März 2020 · Dr. Sven Herpig & Rebecca Beigel

Akteure und Zuständigkeiten in der deutschen Cybersicherheits-politik

4. Auflage

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Inhalt

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 Bundesamt für Sicherheit in der Informationstechnik 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 Cyber-Sicherheitsstrategie für Deutschland[2]. Hierbei lag das Augenmerk vor allem auf dem neu zu schaffenden Nationalen Cyber-Abwehrzentrum (Cyber-AZ/NCAZ). Seitdem hat sich einiges getan: Cybersicherheit ist für die Sicherheitspolitik in Deutschland ein elementarer Bestandteil geworden, weswegen einige neue Akteure hinzugekommen sind. Hierzu zählen die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) und die Agentur für Innovation in der Cybersicherheit (ADIC). Jedoch gab es auch in der aktualisierten Version der Cyber-Sicherheitsstrategie für Deutschland 2016[3] keine grafische oder anderweitige Übersicht über die immer komplexer werdende Architektur deutscher Behörden im Cyberraum. Für eine effektive und effiziente deutsche Aufstellung im Cyberraum ist, gerade auch vor dem Hintergrund begrenzter Ressourcen[4], eine strukturierte politische Herangehensweise unverzichtbar.

Aus diesem Grund wollen wir im Rahmen unserer Arbeit zu Cybersicherheitspolitik an der Stiftung Neue Verantwortung hierzu einen Beitrag leisten. In dieser Veröffentlichung stellen wir eine grafische Abbildung der staatlichen Cybersicherheitsarchitektur, ein Abkürzungs- und Akteursverzeichnis sowie eine Erklärung der Verbindungen einzelner Akteure vor. In der aktuellen Version wurden Anpassungen an der EU-, Bund- und Länderebene vorgenommen. Weitere internationale Akteure (NATO, UN), kommunale Strukturen sowie Akteure der Privatwirtschaft, Wissenschaft und Zivilgesellschaft wurden bisher nicht berücksichtigt. Am Ende dieser Veröffentlichung findet sich

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 Julia Schütze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.

zusätzlich eine Seite mit wissenswerten Informationen rund im Cyber- und IT-Sicherheit in Deutschland.

Das Dokument wird auch zukünftig periodisch aktualisiert, um den neuesten Entwicklungsstand abzubilden und zusätzliche Erweiterungen vorzunehmen. Basis sind ausschließlich Open Source Informationen. Wir freuen uns daher über jeden Hinweis. Änderungs- und Ergänzungsvorschläge nimmt Rebecca Beigel gerne entgegen.

Die Verknüpfungen in der Visualisierung repräsentieren 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. Die Farben haben keine Bedeutung und dienen lediglich zur besseren Lesbarkeit.

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	Vorliegende Version

3. Akteure und Abkürzungen

AA	Auswärtiges Amt
AfCS/ACS	Allianz für Cyber-Sicherheit
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKS	Bundesakademie für Sicherheitspolitik
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BKAmt	Bundeskanzleramt
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
BWI	Bundesweite IT-Systemhaus GmbH
Bw	Bundeswehr
CAZ	Cyber-Allianz-Zentrum – Bayern

CCC	Cyber-Competence-Center – Brandenburg
CCCN	*European Cybersecurity Industrial, Technology and Research Competence Centre*
CEPO	Europäische Polizeiakademie
CERT-Bund	Computer Emergency Response Team des Bundes (CERT-Bund) und Bürger-CERT
CERT-EU	Computer Emergency Response Team der Europäischen Kommission
CERT-Verbund	Verbund von Computer Emergency Response Teams
CIH	Cyber Innovation Hub
CMPD	Direktion Krisenbewältigung und Planung
CODE	Forschungsinstitut Cyber Defence
cPPP	Contractual Public Private Partnership on Cybersecurity
CSIRTs Netzwerk	Computer Security Incident Response Teams Netzwerk
Cyberabwehr Bayern	
Cyberagentur	*Agentur für Innovation in der Cybersicherheit*
Cyberbündnis mit der Wirtschaft	
Cybercrime-Kompetenz-zentrum	Cybercrime-Kompetenzzentrum (Nordrhein-Westfalen)
Cyber Security Cluster Bonn	Cyber Security Cluster Bonn e. V.
Cyber-SR	Cyber-Sicherheitsrat
Cyberwehr	Cyberwehr (Baden-Württemberg)
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken	
Dezernat Cybercrime des Landeskriminalamtes Meck-lenburg-Vorpommern	
Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz	
Dezernat Cybercrime des Landeskriminalamtes Thüringen	
Dezernat LPP 222 Cybercrime	Dezernat LPP 222 Cybercrime (Saarland)
DIIS	*Deutsches Institut für Internet Sicherheit/ Deutsches Institut für Cyber-Sicherheit*
DsiN	Deutschland sicher im Netz e. V.

EAD	Europäischer Auswärtiger Dienst
ECCC	*Europäisches Kompetenzzentrum für Cybersicherheit*
ECSO	European Cyber Security Organisation
ECTEG	European Cybercrime Training and Education Group
EC3	European Cybercrime Center
EGC group	European Government CERTs group
EJCN	European Judicial Cybercrime Network
EJTN	European Judicial Training Network
EK	Europäische Kommission
EMERGE IoT	EMERGE IoT (Mecklenburg-Vorpommern)
ENISA	Agentur der Europäischen Union für Cybersicherheit
ENISA-Beratungsgruppe	
ER	Europäischer Rat
ERCC	Zentrum für die Koordination von Notfallmaßnahmen
EUCTF	European Union Cybercrime Task Force
EU Hybrid Fusion Cell	
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht
EUMS INT	Intelligence Directorate des EU-Militärstabs
Eurojust	
Europäische Gruppe für die Cybersicherheitszertifizierung	
Europol	European Union Agency for Law Enforcement Cooperation
EVA	Europäische Verteidigungsagentur
LKA 54	Fachkommissariat Cybercrime (Hamburg)
FITKO	*Föderale IT-Kooperation*
GD CONNