 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 werden[79].

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, sowie halbjährlich auf Ebene der Außen- und

77 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.
78 NATO School, NATO School Oberammergau – Naval Postgraduate School Cyber Security Professional Programme Closure in Morocco.
NATO School, Organization.
79 NATO, Security Committee (SC).

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 oder Angriffes 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. 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. 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 teilgenommen[80].

80 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.

6. Erläuterung – Akteure auf Bundesebene

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. Die Cyberagentur bildet gemeinsam mit der SprinD ein Ökosystem, das vielversprechende Ideen und Innovationen identifizieren, fördern und entwickeln soll. Beide sind als Initiativen der „Hightech-Strategie 2025“ der Bundesregierung entstanden. Insbesondere zur Vermeidung von Redundanzen gibt es eine enge 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 Personalräten:innen der Beschaffungsämter der Bundeswehr und Vertreter:innen der Wissenschaft bestehen[81].

Agentur für Sprunginnovationen (SprinD)
Die Agentur für Sprunginnovationen mit Sitz in Leipzig dient als staatliches Instrument für die Entwicklung von Innovationen. SprinD fördert sowohl Forschungsideen als auch Tochtergesellschaften, die sich als Innovationen eignen oder solche durch Potenzial und Arbeitsplätze fördern. Grundsätzlich ist die Agentur offen für Forschungsideen aus allen Themenbereichen. Sie soll „Innovationen auf den Weg bringen, die technologisch radikal neu sind und ein hohes Potenzial für eine marktverändernde Wirkung mit neuen Produkten, Dienstleistungen und Wertschöpfungs-

81 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.

ketten enthalten". Für ihre Arbeit stehen der Agentur für die ersten zehn Jahre eine Milliarde Euro zur Verfügung.

Die SprinD wurde gemeinsam von BMBF und BMWi gegründet. Dem Aufsichtsrat der SprinD gehören neben Mitgliedern aus Wissenschaft und Politik auch Vertreter:innen des BMF, BMBF und BMWi an. Sie koordiniert ihre Aufgaben mit der Cyberagentur[82].

Allianz für Cyber-Sicherheit (ACS)
Die Allianz für Cyber-Sicherheit (ACS) bietet einen vertrauensvollen Austausch zwischen den Mitgliedern und dem Bundesamt für Sicherheit in der Informationstechnik zu Cyberbedrohungen, Schutzmaßnahmen und Vorfallsmanagement. Außerdem erhalten die Mitglieder Informationen zum Ausbau ihrer Cybersicherheitskompetenzen. Mitglied kann jede Institution mit Sitz in Deutschland werden.

Die ACS ist eine Public-Private-Partnership von BSI und BITKOM mit Wirtschaft, Behörden, Forschung und Wissenschaft. Im Beirat der ACS sind u. a. Vertreter:innen aus BMI und BSI Mitglied. Teilnehmer der ACS sind u. a. das BBK, die BaFin, das BKartA, das BKA, das BMVI, das BMWi, die Bw, ein Institut der UniBw München, sowie die Vitako[83].

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 u. a. mit der Berichterstattung an die Zentrale in Berlin betraut sind.

Das AA ist im Cyber-SR vertreten. Es stellt im Wechsel mit dem BMVg die Leitung der BAKS[84].

82 Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.
Bundesministerium für Bildung und Forschung, Agentur für Sprunginnovationen.
Bundesministerium für Bildung und Forschung, Bundesregierung setzt Gründungskommission für die Agentur für Sprunginnovationen ein.
Bundesministerium für Wirtschaft und Energie, Aufsichtsrat der Agentur für Sprunginnovationen SprinD tritt zur konstituierenden Sitzung zusammen.
Deutschlandfunk, „Um Erfolg zu haben, müssen wir uns das Scheitern trauen".
Lina Rusch, Potsdam oder Leipzig? Karliczek vertraut auf SprinD-Gründungsdirektor bei Standortfrage.
Tagesschau, Die Suche nach dem nächsten großen Ding.

83 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.

84 Auswärtiges Amt, Cyber-Außenpolitik.
Auswärtiges Amt, Einrichtung einer Zuständigkeit für Cyber-Außenpolitik.

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 Cyberangriffen zu schützen.

Das BAAINBw gehört zum Geschäftsbereich des BMVg. Es versorgt die Bw mit IT und digitalisierten Waffensystemen und verantwortet die Steuerung der BWI[85].

Bundesakademie für Sicherheitspolitik (BAKS)
Die Bundesakademie für Sicherheitspolitik ist eine Weiterbildungsstätte des Bundes für Sicherheitspolitik. In unterschiedlichen Veranstaltungsformaten, wie z. B. dem „Berliner Forum zur Cyber-Sicherheit", setzt sie sich mit den sicherheitspolitischen Herausforderungen im digitalen Raum 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, BMJV, BMWi, BMZ und das BKAmt) repräsentiert. Als Beiratsmitglieder der BAKS fungieren u. a. Vertreter:innen der GIZ, der Bw, des BMI und der UniBw[86].

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Die Aufgabe der Bundesanstalt für Finanzdienstleistungsaufsicht ist es, ein funktionsfähiges, integres 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 Falle eines Cyberangriffs besteht enger Informationsaustausch mit dem BSI. Die BaFin gehört zum Geschäftsbereich des BMF und ist im Cyber-AZ vertreten[87].

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 Cyberangriffen auf Kritische Infrastrukturen.

85 Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, Das BAAINBw.
86 Bundesakademie für Sicherheitspolitik, Cyber-Realität zwischen Freiheit und Sicherheit.
Bundesakademie für Sicherheitspolitik, Der Beirat.
Bundesakademie für Sicherheitspolitik, Das Kuratorium, der Bundessicherheitsrat.
87 Bundesanstalt für Finanzdienstleistungsaufsicht, Aufgaben & Geschichte der BaFin.
Bundesanstalt für Finanzdienstleistungsaufsicht, BaFinPerspektiven. Ausgabe 1 2020: Cybersicherheit.

Das BBK ist im Cyber-AZ vertreten und sein Personal besetzt das Gemeinsame Melde- und Lagezentrum. Es gehört zum Geschäftsbereich des BMI und ist im UP KRITIS sowie der ACS vertreten[88]*.*

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 u. a. 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 BfIT übernimmt den Vorsitz des Verwaltungsrates der BDBOS. Zur Sicherung der NdB arbeitet die BDBOS als Partnerbehörde eng mit dem BSI zusammen. Der Digitalfunk steht u. a. der BPol, dem BKA, ZKA, BBK sowie dem BfV und den LfV zur Verfügung[89]*.*

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 Bundesnachrichtendienst 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 u. a. extremistische Bestrebungen und Spionagevorhaben[90]*.*

88 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Gemeinsames Melde- und Lagezentrum von Bund und Ländern.

89 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.

90 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).

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik kommt die Aufgabe zu, die Sicherheit in der Informationstechnik des Bundes zu stärken und den Schutz der Regierungsnetze zu gewährleisten. Um im Falle eines Cybervorfalls 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. Für die Bundesverwaltung fungiert das BSI zudem als zentrale Meldestelle für IT-Sicherheit. 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 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) aufgebaut. Der Zweitstandort des BSI in Freital übernimmt u. a. die Arbeit des Verbindungswesens in der Region Ost (Thüringen und Sachsen). Ein dritter Standort des BSI mit dem Schwerpunktthema KI wird in Saarbrücken aufgebaut. Jährlich veröffentlicht das BSI einen Lagebericht zur IT-Sicherheit in Deutschland.

Das BSI gehört zum Geschäftsbereich des BMI und ist am UP KRITIS beteiligt. Es beherbergt unter anderem das Cyber-AZ, ACS, LZ, CERT-Bund und das Bürger-CERT. Neben Bundes- und Landesverwaltungen erhalten auch alle im VCV organisierten Länder-CERTs anlassbezogene Cybersicherheitswarnungen durch das BSI. Zusammen mit dem ITZBund hat das BSI einen „Lenkungskreis Informationssicherheit" etabliert. Das BSI hat zudem eine Kooperationsvereinbarung mit dem vzbz unter anderem bezüglich digitalen Verbraucherschutzes geschlossen. Das BSI ist im Beirat des DsiN vertreten und kooperiert mit dem G4C. Es arbeitet mit der ENISA zusammen, ist Mitglied im SOG-IS und ist zudem 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[91].

91 Bundesamt für Sicherheit in der Informationstechnik, Auftrag.
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.

Bundesamt für Verfassungsschutz (BfV)
Das Bundesamt für Verfassungsschutz untersucht, wie neue technische Möglichkeiten beispielsweise von Extremisten, Terroristen oder ausländischen Nachrichtendiensten genutzt werden, um in Deutschland Spionage, Desinformation oder Computersabotage zu betreiben. Das BfV versucht Cyberangriffe auf staatliche und private Einrichtungen abzuwehren und aufzuklären. Jährlich veröffentlicht das BfV einen Verfassungsschutzbericht, der u. a. auch über den Status quo der Bedrohung durch Cyberangriffe 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 AA. Es ist im Cyber-AZ und der Initiative Wirtschaftsschutz vertreten und greift auf die Expertise von ZITiS zurück. Darüber hinaus besteht Austausch seitens der Cyber-Abwehr des BfV mit ihren entsprechenden Counterparts in den Landesbehörden für Verfassungsschutz (LfV), sofern vorhanden[92].

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, sowie nicht-öffentlicher Stellen. Sie:er ist in der Ausübung seines:ihres Amtes politisch unabhängig und unterliegt lediglich der parlamentarischen Kontrolle durch den Bundestag.

BfDI und BSI kooperieren miteinander. Kontakte bestehen zudem mit dem EDSB. Die:der BfDI ist im Beirat der DsiN vertreten[93].

Bundeskanzleramt (BKAmt)
Das Bundeskanzleramt unterstützt den:die Bundeskanzler:in bei ihrer inhaltlichen Arbeit. Dazu unterhält es durch seine „Spiegelreferate“ engen 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. Innerhalb des BKAmt ist das Amt der:s Beauftragten der Bundesregierung für Digitalisierung institutionell aufgehängt.

92 Bundesamt für Verfassungsschutz, Cyberangriffe.
Bundesamt für Verfassungsschutz, Welche Ziele verfolgen ausländische Nachrichtendienste?. (Webseite entfernt)
Deutscher Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

93 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Eurojust und Europäische Staatsanwaltschaft.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Geschäftsverteilungsplan.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 28. Tätigkeitsbericht zum Datenschutz 2019.

Das BKAmt ist im Cyber-SR vertreten und ihm ist der BND nachgeordnet. Aus seinem Haushalt wird die institutionelle Zuwendung an die SWP gezahlt[94].

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, u. a. 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 BMWi. BKartA und BSI arbeiten im Bereich des digitalen Verbraucherschutzes zusammen. Es ist darüber hinaus Mitglied der ACS[95].

Bundeskriminalamt (BKA)
Das Bundeskriminalamt hat als Zentralstelle der deutschen Polizei sein Aufgabenfeld der nationalen Verbrechensbekämpfung auch auf den Cyberraum ausgeweitet. Es klärt Straftaten im Cyberraum auf, ermittelt und versucht Cyberkriminalität vorzubeugen. Dem BKA fällt hier die „originäre Strafverfolgungskompetenz in Fällen von Cyber-Crime unter Betroffenheit von Behörden oder Einrichtungen des Bundes, der inneren oder äußeren Sicherheit Deutschlands oder zum Nachteil Kritischer Infrastrukturen“ zu. Es hat dazu eine Abteilung „Cybercrime“ (CC) eingerichtet, in der Kompetenzen zur Verfolgung von Cyberkriminalität gebündelt werden. Zu diesem Zwecke kann das BKA u. a. 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).

Das BKA gehört zum Geschäftsbereich des BMI. Es ist im Cyber-AZ, sowie im G4C und der Initiative Wirtschaftsschutz vertreten. Es ist im DsiN Beirat und greift auf die Expertise von ZITiS zurück. Das BKA ist der deutsche Ansprechpartner für Europol und dient als Nationale Stelle[96].

94 Bundeskanzleramt, Chef des Bundeskanzleramtes.
95 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.
96 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.

Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
Das Bundesministerium der Justiz und für Verbraucherschutz ist vor allem ein Gesetzgebungsministerium, das auch andere Bundesministerien bei ihren Rechtsetzungsvorhaben unterstützt. Innerhalb der Bundesregierung ist es für die wirtschaftliche Verbraucherpolitik zuständig. In diesem Rahmen beschäftigt es sich u. a. mit Themen wie dem Schutz von Bürgern und Onlinehändlern vor Cyberkriminalität oder Online-Mobbing.

Das BMJV ist im Cyber-SR vertreten[97].

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 des Ressorts Verteidigung (CISO Ressort) in der Abteilung Cyber- und Informationstechnik (CIT) federführend zuständig.

Das BMVg ist im Cyber-SR vertreten. Ihm ist die Bw nachgeordnet und die BAKS gehört zu seinem Geschäftsbereich. Die Cyberagentur soll unter gemeinsamer Federführung des BMVg und BMI eingerichtet werden. Das BMVg setzt zudem auf nationale und internationale Kooperationen und Partnerschaften, zum Beispiel mit dem Cyber Innovation Hub oder dem Cooperative Cyber Defence Centre of Excellence der NATO[98].

Bundesministerium des Innern, für Bau und Heimat (BMI)
Das Bundesministerium des Innern, für Bau und Heimat ist u. a. für die zivile Sicherheit im Cyberraum zuständig. Der Abteilung Cyber- und Informationssicherheit (CI) des BMI obliegt u. a. 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 (BfIT), der:die auch Vorsitzender des Cyber-Sicherheitsrates ist.

97 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)

98 Bundesministerium der Verteidigung, Cybersicherheit.
Bundesministerium der Verteidigung, Cyber Innovation Hub.
Bundesministerium der Verteidigung, Die Abteilungen des Verteidigungsministeriums.
Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land 2018.

Das BMI ist im Cyber-SR vertreten. Seinem Geschäftsbereich sind BPol, BKA, BSI, BfV, BDBOS und BBK zugeordnet. Die Gründung von ZITiS geht auf einen Erlass des BMI zurück. Das BMI ist in den Initiativen UP KRITIS, DsiN (Beirat), sowie der ACS vertreten. Die Cyberagentur wurde unter gemeinsamer Federführung des BMI und BMVg eingerichtet[99].

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" zur Förderung multi-sektoraler Cybersicherheitsforschung sowie die Initiative StartUpSecure ins Leben gerufen, die u.a „Unternehmensgründungen im Bereich der IT-Sicherheit" unterstützt.

Das BMBF ist im Cyber-SR vertreten und fördert die Kompetenzzentren für IT-Sicherheit[100].

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 Cyber-SR vertreten. Ihm nachgeordnet ist das ZKA und es hat außerdem die Rechts- und Fachaufsicht über die BaFin. BMZ und BMF sind Gesellschafter der GIZ[101].

Bundesministerium für Gesundheit (BMG)

Das Bundesministerium für Gesundheit ist vor allem für die Leistungsfähigkeit der gesetzlichen Krankenversicherung sowie der Pflegeversicherung verantwortlich. Mit dem E-Health-Gesetz soll eine digitale Infrastruktur mit höchsten Sicherheitsstandards im Gesundheitswesen geschaffen werden.

99 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.

100 Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt" und StartUpSecure.
Fraunhofer SIT, Institutsgeschichte.
Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

101 Bundesfinanzministerium, Grundelemente zur Cyber-Sicherheit.
Bundesfinanzministerium, Themen.

Das BMG hat die gematik mit dem Aufbau einer Telematikinfrastruktur beauftragt, welche die Voraussetzung für eine sichere Vernetzung des Gesundheitswesens bildet[102].

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)
Das Bundesministerium für Verkehr und digitale Infrastruktur 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 BMVI seine Krisenszenarien auch hinsichtlich möglicher Cyberangriffe auf digitale Infrastrukturen weiter.

Das BMVI ist im Cyber-SR vertreten[103].

Bundesministerium für Wirtschaft und Energie (BMWi)
Das Bundesministerium für Wirtschaft und Energie 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 BMWi setzt sich dabei vor allem für IT-Sicherheit in der Industrie 4.0 ein.

Das BMWi ist im Cyber-SR vertreten. Es hat die Initiative IT-Sicherheit in der Wirtschaft ins Leben gerufen. Es ist im Beirat von DsiN vertreten und die BNetzA gehört zu seinem Geschäftsbereich[104].

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 und unterstützt Cyber Capacity Building durch Bildungsprogramme vor Ort.

Das BMZ ist der wichtigste Auftraggeber der GIZ und neben dem BMF einer der beiden Gesellschafter[105].

Bundesnachrichtendienst (BND)
Der Bundesnachrichtendienst ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland und handelt im Auftrag der Bundesregierung. Im Ausland erfasst

102 Bundesministerium für Gesundheit, Aufgaben und Organisation.
Bundesministerium für Gesundheit, E-Health-Gesetz.
103 Bundesministerium für Verkehr und digitale Infrastruktur, Krisenmanagement.
104 Bundesministerium für Wirtschaft und Energie, IT-Sicherheit.
Bundesministerium für Wirtschaft und Energie, IT-Sicherheit für die Industrie 4.0.
105 Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Glossar – Digitalisierung und nachhaltige Entwicklung.
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?.

er Angriffe, 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 auch unter dem Akronym SSCD (SIGINT Support to Cyber Defense).

Der BND gehört zum Geschäftsbereich des BKAmt. 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. Sein Personal wird unter anderem an der UniBw München ausgebildet[106].

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 verantwortet demnach auch IT-Sicherheitsanforderungen in den entsprechenden Sektoren.

Die BNetzA gehört zum Geschäftsbereich des BMWi. Gemeinsam mit dem BSI hat sie den IT-Sicherheitskatalog herausgebracht, zu dessen Umsetzung alle Betreiber von Gas- und Stromnetzen verpflichtet sind[107].

Bundesverband der Verbraucherzentralen und Verbraucherverbände (vzbv)
Der gemeinnützige Verbraucherzentrale Bundesverband e. V. (vzbz) 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 Hauptsitz des vzbv befindet sich in Berlin, ein Team ist zudem in Brüssel angesiedelt. 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.

Seine Kernarbeit wird zu einem Anteil von 97 Prozent durch das BMJV finanziert. Die vzbv und das BSI haben eine Grundsatzvereinbarung über ihre Zusammenarbeit[108].

106 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.
107 Bundesnetzagentur, Aufgaben und Struktur.
Bundesnetzagentur, IT-Sicherheit im Energiesektor.
108 Bundesministerium für Justiz und Verbraucherschutz, Verbraucherzentralen.
Bundesamt für Sicherheit in der Informationstechnik, BSI und Verbraucherzentrale stärken digitalen Verbraucherschutz.
Verbraucherzentrale Bundesverband, Häufige Fragen (FAQ).
Verbraucherzentrale Bundesverband, Über Uns.

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. 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 im Cyber-AZ vertreten und greift auf die Expertise von ZITiS zurück. Die ZAC sind bei den Polizeien des Bundes und der Länder angesiedelt. Das CERT BPol ist Gast im CERT-Verbund[109].

Bundeswehr (Bw)
Die Bundeswehr ist 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. Der MilOrgBer CIR wird durch das KdoCIR geführt, zu ihm gehören beispielweise KdoITBw, KdoStratAufkl sowie das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw).

Die Bw gehört zum Geschäftsbereich des BMVg. Sie bildet Teile ihres Personals an den UniBw aus und ist im Cyber-AZ sowie in verschiedenen nationalen und internationalen CERT-Verbunden vertreten[110].

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. Diese soll ehemaligen Soldat:innen eine Eingliederung und die Arbeit im BWI ermöglichen.

109 Bundespolizei, Startseite.
Bundespolizei kompakt, 04/2015.
Deutscher Bundestag (Drucksache18/13555), Antwort der Bundesregierung auf die Kleine Anfrage: Aktuelle Situation und Ausrichtung der Bundespolizei.
Hintergrundgespräche, 2019.
110 Bundeswehr, Auftrag und Aufgaben der Bundeswehr.
Bundeswehr, Das Kommando Cyber- und Informationsraum.

Die BWI GmbH ist eine Bundesgesellschaft und IT-Systemhaus für Bw und Bund[111].

Bündnis für Cybersicherheit
Das Bündnis für Cybersicherheit soll die Zusammenarbeit zwischen Staat und Wirtschaft stärken. Das Ziel des Bündnisses ist dabei eine bessere Vernetzung beider Sektoren für eine effizientere Gewährleistung von Cybersicherheit – insbesondere auch im internationalen Kontext. Als Forum zwischen Bundesbehörden und Wirtschaftsvertreter:innen soll sich 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.

Das Bündnis für Cybersicherheit basiert auf einer Vereinbarung zwischen dem BMI und dem Bundesverband der deutschen Industrie e. V.[112].

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-Vorfalls. 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 aufgehangen. Es kooperiert mit dem CERT-Verbund und im Rahmen des Verwaltungs-CERT-Verbunds (VCV) auch mit den Länder-CERTs. Auf europäischer Ebene arbeitet CERT-Bund mit der EGC Group sowie der ENISA zusammen[113].

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 Bun-

111 Bundesministerium der Verteidigung, Auf engere Kooperation geeinigt: Bundeswehr und BWI GmbH.
Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.
112 Bundesministerium des Innern, für Bau und Heimat, Industrie und BMI etablieren Bündnis für Cybersicherheit.
113 Bundesamt für Sicherheit in der Informationstechnik, CERT-Bund.
Bundesamt für Sicherheit in der Informationstechnik, Nationale und internationale Zusammenarbeit.
CERT-Bund, Über CERT-Bund.

deswehr 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.

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[114].

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. 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[115].

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 wissenschaftli-

114 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.

115 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.

cher 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 sind Mitglieder im Beirat des Cyber Security Clusters Bonn e. V.[116].

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 BMWi) sowie die Länder Bayern, Hamburg und Nordrhein-Westfalen. Im Aufsichtsrat der DAkkS sind neben Mitgliedern aus der Wirtschaft und Repräsentanten:innen der Länder auch Vertreter:innen des BMWi und BSI vertreten. Die DAkkS ist Mitglied in der EA[117].

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.

BMZ und BMF sind Gesellschafter der GIZ[118].

Deutschland sicher im Netz e. V. (DsiN)
Deutschland sicher im Netz e. V. soll dazu beitragen, die deutsche Bevölkerung, sowie 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.

116 Cyber Security Cluster Bonn, Über uns.
Cyber Security Cluster Bonn, Weisenrat für Cyber-Sicherheit.
Emailaustausch mit Vertreter:innen des Cyber Security Cluster Bonn e. V. im November 2019.
117 Deutsche Akkreditierungsstelle, Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443.
Deutsche Akkreditierungsstelle, Aufsichtsrat.
Deutsche Akkreditierungsstelle, Profil.
Deutsche Akkreditierungsstelle, Sektorkomitee Informationstechnik / Informationssicherheit (SK IT-IS).
Deutsche Akkreditierungsstelle, Welche Aufgabe hat die DAkkS?.
118 Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Bundesregierung.
Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Startseite.
Hintergrundgespräche, 2018.

Das BMI, BMWi, BSI, BKA und BfDI sind im Beirat des DsiN vertreten. Der:die Bundesinnenminister:in ist Schirmherr:in des DsiN. DsiN kooperiert mit der Initiative IT-Sicherheit in der Wirtschaft[119].

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 UniBw München angebunden.

Als Teil der UniBw wird auch am CODE Bw-Personal wissenschaftlich ausgebildet. Ein:e Vertreter:in des BMVg sitzt im Beirat des CODE[120].

Föderale IT-Kooperation (FITKO)

Die Föderale IT-Kooperation koordiniert die Ebenen bei der Digitalisierung der Verwaltung des IT-Planungsrates und verbessert die Handlungs- sowie politisch-strategische Steuerungsfähigkeit des IT-Planungsrates. Die formale Gründung der Agentur erfolgte 2020 und ihr Sitz ist in Frankfurt am Main. FITKO operiert bei seinen Digitalisierungsvorhaben im Rahmen des Onlinezugangsgesetzes mit einem Budget von bis zu 180 Millionen Euro.

Die Föderale IT-Kooperation ist ein operativer Unterbau des IT-Planungsrates. Unter Vorsitz der FITKO wurde 2020 ein Kommunalgremium des IT-Planungsrates eingerichtet[121].

gematik

Die gematik GmbH ist ein Kompetenzzentrum und Dienstleistungsunternehmen für das deutsche Gesundheitswesen. Für dessen sichere Vernetzung und Digitalisierung stellt die gematik die Telematikinfrastruktur 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 Telematikinfrastruktur sowie die Betriebskoordination. Neben der Telematikinfrastruktur ist die gematik auch für die elektronische Gesundheitskarte zuständig, die in Deutschland als ausschließlicher Versicherungsnachweis dient.

119 Deutschland sicher im Netz, Presse.
120 Universität der Bundeswehr München, Forschungsinstitut CODE.
Universität der Bundeswehr München, Forschungsinstitut CODE. Unsere Mission.
Universität der Bundeswehr München, Beirat des Forschungsinstituts CODE.
121 Lina Rusch, Digitaler Staat: Agenturen in den Startlöchern.
IT-Planungsrat, FITKO. (Webseite entfernt)
Matthias Punz, Rechtlicher Rahmen für FITKO-Start steht.

Die gematik wird von verschiedenen Gesellschaftern getragen, so hält das Bundesministerium für Gesundheit beispielsweise 51 Prozent der Gesellschafteranteile. Im Beirat sitzen unter anderem jeweils ein:e Vertreter:in der:s Bundesbeauftragte:n für den Datenschutz und die Informationsfreiheit, des Bundesamts für Sicherheit in der Informationstechnik und des Bundesministeriums für Wirtschaft und Energie[122].

Gemeinsames Lagezentrum Cyber- und Informationsraum (GLZ CIR)
Das Gemeinsame Lagezentrum Cyber- und Informationsraum (GLZ CIR) ist Teil des KdoCIR und erarbeitet als zentrales Analysezentrum Lagebilder zum Cyber- und Informationsraum. Seine Aufgabe ist es Informationen und Lagen zu militärisch relevanten Aspekten des Cyber- und Informationsraums aus unterschiedlichen Quellen zu bündeln, in einen Zusammenhang zu stellen und Handlungsoptionen zu erarbeiten. Es nutzt dabei ein eigenes IT-System, das sich verschiedener Verfahren wie beispielsweise Künstlicher Intelligenz bedient.

Das GLZ CIR ist mit Aufstellung des KdoCIR etabliert worden. Bei der Etablierung des IT-Systems für das GLZ CIR wurde die Bundeswehr außerdem von der BWI unterstützt. Die Analyse der Situation im Cyber- und Informationsraum wird u. a. dem BMVg und dem Cyber-AZ bereitgestellt[123].

Gemeinsames Melde- und Lagezentrum (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.

Das BBK ist im GMLZ vertreten. Partner des GMLZ sind u. a. BPol, BKA und EK. Im Bedarfsfall leitet das GMLZ Aktivierungsanfragen für das Katastrophen- und Krisenmanagement der EU an das ERCC weiter [124].

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 behördli-

122 Bundesministerium für Gesundheit, E-Health-Gesetz.
Gematik, Die elektronische Gesundheitskarte.
Gematik, Telematikinfrastruktur.
Gematik, Themen.
Gematik, Über uns.
123 Bundesministerium der Verteidigung, Lagezentrum Cyber- und Informationsraum im Pilotbetrieb.
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.
124 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.

chen Kooperationspartnern und den Mitgliedern, können diese geeignete präventive Schutzmaßnahmen entwickeln.

Das G4C kooperiert mit dem BKA und dem BSI[125]*.*

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 Bundesministerium für Verkehr und digitale Infrastruktur nachgeordneten Bundesanstalt für IT-Dienstleistungen und dem Zentrum für Informationsverarbeitung und Informationstechnik.

Das ITZBund gehört zum Geschäftsbereich des Bundesministeriums der Finanzen. Zusammen mit dem BSI hat das ITZBund im August 2020 einen „Lenkungskreis Informationssicherheit" etabliert sowie im September 2020 eine Rahmenverwaltungsvereinbarung geschlossen, die eine engere Zusammenarbeit zwischen beiden Institutionen ermöglichen sollen. Der:die BfDI überprüft regelmäßig die Daten- und Informationsverarbeitung des ITZBund[126]*.*

Initiative IT-Sicherheit in der Wirtschaft
Die Initiative IT-Sicherheit in der Wirtschaft ist eine Initiative des Bundesministeriums für Wirtschaft und Energie 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 Steuerunsgkreises sind u. a. Vertreter:innen des BMWi, des BSI und dem DsiN. Letzterer wurde im Rahmen der Initiative ins Leben gerufen[127]*.*

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.

125 German Competence Centre against Cyber Crime e. V. (G4C), Über uns.
126 Informationstechnikzentrum Bund, ITZBund und BSI intensivieren Zusammenarbeit für mehr IT-Sicherheit.
Informationstechnikzentrum Bund, IT-Sicherheit.
Informationstechnikzentrum Bund, Über uns.
127 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.

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 zu[128].

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 IuK). 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 Innenministerkonferenz mit dem BMI verbunden. Regelmäßig erhält die IMK Berichte des Cyber-SR[129].

IT-Planungsrat (IT-PLR)

Der IT-Planungsrat ist ein Gremium zur Verbesserung der föderalen Zusammenarbeit in der Informationstechnik. Es koordiniert die Zusammenarbeit von Bund und Ländern in Fragen der IT, fasst Beschlüsse über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards, steuert E-Government-Projekte und plant und entwickelt das Verbindungsnetz nach dem IT-NetzG. Er setzt sich aus der:m Beauftragten der Bundesregierung für Informationstechnik und aus den für Informationstechnik zuständigen Vertreter:innen der Länder zusammen. Beratend an Sitzungen können drei Vertreter:innen der Gemeinden und Gemeindeverbänden, die von den kommunalen Spitzenverbänden auf Bundesebene entsandt werden, sowie die:der Beauftragte für den Datenschutz und die Informationsfreiheit teilnehmen. Weitere Personen, unter anderem jeweilige Ansprechpartner der Fachministerkonferenzen, können ebenfalls hinzugerufen werden, wenn die Entscheidungen des Rates ihr Fachgebiet tangieren. Im Vorsitz wechseln sich Bund und Länder (in alphabetischer Reihenfolge) jährlich ab. Teil des IT-Planungsrats ist zudem die Arbeitsgruppe Informationssicherheit (AG InfoSic). Diese Arbeitsgruppe ist dafür zuständig, IT-Zielsetzungen für die öffentliche Verwaltung sowie Strategien für deren Umsetzung zu erarbeiten, die in einer entsprechenden Leitlinie festgehalten werden.

128 Bundesamt für Verfassungsschutz, Initiative Wirtschaftsschutz.
Bundesamt für Verfassungsschutz, Initiative Wirtschaftsschutz. Das Informationsportal.

129 Bundesrat, Innenministerkonferenz.
CISO der niedersächsischen Landesverwaltung, Cybersicherheit in der Landesverwaltung.
Secupedia, Nationales Cyber-Abwehrzentrum.
Emailaustausch mit Vertreter:innen des BSI im Februar 2020.
Innenministerkonferenz, 213. Sitzung der Innenministerkonferenz.

Der:die BfDI sowie Vertreter:innen der kommunalen Spitzenverbände sind beratende Mitglieder. Dem IT-Planungsrat untersteht die FITKO sowie ein Kommunalgremium. Der:die Chef:in des Bundeskanzleramtes 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-Strategie[130].

IT-Rat

Der IT-Rat ist als politisch-strategisches Gremium für übergreifende Themen der Digitalisierung sowie die Steuerung der IT der Bundesverwaltung zuständig.

Der Vorsitz des IT-Rats wird durch die:en Chef:in des Bundeskanzleramts wahrgenommen. Stellvertretende:r Vorsitzende:r sind die:der Bundesbeauftragte:r für Digitalisierung sowie der:die Beauftragte:r der Bundesregierung für Informationstechnik (BfIT)[131].

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.

Bei der Etablierung von ITSMIG haben das BMI und das BMWi unterstützt. Beide Ministerien sind im Beirat der Arbeitsgruppe vertreten[132].

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“. Vorrangig soll das Kommando jedoch den CIR strukturieren und die Personalführung gewährleisten. Zudem ist es „Dienstsitz des Inspekteurs CIR und seines Vertreters, der in seiner Funktion als Chief Information Security Officer (CISOBw) die Gesamtverantwortung für die Informations-

130 IT-Planungsrat, Aufgaben des IT-Planungsrats.
IT-Planungsrat, Besprechung des Chefs des Bundeskanzleramtes mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder.
IT-Planungsrat, IT-Planungsrat.
IT-Planungsrat, Umsetzung Leitlinie InfoSic. (Webseite entfernt)
IT-Planungsrat, Zusammensetzung des IT-Planungsrates.
131 Der Beauftragte der Bundesregierung für Informationstechnik, IT-Rat.
132 TeleTrust, IT Security made in Germany.

sicherheit 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 für den Fall eines Angriffs auf die IT-Systeme der Bw zur Verfügung. KdoCIR beschäftigt insgesamt ca. 13.500 Soldat:innen und zivile Mitarbeiter:innen. Der Standort des KdoCIR ist in Bonn.

Innerhalb des Organisationsbereichs sind ihm u. a. das KdoStratAufkl und das KdoITBw unterstellt. Es beheimatet zudem das GLZ CIR. Der CISOBw ist im KdoCIR verortet. Es ist im Cyber-AZ als ständiges Mitglied vertreten und stellt einen der stellvertrenden Koordinatoren. Auf eine Initiative des KdoCIR geht die Etablierung des CIDCC als PESCO-Projekt zurück. Das KdoCIR ist als Beiratsmitglied im Cyber Security Cluster Bonn vertreten. Die Aktivitäten der Bundeswehr zur Cyber-Reserve werden vom KdoCIR gesteuert[133].

Kommando Informationstechnik (KdoITBw)
Das Kommando Informationstechnik ist ein Fähigkeitskommando im Organisationsbereich der Streitkräftebasis und ist mit der Bereitstellung von zentralen IT-Services der Bundeswehr befasst. Der Hauptsitz des KdoITBw befindet sich in Bonn. Das KdoITBw stellt sicher, dass bei den Einsätzen die Einrichtung, der Betrieb und der Schutz der zentralen IT- und Kommunikatons-Elemente gewährleistet sind. Dem Kommando unterstehen sechs „Informationstechnik-Bataillone" und diverse Dienststellen wie beispielsweise das „Betriebszentrum IT-System der Bundeswehr".

KdoITBw ist dem KdoCIR unterstellt und gehört zum Organisationsbereich CIR der Bw[134].

Kommando Strategische Aufklärung (KdoStratAufkl)
Das Kommando Strategische Aufklärung dient der Informationsbedarfsdeckung der Bundeswehr zum Schutz des Personals in Einsatzgebieten sowie zur Krisenfrüherkennung. Dazu betreibt das KdoStratAufkl auch Aufklärung in definierten Bereichen. Die Aufgabenbereiche des Kommandos werden dabei in die Felder „Satellitengestützte Abbildende Aufklärung", „Fernmelde- und Elektronische Aufklärung", den „Elektronischen Kampf" und den Bereich der „Objektanalyse" unterteilt. Ferner arbeitet das Kommando am Fähigkeitsaufbau im Bereich Computer-Netzwerk-Operationen. Es führt mehrere Dienststellen des CIR an, so beispielsweise das Zentrum

133 Bundesamt für Sicherheit in der Informationstechnik, BSI Magazin 2020/01: Mit Sicherheit.
Bundesministerium der Verteidigung, FAQ: Cyber-Abwehr.
Bundeswehr, Auftrag des Organisationsbereichs CIR.
Bundeswehr, Kommando Cyber- und Informationsraum.
134 Bund, Kommando Informationstechnik der Bundeswehr (KdoITBw).
Bundeswehr, Kommando Informationstechnik der Bundeswehr.
Bundeswehr, Zentrum für Cyber-Sicherheit der Bundeswehr.
Bernd Kammermeier, Zentrum für Cyber-Sicherheit der Bundeswehr –Moderner Dienstleister für IT-Sicherheit.

Cyber-Operationen (ZCO). Das ZCO bündelt Fähigkeiten zur Planung, Vorbereitung, Führung und Durchführung von militärischen Cyberoperationen zur Aufklärung und Wirkung. Das Kommando operiert aus Grafschaft-Gelsdorf in Rheinland-Pfalz.

Das KdoStratAufkl untersteht KdoCIR[135]*.*

Nationaler Cyber-Sicherheitsrat (Cyber-SR)
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 Cyber-SR, welcher dreimal jährlich zusammenkommt, u. a. „Vorschläge zur Weiterentwicklung der nationalen Regelungen für mehr Cybersicherheit" gemacht und Räume für öffentlich-private Kooperationen identifiziert werden. Der Cyber-SR 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 Cyber-SR sind BMI, BKAmt, AA, BMVg, BMWi, BMJV, BMF und BMBF sowie Repräsentant:innen der Länder Niedersachen und Hessen vertreten. In Sondersitzungen wurden darüber hinaus in der Vergangenheit auch bereits Vertreter:innen der ENISA, des BfV und der SWP eingeladen. Den Vorsitz des Cyber-SR hat der:die BfIT inne. Der wissenschaftlichen Arbeitsgruppe gehört neben wissenschaftlichen Vertreter:innen auch ein:e Repräsentant:in des BSI an. Neben der Bundesregierung soll der Cyber-SR auch Impulse für die Innenministerkonferenz liefern[136]*.*

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 Cyberangriffe ermöglicht werden.

135 Bund, Kommando Strategische Aufklärung (KdoStratAufkl).
Bund, Zentrum Cyberoperationen (ZCO).
Bundeswehr, Das Zentrum Cyber-Operationen.
Bundeswehr, Kommando Strategische Aufklärung.
136 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, Cyber-Sicherheitsrat.
Fraunhofer-Institut für Sichere Informationstechnologie, Beratung aus der Forschung. Wissenschaftliche Arbeitsgemeinschaft Nationale Cyber-Sicherheit.
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE, Impulspapiere der Wissenschaftlichen AG Nationale Cyber-Sicherheit.

Im CERT-Verbund sind unter anderem das CERTBw, das BSI mit dem CERT-Bund sowie das CERT der BWI vertreten. Von Länderseite sind u.a. das Bayern-CERT, CERT Baden-Württemberg, CERT-NRW und CERT-rlp beteiligt[137].

Nationaler Pakt Cybersicherheit

Der Nationale Pakt Cybersicherheit ist eine Initiative des BMI, welche als deutscher Beitrag den Paris Call for Trust and Security in Cyberspace unterstützen 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 im Rahmen eines Online-Kompendiums wesentliche Akteure der Cybersicherheit in Deutschland erfasst. Darüber hinaus soll der Pakt das Vorgehen mit Handlungsempfehlungen für die nächste Legislaturperiode evaluieren. In der Öffentlichkeit wird der Pakt durch eine „Quadriga" repräsentiert.

Teil des Paktes sind unter anderem das Bündnis für Cybersicherheit und die Cyberagentur. In der „Quadriga" des Nationalen Pakts für Cybersicherheit ist neben einem:r parlamentarischen Staatsekretär:in des BMI zudem der:die Vorstand:ändin des vzbv als zivilgesellschaftlicher Repräsentant vertreten[138].

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 Cyberangriffen 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 zwischen BSI, BPol, BKA, BfV, BBK, BND, KdoCIR, BaFin und BAMAD. Das ZKA ist assoziiert beteiligt. Es schickt seinen Jahresbericht an den Cyber-SR. Neben den o.g. Behörden werden die Cyber-Lagen darüber hinaus u.a. an die LfV sowie Mitglieder des VCV gesendet. Das BKA stellt den:die Ko-

137 Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: CERT-Verbund.
Deutscher CERT-Verbund, Überblick.

138 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.

ordinator: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[139].

Nationales IT-Lagezentrum (LZ)
Das 24 Stunden täglich operierende Nationale IT-Lagezentrum im Bundesamt für Sicherheit in der Informationstechnik 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. 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 Kapazitäten und Strukturen des LZ erlauben es zudem, gegebenenfalls in ein IT-Krisenreaktionszentrum aufzuwachsen.

Das LZ arbeitet eng mit dem GMLZ, CERT-Bund und Cyber-AZ zusammen. Der tägliche Lagebericht IT-Sicherheit des LZ geht u. a. an UP KRITIS, den VCV sowie die ACS[140].

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 Teil der Bw und wird vom KdoCIR geführt, dem wiederum das KdoITBw und das KdoStratAufkl unterstellt sind[141].

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 eingerichte-

139 Hintergrundgespräche, 2019.
Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.
Bundesamt für Sicherheit in der Informationstechnik, BSI Magazin 2020/01: Mit Sicherheit.
Bundeskriminalamt, 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.
140 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.
141 Bundeswehr, Auftrag des Organisationsbereichs CIR.

ten 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[142].

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 u. a. Vertreter:innen aus BKAmt, BMBF, BMZ, BMI, AA, BMF, BMWi und BMVg vertreten[143].

Transferstelle IT-Sicherheit im Mittelstand (TISiM)
Die Transferstelle wurde im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie (BMWi) 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 mit rund 5 Millionen Euro im Jahr bezuschusst.

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 Allianz für Cyber-Sicherheit aus[144].

142 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.

143 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.

144 Bundesministerium für Wirtschaft und Energie, Altmaier: „Wir stärken die Kompetenzen des Mittelstands im Bereich IT-Sicherheit“.
Bundesministerium für Wirtschaft und Energie, Neue Transferstelle IT-Sicherheit bündelt Hilfestellungen bundesweit.
Deutschland sicher im Netz, Transferstelle.

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 aktuell 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[145]*.*

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.

Am VCV beteiligt sind das BSI und das CERT-Bund, sowie Länder CERTs und das LSI[146]*.*

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

145 Universität der Bundeswehr München, Hintergrundinformationen.
Universität der Bundeswehr Hamburg, Studium.
146 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).

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. 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. Sowohl EU-HYBNET als auch FORMOBILE sind Teil von Horizon 2020. Die Koordination des EU-HYBNET-Projektes obliegt dem Hybrid CoE und weitere Projektpartner sind u. a. das GD JRC sowie die UniBwM. 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[147].

Zollkriminalamt (ZKA)

Das Zollkriminalamt (ZKA) 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 dem BMF nachgeordnet und ist im Cyber-AZ vertreten und kann als Sicherheitsbehörde des Bundes auf Dienstleistungen von ZITiS zurückgreifen[148].

147 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.

148 Anna Loll, Datensicherheit oder Abwehr von Cyberkriminalität. Politik und Gesellschaft müssen sich mal entscheiden.
Der Zoll, Die Aufgaben des Zolls.

7. Erläuterung – Akteure auf Landesebene

Computer Emergency Response Teams der Bundesländer (Länder-CERTs)
Die Länder-CERTs sind die Computer Emergency Response Teams der einzelnen Bundesländer, die an unterschiedlichen Stellen angegliedert sind.

- Das CERT BWL (Baden-Württemberg) ist beim IT-Baden-Württemberg (BITBW) angesiedelt.
- Das Bayern-CERT ist am LSI angesiedelt.
- Das Berlin-CERT wird vom IT-Dienstleistungszentrum Berlin (ITDZ Berlin) geführt.
- Das CERT-Brandenburg wird vom Brandenburgischen IT-Dienstleister (ZIT-BB) betrieben.
- Die Länder Bremen, Schleswig-Holstein, Hamburg und Sachsen-Anhalt haben ein gemeinsames CERT Nord.
- Das hessische CERT ist bei der Gründung von H3C in dessen Bereich Cybersecurity integriert worden. Dieser nimmt alle Aufgaben des CERTs wahr.
- Das CERT M-V wird vom Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ M-V) betrieben.
- Das N-CERT (Niedersachsen) ist beim Ministerium für Inneres und Sport angegliedert.
- Das CERT NRW liegt beim Landesbetrieb Information und Technik Nordrhein-Westfalen.
- Das CERT-rlp gehört zum Landesbetrieb Daten und Information.
- Das CERT Saarland wird durch eine Vereinbarung zwischen dem Saarland und Rheinland-Pfalz vom CERT-rlp bereitgestellt.
- Das SAX.CERT (Sachsen) ist an den Staatsbetrieb Sächsische Informatik Dienste angegliedert.
- Das ThüringenCERT wird durch das Thüringische Landesrechenzentrum betrieben.

Im Rahmen des Verwaltungs-CERT-Verbunds (VCV) kooperieren Bund und Länder beim Aufbau und Betrieb der Länder-CERTs. Die Länder-CERTs kooperieren mit dem CERT-Bund im BSI[149].

149 Staatsministerium Baden-Württemberg, Systeme des Landesamtes für Geoinformation wieder in Betrieb.
Brandenburgischer IT-Dienstleister, CERT-Brandenburg.
Bundesamt für Sicherheit in der Informationstechnik, BSI und Thüringen: Engere Zusammenarbeit bei der Cyber-Sicherheit (Webseite entfernt).
Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.
Information und Technik Nordrhein-Westfalen, Informationssicherheit für die Landesverwaltung NRW.
ITDZ Berlin, Sicherheit.
Kommune 21, CERT für saarländische Kommunen.
Landesamt für Sicherheit in der Informationstechnik, Staatsverwaltung.
Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).
Niedersächsische Ministerium für Inneres und Sport, Niedersachsen-CERT.
Ministerium des Innern und für Sport Rheinland-Pfalz, CERT-rlp.
Staatsbetrieb Sächsische Informatik Dienste, CERT & Informationssicherheit.
Thüringer Landesrechenzentrum, ThüringenCERT.

Cyberabwehr Bayern
Die Cyberabwehr ist eine Informations- und Koordinierungsplattform und garantiert seit Januar 2020 einen engen und 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 Angriffen auf die IT-Sicherheitsstruktur soll durch die Cyberabwehr Bayern auch ein Überblick über die Gefährdungslage im Cyberraum gegeben und ein bayerisches Lagebild geschaffen werden. Gleichzeitig soll es als Ansprechstelle für das Cyber-AZ dienen und so den Austausch zwischen dem Bund und dem Land Bayern erleichtern. 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 Cyber-Allianz-Zentrum Bayern im Bayerischen Landesamt für Verfassungsschutz verortet. Teil der Cyberabwehr sind das Bayerische Landeskriminalamt, das Bayerische Landesamt für Sicherheit in der Informationstechnik, die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, das Bayerische Landesamt für Datenschutzaufsicht und der Landesbeauftragte für den Datenschutz sowie das Cyber-Allianz-Zentrum Bayern[150].

Cyber-Allianz-Zentrum (CAZ) – Bayern
Das Cyber-Allianz-Zentrum Bayern gehört zum Bayerischen Landesamt für Verfassungsschutz und unterstützt in Bayern ansässige Unternehmen, Hochschulen, Betreiber Kritischer Infrastrukturen im Bereich der Prävention und Abwehr elektronischer Angriffe. 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 Angriff betroffene Unternehmen oder Einrichtungen mit Informationen zu den Angriffsmustern. Das CAZ war die erste institutionelle Säule der „Initiative Cybersicherheit Bayern“ des Bayerischen Staatsministeriums des Innern, für Sport und Integration[151].

Cyber-Competence-Center (CCC) – Brandenburg
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 über-

150 Bayernkurier, Bayern stärkt die Cyber-Abwehr.
STMI Bayern, Bayern stärkt Cyberabwehr und Digitalfunk.
Tagesspiegel, Cyberabwehr: Neues Lagezentrum in Bayern geplant.
Verfassungsschutz Bayern, Cyberabwehr Bayern.
151 Bayerisches Landesamt für Verfassungsschutz, Cyber-Allianz-Zentrum Bayern (CAZ).

nimmt sowohl präventive als auch repressive Aufgaben und unterstützt Ermittlungen der Polizeidirektionen und -inspektionen zur Bekämpfung der Cyberkriminalität.

Am CCC wurde auch die ZAC für Wirtschaftsunternehmen und Behörden eingerichtet[152].

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 Zentralen Ansprechstelle für die Wirtschaft[153].

Cyber Defense Center der Landesverwaltung Berlin (CDC-Lv)
Das Cyber Defense Center der Berliner Landesverwaltung ist im dortigen IT-Dienstleistungszentrum (ITDZ Berlin) angesiedelt. Es besteht aus einem Security Operation Center (SOC), dem Berlin-CERT, einem Bereich für Analyse und Forensik, sowie 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 Angriffen auf das Berliner Landesnetzes zu.

Das CDC-Lv berichtet durch das Berlin-CERT an den:die Berliner Landesbeauftragte:r für Informationssicherheit. Auf Arbeitsebene besteht Austausch mit dem Berliner BSI-Verbindungsbüro[154].

Cybercrime Competence Center (4C) – Sachsen-Anhalt
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 Zentrale Ansprechstelle für die Wirtschaft[155].

152 Polizei Brandenburg, Cyber-Competence-Center im Landeskriminalamt.
153 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.
154 ITDZ Berlin, Innovationsmanagement im ITDZ Berlin.
Hintergrundgespräch, 2021.
155 Hallelife.de, Sachsen-Anhalt startet Kompetenzzentrum gegen Internetkriminalität.

Cybercrime-Kompetenzzentrum – Nordrhein-Westfalen
Das im Landeskriminalamt Nordrhein-Westfalen eingerichtete Cybercrime-Kompetenzzentrum beherbergt Ermittlungskommissionen für herausragende Verfahren, Expert:innen für Computerforensik, Telekommunikationsüberwachung, Auswertung, Analyse und Prävention sowie die Zentrale Internetrecherche und die Auswertestelle für Kinderpornografie.

Dort ist auch die ZAC für die Wirtschaft angesiedelt[156].

Cyberwehr – Baden-Württemberg
Die Cyberwehr ist eine Kontakt- und Beratungsstelle für kleine und mittlere Unternehmen sowie eine Koordinierungsstelle bei Cyberangriffen. Derzeit befindet sie sich in der Pilotphase, in der sie ausschließlich in den Stadt- und Landkreisen Karlsruhe, Rastatt, Baden-Baden zur Verfügung steht. Langfristig ist das Ziel der landesweite Aufbau regionaler Infrastrukturen für die Ersthilfe im Falle eines IT-Sicherheitsvorfalls. Die eingerichtete Hotline dient als erste Anlaufstelle und einheitliche Notfallnummer im Fall eines Cyberangriffs. Die Cyberwehr führt mit dem betroffenen Unternehmen ein mehrstündiges Telefonat, um eine initiale Vorfallsdiagnose zu stellen und stellt im Anschluss, wenn gewünscht, Expert:innen bereit, die das Unternehmen bei der Schadensbegrenzung unterstützen. Im Gegensatz zur Zentralen Anlaufstelle Cybercrime des Landeskriminalamts wird die Cyberwehr im Bereich der Angriffsabwehr und der Schadensbegrenzung erst aktiv, wenn ein Vorfall eingetreten ist. Die Aufgaben der Zentralen Anlaufstelle Cybercrime hingegen erstrecken sich auch präventive Maßnahmen sowie die Strafverfolgung im Schadensfall oder einem versuchten Angriff. Durch gesetzliche Regelungen hat die Anlaufstelle im Rahmen der Strafverfolgung exklusive Befugnisse zur Aufklärung des Sachverhalts oder des Verhinderns eines weiteren Angriffs.

Die Cyberwehr arbeitet eng mit der ZAC des LKA, dem Landesamt für Verfassungsschutz im Bereich der Cyberspionage und dem CERT BWL (Baden-Württemberg) sowie dem Forschungszentrum Informatik am Karlsruher Institut für Technologie zusammen[157].

Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken
Mit dem bei der Staatsanwaltschaft Saarbrücken angesiedelten Sonderdezernat „Cybercrime“ möchte das saarländische Justizministerium der Kriminalität im Netz entgegentreten. Das Dezernat soll mit dem Institut für Rechtsinformatik und dem CISPA Helmholtz Center for Information Security speziell geschult werden[158].

156 Polizei Nordrhein-Westfalen Landeskriminalamt, Das Cybercrime-Kompetenzzentrum beim LKA NRW.
157 Cyberwehr, Die Cyberwehr.
Staatsministerium Baden-Württemberg, Landesregierung initiiert „Cyberwehr Baden-Württemberg“.
158 Juristisches Internetprojekt Saarbrücken, Neues Dezernat „Cybercrime“ bei der Staatsanwaltschaft Saarbrücken.

Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern
Das Dezernat 45 des Landeskriminalamts in Mecklenburg-Vorpommern ermittelt mit Cybercrime-Spezialist:innen in solchen Fällen und beherbergt auch die mecklenburg-vorpommersche ZAC.

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[159].

Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz
Das Dezernat 47 nimmt eine Zentralstellenfunktion ein und unterstützt außerdem 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 Dezernat bildet außerdem die ZAC für Wirtschaftsunternehmen.

Das LKA ist Mitglied der Allianz für Cyber-Sicherheit[160].

Dezernat Cybercrime des Landeskriminalamtes Thüringen
Das Dezernat Cybercrime des Landeskriminalamts Thüringen beschäftigt sich unter anderem mit Betrug im Internet und Ermittlungen zu Kinder- und Jugendpornografie im Netz.

Das Dezernat beheimatet auch die ZAC Thüringens[161].

Dezernat LPP 222 Cybercrime – Saarland
Das Dezernat Cybercrime der saarländischen Kriminalpolizei setzt sich mit besonders schwerwiegenden Fällen auseinander, insbesondere wenn der öffentliche Bereich betroffen, ein sehr hoher Schaden entstanden oder die technischen Anforderungen hoch sind.

Die ZAC des Saarlandes ist ebenfalls dort angesiedelt[162].

159 Landeskriminalamt Mecklenburg-Vorpommern, Cybercrime in M-V. Aktuelle Aspekte.
Landespolizei Mecklenburg-Vorpommern, LKA-MV: Internationaler Ermittlungserfolg gegen Kinderpornografie-plattform im Darknet.
160 Polizei Rheinland-Pfalz, Aufgaben des Dezernates Cybercrime.
161 Heise Online, Cybercrime: Neue Herausforderungen für Thüringer LKA.
Ministerium für Inneres und Kommunales Thüringen, Internetkriminellen gemeinsam mit den Unternehmen das Handwerk legen.
162 sol.de, Saar-Kripo eröffnet neue „Cybercrime"-Dienststelle. (Website entfernt)

EMERGE IoT – Mecklenburg-Vorpommern
EMERGE IoT ist ein Kooperationsprojekt (gefördert durch den Fonds für die Innere Sicherheit der Europäischen Union), welches sich der Aufklärung, Verfolgung und Prävention von strafbaren Sachverhalten rund um das Internet der Dinge widmet. Ziel ist es, die technischen Grundlagen des Internets der Dinge zu analysieren und Werkzeuge zu entwickeln, die die Ermittlungen rund um mögliche Angriffsszenarien im Internet der Dinge erleichtern und verbessern können.

Beteiligt sind das LKA Mecklenburg-Vorpommern und die Universität Rostock[163]*.*

Fachkommissariat Cybercrime (LKA 54) – Hamburg
Die Polizei Hamburg hat mit dem Fachkommissariat eine Dienststelle geschaffen, die die Kompetenzen von kriminalpolizeilicher Ermittlung und angestellten Informatikern bündelt und so polizeiliches und technologisches Wissen zusammenführt.

Die ZAC in Hamburg ist dem Fachkommissariat angegliedert[164]*.*

Hessen Cyber Competence Center (Hessen3C)
Das Hessen Cyber Competence Center ist eine Kompetenzstelle, die eine interdisziplinäre Zusammenarbeit und institutionalisierte Kooperation staatlicher Behörden in 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.

Hessen3C tauscht sich mit der Hessischen Polizei und dem Hessischen Verfassungsschutz zu Cyberthemen aus und erstellt gemeinsam ein Lagebild. Mitarbeiter:innen des Hessen3Cs stammen aus dem CERT Hessens, der Polizei und des Landesamtes für Verfassungsschutz – 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. Es bestehen Arbeitsbeziehungen mit dem VCV, dem CERT-Bund sowie den weiteren Länder-CERTs. Seit März 2021 ist Hessen3C zudem im Cyber-AZ vertreten[165]*.*

163 Universität Rostock, Universität Rostock unterstützt das Landeskriminalamt Mecklenburg-Vorpommern in Sachen Cyber-Kriminalitätsbekämpfung.
164 Polizei Hamburg, Zentrale Ansprechstelle Cybercrime (ZAC).
165 Bundesverwaltungsamt, Referentin/Referent (m/w/d) im Hessen CyberCompetenceCenter. (Dieser Link läuft ggf. aus, bei Interesse kann eine Kopie bei den Autor:innen angefragt werden).
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.

Informationssicherheitsbeauftragte:r der Landesverwaltung (Länder-CISO)

- In Baden-Württemberg wird der:die Informationssicherheitsbeauftragte:r (Chief Information Security Officer, CISO) durch das dortige Innenministerium benannt. Ihm:ihr obliegt die Festlegung und Fortschreibung von Richtlinien im Bereich der Informationssicherheit für die Landesverwaltung, *die Beratung des Länder-CIO, sowie die Erarbeitung eines jährlichen Berichts zur Lage der Umsetzung und Wirksamkeit von vorgenommenen Maßnahmen im Bereich der IT-Sicherheit, welcher wiederum dem Länder-CIO vorgelegt wird*[166].
- Bayern's IT-Sicherheitsbeauftragte:r (CISO) ist im Bayerischen Staatsministerium der Finanzen und für Heimat angesiedelt. Er:sie 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 und *ihm:ihr obliegt die Fachaufsicht über das bayerische CERT*[167].
- 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 der:dem Staatssektretär:in. Für den Bereich der IT-Sicherheit obliegt dem:der Landes-InfSiBe die fachliche Steuerung des ITDZ Berlin*[168].
- In Brandenburg wird ein:e landesweite:r IT-Sicherheitsmanager:in durch Abteilung 6 (Digitalisierung, E-Government und IT-Leitstelle) innerhalb des Ministerium des Innern und für Kommunales des Landes Brandenburg eingesetzt. Ihm:ihr kommt u. a. 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 informiert[169].
- Der:die Bremer CISO ist bei der:dem Senator:in für Finanzen der Hansestadt angesiedelt. Seit der erstmaligen Vorlage im Juli 2020 erstellt der:die Bremer CISO einen nicht-öffentlichen Jahresbericht zur Informationssicherheit in der bremischen Verwaltung, um Probleme, Lösungen und Alternativen zu adressieren[170].
- In der Freien Hansestadt Hamburg wurde ein:e Informationssicherheitsbeauftragte:r (InSiBe) innerhalb des Amtes für IT und Digitalisierung der Senatskanzlei

166 Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit.
167 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.
168 Senatsverwaltung für Inneres und Sport Berlin, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin.
169 Brandenburgisches Vorschriftensystem, Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg.
170 CISO Bremen, Vorlage für die Sitzung des Senats am 14.7.2020. Jahresbericht zur Informationssicherheit in der bremischen Verwaltung.

Hamburg, *dem wiederum der:die Landes-CIO vorsteht, eingerichtet*[171].

- Derzeit ist in Hessen der:die Leiter:in der Abteilung VII „Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung" des dortigen Ministeriums des Innern und für Sport in Personalunion der:die Landes-CISO.
  Ein:e Vertreter:in des Hessen3C agiert als seine:ihre Stellvertreter:in[172].
- In Mecklenburg-Vorpommern ist der:die Beauftragte:r für Informationssicherheit (BeLVIS) im Ministerium für Inneres und Europa des Landes angesiedelt.
  Er:sie berichtet dem Landes-CIO und koordiniert das ressortübergeifende Informationssicherheitsmanagement. Dem:der BeLVIS untersteht das CERT M-V und er:sie vertritt Mecklenburg-Vorpommern u. a. im VCV[173].
- Das Informationssicherheitsmanagement der Landesverwaltung in Niedersachsen verantwortet ein:e Informationssicherheitsbeauftragte:r (CISO), der:die im niedersächsischen Ministerium für Inneres und Sport angesiedelt ist[174].
- Der Posten der:des Informationssicherheitsbeauftragten des Landes Nordrhein-Westfalen fällt dem:der Leiter:in des Referates II B 4 (Informationssicherheit in der Landesverwaltung) innerhalb des dortigen Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie zu[175].
- In Rheinland-Pfalz ist der:die Informationssicherheitsbeauftragte:r der Landesverwaltung (CISO-rlp) in Referat 392 (Ressortübergreifende Informationssicherheit) der Abteilung 9 (IT-Zentralstelle, Breitband) des dortigen Ministeriums des Innern und für Sport beheimatet.
  Enger Austausch besteht mit dem BSI, CERT-rlp sowie den Sicherheitsbehörden des Landes[176].
- Im Saarland kommt dem:der Leiter:in der Stabsstelle Informationssicherheitsmanagement und IT-Recht im saarländischen Ministerium für Finanzen und Europa auch die Funktion des:der CISO zu.
  Er:sie verfügt über ein direktes Vortragsrecht gegenüber dem:der Länder-CIO, berichtet zu Risiken und Stand der Umsetzung von IT-Sicherheitsmaßnahmen und kann ggf. Maßnahmen zur Eindämmung ersterer empfehlen[177].
- Der:die sächsische Beauftragte:r für Informationssicherheit des Landes (BfIS) ist zeitgleich Leiter:in des Referats 45 in der Sächsischen Staatskanzlei, das sich mit Informations- und Cybersicherheit sowie kritischen Infrastrukturen befasst.
  Er:sie wird durch den:die Länder-CIO benannt und verfügt über ein unmittelbares Vorspracherecht. Er:sie ist Mitglied in der AG Informationssicherheit des IT-Pla-

171 Freie Hansestadt Hamburg, Rahmen-Sicherheitskonzept.
172 Ministerium des Innern und für Sport Hessen, Der zentrale Informationssicherheitsbeauftragte der Landesverwaltung.
Hessischer Landtag (Drucksache 20/1520), Antwort auf Kleine Anfrage: Umsetzung Informationssicherheitsrichtlinie.
173 DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, DVZ.info 02/14.
Ministerium für Inneres und Sport Mecklenburg-Vorpommern, Stellenausschreibung Beauftragte/Beauftragter der Landesverwaltung für Informationssicherheit.
174 Ministerium für Inneres und Sport Niedersachsen, Informationssicherheit.
Ministerium für Inneres und Sport, Informationssicherheit in Niedersachsen.
175 Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie Nordrhein-Westfalen, Geschäftsverteilungsplan.
176 Ministerium der Justiz Rheinland-Pfalz, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Rheinland-Pfalz.
Ministerium des Innern und für Sport Rheinland-Pfalz, Stellenausschreibung Referentin / Referenten (m/w/d) im Referat 392.
177 Ministerium für Finanzen und Europa Saarland, Stabstelle Informationssicherheit und IT-Recht.

nungsrates, einer Länderarbeitsgruppe der IMK, sowie der ACS und UP KRITIS[178].

- Das Ministerium der Finanzen in Sachsen-Anhalt beheimatet neben dem:der Landes-CIO auch den:die Informationssicherheitsbeauftragte:r des Landes (CISO).
  Er:sie unterrichtet den:die CIO und verantwortet Prozesse zur Umsetzung und Einhaltung von Informationssicherheitsstandards[179].
- In Schleswig-Holstein ist der:die Informationssicherheitsbeauftragte:r für die Landesverwaltung (CISO) innerhalb des zentralen IT-Sicherheitsmanagements (Abteilung 3) des dortigen Ministeriums für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung angesiedelt. Der:dem CISO obliegt das ressortübergreifende Informationssicherheitsmanagement.
  Er:sie verfügt über ein Vortragsrecht ggü. dem:der als Länder-CIO agierenden Staatssekretär:in und ist zudem in der AG InfoSic des IT-PLR für Schleswig-Holstein vertreten[180].
- Der:die thüringische IT-Sicherheitsbeauftragte:r wird durch das für E-Government und ressortübergreifende Thüringische Finanzministerium eingesetzt und *ist unmittelbar dem:der Landes-CIO unterstellt*[181].

Kompetenz- und Forschungszentren für IT-Sicherheit (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 gefördert[182].

Kompetenzzentrum Cybercrime – Bayern
Das Kompetenzzentrum Cybercrime (Dezernat 54) wurde beim Landeskriminalamt Bayern eingerichtet. Eine der Aufgaben des Kompetenzzentrum Cybercrime ist es, den Ernstfall, also beispielsweise einen Cyberangriff, 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 Cyberkriminalität an, die überregionale Bedeutung haben und von den örtlichen Polizeidienststellen nicht bearbeitet werden können[183].

178 Sächsische Staatskanzlei, Beauftragter für Informationssicherheit des Landes (BfIS).
179 Ministerium der Finanzen Sachsen-Anhalt, Organisationsplan.
Ministerium für Justiz und Gleichstellung Sachsen-Anhalt, Leitlinie zur Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt.
180 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.
181 Finanzministerium Thüringen, Informationssicherheitsleitlinie der Thüringer Landesverwaltung.
182 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.
183 Bayerische Staatsregierung, Cyber-Kompetenzzentrum im Landeskriminalamt.

Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen
Im August 2020 wurde die Einrichtung der Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen durch das Landeskabinett beschlossen.

Diese soll als Servicestelle der Landesregierung in der neuen Digitalabteilung des Innenministeriums Nordrhein-Westfalen angesiedelt werden und hat die Aufgabe, Informationen zur Cybersicherheit des Bundeslandes für die Landesverwaltung zu bündeln und als Schnittstelle zum BSI zu fungieren. Es können sich zudem Überschneidungen mit den Zuständigkeitsbereichen des Verfassungsschutzes und dem Cybercrime-Kompetenzzentrum des Landeskriminalamts im Bereich der Cybersicherheit und Cyberabwehr ergeben[184].

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 Kommunen und Bürger beratend unterstützen.

Das LSI ist Mitglied im VCV, beheimatet das Bayern-CERT und kooperiert mit dem BSI[185].

Landesbeauftragte:r für Informationstechnologie (Länder-CIO)
Die folgenden Bundesländer haben eine:n Beauftragte für Informationstechnologie, eine:n sogenannten CIO (Chief Information Officer) des Landes, bestimmt:

- 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 Innenministerium Baden-Württembergs zugeordnet[186].
- Das Land Bayern hat eine:n Beauftragte:n für Informations- und Kommunikationstechnik der Bayerischen Staatsregierung (CIO Bayern) bestimmt. Der:die CIO Bayern übernimmt beispielsweise Verantwortung für die IT- und E-Government-Strategie sowie die Digitalisierung der Verwaltung und vertritt Bayern im IT-Planungsrat. Aktuell wird die Position von der Bayerischen Staatsministerin für Digitales ausgefüllt[187].
- In Berlin übernimmt die Staatssekretärin für Informations- und Kommunikationstechnik in der Senatsverwaltung für Inneres und Sport Berlin die Position des Landes-CIOs, die an den:die Innensenator:in berichtet. Er:sie vertritt das Land Berlin im IT-Planungsrat[188].

184 Behörden Spiegel, Neue Koordinierungsstelle für Cyber-Sicherheit in NRW.
Ministerium des Inneren des Landes Nordrhein-Westfalen, Kabinett beschließt Einrichtung von Koordinierungsstelle für Cybersicherheit.
185 Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.
186 CIO Baden-Württemberg, Stefan Krebs.
187 Bayerisches Staatsministerium für Digitales, IT-Beauftragte der Bayerischen Staatsregierung.
188 CIO, Sabine Smentek wird CIO vom Land Berlin.

- Das Land Brandenburg hat eine:n Chief Process Innovation Officer bestimmt, der:die sich auch im IT-Angelegenheiten des Landes kümmert. Er:sie ist im Innenministerium angesiedelt[189].
- In Bremen ist die CIO-Stelle beim Staatsrat des Finanzressorts verortet[190].
- Hamburg bestimmt eine:n Chief Digital Officer, der:die das Amt für IT und Digitalisierung leitet[191].
- Der:die CIO des Landes Hessen ist für die Informationstechnologie und E-Government-Themen des Landes zuständig. Der:die CIO ist im Hessischen Ministerium für Digitale Strategie und Entwicklung angesiedelt und vertritt Hessen im IT-Planungsrat[192].
- In Mecklenburg-Vorpommern ist die Position des:der CIO durch das Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern besetzt[193].
- Der:die CIO Niedersachsens leitet die Stabsstelle „Informationstechnik der Landesverwaltung“ des Ministeriums für Inneres und Sport. Neben der IT-Strategie und E-Government zählt auch die Verwaltungsmodernisierung zu den Aufgaben des:der CIO[194].
- Der:die CIO Nordrhein-Westfalens ist im Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie angesiedelt. Der:die CIO übernimmt die Steuerung der IT ebenso wie beispielsweise Aufgaben der Standardisierung und die Vertretung des Landes im IT-Planungsrat[195].
- 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“[196].
- Auch das Saarland hat eine:n CIO, den:die Bevollmächtigte:n des Saarlandes für Innovation und Strategie[197].
- Sachsens CIO ist aktuell der:die Amtschef:in der Sächsischen Staatskanzlei, der:die für die Stabsstelle „Landesweite Organisationsplanung, Personalstrategie und Verwaltungsmodernisierung“ zuständig ist und das Land im IT-Planungsrat vertritt[198].
- Aktuell stellt das Finanzministerium von Sachsen-Anhalt den:die Landes-CIO, der:die Beauftragte:r der Landesregierung für Informations- und Kommunikati-

189 CIO, Die IT-Chefs der Bundesländer.
190 Freie Hansestadt Bremen, Staatsrat Dr. Martin Hagen.
191 Senatskanzlei Hamburg, Senatskanzlei Amt für IT und Digitalisierung.
192 Hessische Ministerin für Digitale Strategie und Entwicklung, CIO.
193 Regierung Mecklenburg-Vorpommern, Staatssekretärin Ina-Maria Ulbrich.
194 Niedersächsisches Ministerium für Inneres und Sport, Neuer CIO in Niedersachsen: Dr. Horst Baier ist IT-Bevollmächtigter der Landesregierung.
195 Die Landesregierung Nordrhein-Westfalen, Prof. Andreas Meyer-Falcke neuer CIO.
196 Ministerium des Innern und für Sport Rheinland-Pfalz, Digitale Verwaltung Rheinland-Pfalz.
197 Staatskanzlei Saarland, Bevollmächtigter für Innovation und Strategie Chief Information Officer (CIO).
198 Sächsische Staatskanzlei, Staatssekretäre.

onstechnik ist und Sachsen-Anhalt im IT-Planungsrat vertritt[199].
- Der:die CIO in Schleswig-Holstein ist zuständig für das Zentrale IT-Management Schleswig-Holstein und ist an die Staatskanzlei angebunden[200].
- Der:die CIO von Thüringen ist im Finanzministerium des Landes angesiedelt und für die Vereinheitlichung von IT- und E-Government-Strukturen verantwortlich[201].

Landesbehörden für Verfassungsschutz (LfV)

- Innerhalb des Landesamts für Verfassungsschutz Baden-Württemberg befasst sich vor allen Dingen die Abteilung 4 mit cybersicherheitsrelevanten Arbeitsfeldern. Dort sind u. a. Zuständigkeiten für Spionage- und Cyberabwehr sowie Geheim- und Sabotageschutz angesiedelt[202].
- In Bayern befasst sich das dortige Landesamt für Verfassungsschutz in seiner Abteilung 5 u. a. mit Wirtschaftsschutz und Spionageabwehr. Dort ist ebenfalls das Cyber-Allianz-Zentrum Bayern (CAZ) und die ihm unterstellte Cyberabwehr angesiedelt[203].
- Die Senatsverwaltung für Inneres und Sport Berlins beherbergt die Verfassungsschutzbehörde des Landes (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 Senatsverwaltung an das BfV übertragen*[204].
- In Brandenburg ist die Landesverfassungsschutzbehörde im Ministerium des Innern und für Kommunales des Landes angesiedelt (Abteilung 5). Unter ihre Arbeitsfelder fallen u. a. die Spionageabwehr und der Wirtschaftsschutz. Im letzten Brandenburger Verfassungsschutzbericht wird u. a. auch auf aktuelle Entwicklungen im sog. „Cyber-Extremismus“ Bezug genommen[205].
- In der Eigenbeschreibung des Bremer Landesamts für Verfassungsschutz, sowie im letzten Bremer Verfassungsschutzbericht wird auf keine originäre Zuständigkeit für Wirtschaftsschutz oder Cyberabwehr Bezug genommen[206].
- Im Landesamt für Verfassungsschutz Hamburg wird in der Abteilung V3 u. a. zur Spionageabwehr gearbeitet. Das unterstellte Referat V32 verfügt über Kompetenzen und Aufgaben im Bereich des Wirtschaftsschutzes. Sein letzter Verfas-

199 Sachsen-Anhalt, Der Beauftragte der Landesregierung für Informationstechnik (CIO).
200 Schleswig-Holstein, E-Government – Steuerung und Zusammenarbeit.
201 Freistaat Thüringen, CIO des Freistaats Thüringen.
202 Landesamt für Verfassungsschutz Baden-Württemberg, Aufbau und Organisation.
Landesamt für Verfassungsschutz Baden-Württemberg, Cyberspionage.
203 Landesamt für Verfassungsschutz Bayern, Organisation.
Landesamt für Verfassungsschutz Bayern, Spionageabwehr / Wirtschaftsschutz.
204 Senatsverwaltung für Inneres und Sport Berlin, Organigramm.
Senatsverwaltung für Inneres und Sport Berlin, Verfassungsschutzbericht 2019.
205 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.
206 Landesamt für Verfassungsschutz Bremen, Über Uns.
Freie Hansestadt Bremen, Verfassungsschutzbericht 2019.

sungsschutzbericht verweist zudem auf Gefahren durch Cyberspionage, Cybersabotage und Cyberangriffe[207].

- Im Landesamt für Verfassungsschutz Hessen befasst sich das Dezernat 30 mit der Spionageabwehr und Wirtschaftsschutz. Zum Schutz der Wirtschaft wird Cyberspionage als ein expliziter Aufgabenbereich aufgeführt[208].
- In Mecklenburg-Vorpommern ist die Landesverfassungsschutzbehörde im Ministerium für Inneres und Europa angesiedelt. Unter das Arbeitsfeld Spionageabwehr und Wirtschaftsschutz fallen u. a. Bedrohungen durch Cyberangriffe und Wirtschaftsspionage[209].
- Die niedersächsische Landesverfassungsschutzbehörde (Abteilung 5), angesiedelt im dortigen Ministerium für Inneres und Sport, befasst sich u. a. 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 u. a. „Daten im Kontext von IT-gestützten Spionage- und Sabotageoperationen fremder Nachrichtendienste erhoben, gesammelt, analysiert und bewertet“[210].
- Das Ministerium des Innern des Landes Nordrhein-Westfalen beherbergt die Verfassungsschutzbehörde des Landes. Dort (Abteilung 6, Gruppe 61) befinden sich Zuständigkeiten für ein Cyber-Zentrum für Analysen, Prototyping und Internetaufklärung (Referat 611) sowie Spionageabwehr, Wirtschaftsschutz und Cyberabwehr (Referat 613)[211].
- In Rheinland-Pfalz ist die Landesverfassungsschutzbehörde im Ministerium des Innern und für Sport des Landes institutionell angesiedelt. Unter ihre Aufgabenbereiche fallen u. a. Spionage, Cyberabwehr sowie Wirtschaftsschutz[212].
- Das Ministerium für Inneres, Bauen und Sport des Saarlandes beherbergt die dortige Landesverfassungsschutzbehörde. Dort wird u. a. zur Spionageabwehr und Wirtschaftsschutz gearbeitet. Der letzte saarländische Verfassungsschutzbericht verweist auf Gefahren durch Cyber- und elektronische Angriffe[213].
- Das sächsische Landesamt für Verfassungsschutz ist institutionell im dortigen Staatsministerium des Innern aufgehängt. *Enge Arbeitsbeziehungen bestehen mit BfV, seinen Counterparts in allen Bundesländern, dem BND, dem MAD, dem BSI sowie dem Cyber-AZ*[214].
- In Sachsen-Anhalt befindet sich die Landesverfassungsschutzbehörde im Minis-

207 Landesamt für Verfassungsschutz Hamburg, Organigramm des Landesamtes für Verfassungsschutz.
Behörde für Inneres und Sport Freie Hansestadt Hamburg, Verfassungsschutzbericht 2019.
208 Landesamt für Verfassungsschutz Hessen, Organigramm.
Landesamt für Verfassungsschutz Hessen, Wirtschaftsschutz. Was ist Cyberspionage?.
209 Ministerium für Inneres und Europa Mecklenburg-Vorpommern, Spionageabwehr und Wirtschaftsschutz.
210 Ministerium für Inneres und Spor Niedersachsen, Die Cyberabwehr beim Verfassungsschutz Niedersachsen.
Ministeriums für Inneres und Sport Niedersachsen, Organisationsplan des Niedersächsischen Ministeriums für Inneres und Sport.
211 Ministerium des Innern Nordrhein-Westfalen, Organisationsplan.
212 Ministerium des Innern und für Sport Rheinland-Pfalz, Spionageabwehr, Wirtschaftsschutz und Cybersicherheit.
213 Ministerium des Innern, Bauen und Sport Saarland, Lagebild Verfassungsschutz 2019.
214 Staatsministerium des Innern Sachsen, Sächsischer Verfassungsschutzbericht 2019.

terium für Inneres und Sport (Abteilung 4). Im Referat 44 ist eine Zuständigkeit für Spionageabwehr und Wirtschaftsschutz verortet. Gemäß sachsen-anhaltischen Verfassungsschutzbericht fallen unter Spionageabwehr auch Cyberangriffe[215].

- Die Landesverfassungsschutzbehörde des Landes Schleswig-Holstein ist im dortigen Ministerium für Inneres, ländliche Räume und Integration angesiedelt (Abteilung IV 7). Unter ihre Arbeitsfelder fällt u. a. Spionageabwehr und Wirtschaftsschutz. Ein weiteres Referat (IV 76) befasst sich darüber hinaus mit „Digitale[m] Arbeiten, IT, G10 und Geheimschutz“[216].
- In Thüringen ist das Landesamt für Verfassungsschutz innerhalb des Thüringer Ministerium für Inneres und Kommunales organisatorisch angesiedelt. Im Rahmen des Referats 54 wird sich dort mit der Spionageabwehr befasst, welche auch Cyberabwehr sowie Wirtschaftsschutz beinhaltet[217].

Netzverweis.de – Mecklenburg-Vorpommern

Der Internetauftritt netzverweis.de ist eine gemeinsame Initiative des Landeskriminalamtes Mecklenburg-Vorpommern und der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH unter der Schirmherrschaft des Ministeriums für Inneres und Europa. 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 bearbeitet und verfolgt[218].

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 ab[219].

Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus

Bei der Staatsanwaltschaft Cottbus ist die brandenburgische Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer und Datennetzkriminalität angesiedelt[220].

215 Ministerium für Inneres und Sport Sachsen-Anhalt, Organisationsplan.
Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Verfassungsschutzbericht 2019.
216 Der Ministerpräsident des Landes Schleswig-Holstein, Spionageabwehr und Wirtschaftsschutz.
Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung, Organisationsplan.
217 Ministerium für Inneres und Kommunales Thüringen, Organigramm.
Ministerium für Inneres und Kommunales Thüringen, Wirtschaftsspionage / Wirtschaftsschutz.
218 Netzverweis, Online-Meldestelle.
Regierung Mecklenburg-Vorpommern, Landesregierung.
219 Justiz Online in Mecklenburg-Vorpommern, Zuständigkeit.
220 Staatsanwaltschaft Cottbus, Schwerpunktstaatsanwaltschaft. (Webseite entfernt)

Sicherheitskooperation Cybercrime
Die Sicherheitskooperation ist eine Initiative der Landeskriminalämter aus sechs Bundesländern (Baden-Württemberg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz und Sachsen) und des Bitkom, die eine Plattform für Polizei und Digitalwirtschaft bietet, um gemeinsam den Gefahren durch Cybercrime zu begegnen und dazu Wissen und technische Kompetenzen auszutauschen[221].

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-Handel[222].

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC)
Die Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft stehen Unternehmen präventiv und reaktiv im Falle von Internetstraftaten zur Verfügung. In jedem Bundesland ermitteln speziell ausgebildete Polizeibeamte:innen gemeinsam mit IT-Spezialisten:innen. Auf Länderebene sind die ZAC meist beim LKA angesiedelt, gegebenenfalls auch bei den dort bereits aufgebauten Cyber-Kompetenzzentren (siehe Beschreibungen der Kompetenzzentren). Die ZAC auf Bundesebene ist unter anderem bei der BPol angesiedelt[223].

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 arbeitet die Zentralstelle auch zu verfahrensunabhängigen Fragestellungen im Bereich der Cyberkriminalität.

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 der bayerischen Polizei oder des BKAs und mit internationalen Partnern, beispielsweise bei Verfahren zu organisierter Cyberkriminalität. Die Zentralstelle ist Mitglied in der ACS[224].

221 Sicherheitskooperation Cybercrime, Aktivitäten.
Sicherheitskooperation Cybercrime, Die Kooperation.
222 Diana Nadeborn, Berliner Staatsanwaltschaft rüstet auf gegen Cyberkriminalität.
223 Bundeskriminalamt, Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft.
Der Polizeipräsident in Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.
224 Bundesamt für Sicherheit in der Informationstechnik, Teilnehmerliste der Allianz für Cyber-Sicherheit.
Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB).

Zentralstelle Cybercrime Sachsen (ZCS)
Die bei der Generalstaatsanwaltschaft Dresden angesiedelte Zentralstelle ist das justizielle Gegenstück zum SN4C des Landeskriminalamtes Sachsen und fokussiert sich auf die Verfolgung von Straftaten mit Internetbezug[225].

Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität – Baden-Württemberg
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 Baden-Württemberg[226].

Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) – Hessen
Die Zentralstelle wurde als Außenstelle der Generalstaatsanwaltschaft Frankfurt (a.M.) in Gießen errichtet. Sie ist die operative Zentralstelle bei besonders aufwändigen 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 European Judicial Cybercrime Network[227].

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 ZAC Nordrhein-Westfalen, die beim Landeskriminalamt angesiedelt ist) ist bei der Staatsanwaltschaft Köln die landesweit

225 Staatsministerium der Justiz, Sächsisches Justizministerialblatt Nr. 5/2018.
MDR Sachsen, Sachsen fehlen Polizisten fürs Netz. (Website entfernt)
226 Ministerium der Justiz und für Europa Baden-Württemberg, Zentralstelle für die Bekämpfung von informations- und Kommunikationskriminalität eingerichtet. (Webseite entfernt)
227 Staatsanwaltschaften Hessen, Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT).

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[228]*.*

228 Justiz-ONLINE, Zentral- und Ansprechstelle Cybercrime (ZAC NRW).

8. Erläuterung – Akteure auf Kommunalebene

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 u. a. eine Kooperation mit der KGSt[229].

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-Grundschutzstandards verantworten[230]. Ihnen bietet das IT-SiBe-Forum Möglichkeiten für Informations- und Erfahrungsaustausch. Grundsätze des IT-SiBe-Forums stellen hierbei u. a. die Wahrung der kommunalen Selbstverwaltung, gegenseitige Unterstützung sowie eine Bündelungsfunktion für Ebenen übergreifende Zusammenarbeit dar.

Aus dem IT-SiBe-Forum bilden sich zudem Arbeitsgruppen der kommunalen Spitzenverbände mit Praktikern der IT-Sicherheit aus der Kommunalebene. Zuletzt war das

229 Vitako, Gremien.
Vitako. Satzung.
Vitako, Verband.
Vitako, Verein.

230 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.

IT-SiBe-Forum in diesem Kontext u. a. an der Überarbeitung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ sowie der „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ aktiv beteiligt[231].

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 vertreten[232].

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- 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.

231 Heino Sauerbrey, Ziel und Zweck des Internetforums für IT-Sicherheitsbeauftragte der Länder und Kommunen.
IT-SiBe-Forum, Grundsätze.
IT-SiBe-Forum, Kurzinformation.
IT-SiBe-Forum, Meilensteine.

232 KGSt, Über Uns.
KGSt, IT-Strategie, IT-Steuerung und Informationssicherheit.
KGSt, Organisation, Digitales und IT.
KGSt, Innovationszirkel: Digitales und IT-Steuerung.

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-Angriffe 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 Verteter: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[233]*.*

Kommunalgremium des IT-Planungsrates

Unter dem Vorsitz der FITKO wurde 2020 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 FITKO 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. Gegenüber dem IT-Planungsrat agiert das FITKO-Kommunalgremium als beratendes Organ auf strategischer Ebene und erstattet über die FITKO regelmäßig Bericht. Neben monatlichen virtuellen Treffen sind zwei jährliche persönliche Zusammenkünfte pro Jahr vorgesehen.

In dem Kommunalgremium (insgesamt 14 Mitglieder) sind je drei Vertreter:innen der Landkreise, Städte und Gemeinden inklusive ihres Spitzenverbandes, drei Vertreter:innen der Vitako sowie zwei Vertreter:innen der KGSt vertreten[234]*.*

233 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.
Klaus Schubert & Martina Klein, Kommunale Spitzenverbände.

234 FITKO, Wie unterstützt die FITKO die Digitale Transformation?.
Innenministerkonferenz, Bericht zum IT-Planungsrat.
KGSt, OZG-Umsetzung: Die kommunale Stimme stärken.

9. Gut zu wissen

Wenn Sie Fragen rund um IT-Sicherheit haben, können Sie kostenlos beim Bundesamt für Sicherheit in der Informationstechnik die Hotline des BSI für Bürger anrufen (0800 274 1000, Montag bis Freitag von 08:00 Uhr bis 18:00 Uhr)[235].

IT-Sicherheit versus Cybersicherheit: IT-Sicherheit hat eine relativ enge Definition, die sich aus dem Schutz der Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) von Daten zusammensetzt[236]. Im Verlauf der letzten Dekade nahm vor allem im anglo-amerikanischen, aber auch europäischen Raum der Gebrauch des Wortes Cybersicherheit im Vergleich zu IT-Sicherheit zu. Cybersicherheit ist breiter angelegt als IT-Sicherheit und umfasst zusätzlich auch sozio-kulturelle, politische, rechtliche und weitere Dimensionen[237]. Zusätzlich wird in Deutschland unter Cybersicherheit offiziell spätestens seit der Cyber-Sicherheitsstrategie für Deutschland 2016 nicht mehr nur noch die Erhöhung von IT-Sicherheit in den vorgenannten Dimensionen, sondern auch der Einsatz von teils invasiven Instrumenten zur Herstellung der öffentlichen Sicherheit verstanden – unter anderem durch den Einsatz des Bundestrojaners[238] oder Aktiver Cyberabwehr[239].

Es heißt jetzt Cybersicherheit ohne Bindestrich. Die Bundesregierung hat bis circa 2016/2017 bei Begriffen mit dem Bindestrich verwendet, dies geht unter anderem aus dem Glossar der Cyber-Sicherheitsstrategie für Deutschland 2016 hervor[240]. Spätestens seit 2018 werden Begriffe mit Cyber zusammengeschrieben, wie die Benennung der neuen Referate in der Abteilung Cyber- und Informationssicherheit im Bundesministerium des Innern, für Bau und Heimat[241] sowie die Namensgebung der Agentur für Innovation in der Cybersicherheit[242] und des Nationalen Pakts für Cybersicherheit[243] belegen.

Computer Emergency Response Team (CERT) versus Computer Security Incident Reponse Team (CSIRT): Bei CERTs und CSIRTs handelt es sich im digitale Notfallteams die staatlich, privatwirtschaftlich oder anderweitig organisiert sein können. Je nach Ausgestaltung können ihnen unterschiedliche Aufgaben zukommen, wie z. B. die Erstellung präventiver Handlungsempfehlungen zur Schadensvermeidung, das Hinweisen auf Schwachstellen in Hardware- und Software-Produkten, die Unterstützung bei der Reaktion auf IT-Sicherheitsvorfälle oder die Aussprache von Empfehlungen zur Schadensbegrenzung/-beseitigung. Inhaltlich gibt es keinen

235 Bundesamt für Sicherheit in der Informationstechnik, BSI für Bürger.
236 Bundesamt für Sicherheit in der Informationstechnik, Glossar.
237 Sven Herpig, Anti-War and the Cyber Triangle.
238 Netzpolitik.org, Bundestrojaner.
239 Sven Herpig, Hackback ist nicht gleich Hackback.
240 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
241 Bundesministerium des Innern, Organisationsplan.
242 Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.
243 Bundesministerium des Innern, für Bau und Heimat, Nationaler Pakt Cybersicherheit.

Unterschied zwischen CERTs und CSIRTs. Damit ein digitales Notfallteam sich aber CERT nennen kann, muss es sich vorab beim CERT Coordination Center an der Carnegie Mellon University registrieren. Ein Großteil der CERTs und CSIRTs sind im Forum of Incident Response and Security Teams (FIRST) Dachverband vertreten[244].

Cyberveranstaltungen. Mit der wachsenden Relevanz des Themas IT- und Cybersicherheitspolitik steigt auch die Anzahl der Veranstaltungen in dem Bereich. Allein für Deutschland ist ein Überblick über die Vielzahl an Konferenzen und weiteren Ereignissen kaum möglich. Um etwas mehr Übersicht zu schaffen, hat die Stiftung Neue Verantwortung hierfür einen entsprechenden Kalender online gestellt. Er ist unter www.stiftung-nv.de/de/cyber-veranstaltungskalender zu finden.

Was ist eigentlich **„Aktive Cyberabwehr“** (auch bekannt als „Hackback“)? Zu diesem Thema hat die SNV anhand von Veröffentlichungen und Hintergrundgesprächen eine kurze Handreichung mit Definition und Maßnahmenübersicht entwickelt, sowie eine Leseliste mit Analysen von Sachverständigen und anderen Akteuren zusammengestellt.

244 Carnegie Mellon University, Software Engineering Institute. FIRST, About FIRST.

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 Internationale Cyber-Sicherheitspolitik. Bei der SNV befasst Sven sich vorrangig mit der deutschen Cybersicherheitspolitik, Staatlichem Hacken (u. a. dem „Bundestrojaner“) und IT-Schwachstellenmanagement, dem Schutz der Wahlen in vernetzten Gesellschaften, Angriffen auf Machine Learning Anwendungen und der Resilienz-Strategie der Europäischen Union.

Christina Rupp ist Studentische Mitarbeiterin im Projekt Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung. Ihre Forschungsschwerpunkte liegen im Bereich der Cyberdiplomatie und Cyberaußenpolitik, insbesondere internationaler Normen für verantwortliches Verhalten im Cyberraum.

So erreichen Sie die Autor:innen:

Dr. Sven Herpig
Projektleiter für Internationale Cybersicherheitspolitik
sherpig@stiftung-nv.de
+49 (0) 30 81 45 03 78 91

Christina Rupp
Studentische Mitarbeiterin Internationale Cybersicherheitspolitik
crupp@stiftung-nv.de

Impressum

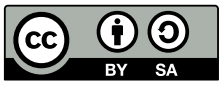
Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

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 CreativeCommons-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:
http://creativecommons.org/licenses/by-sa/4.0/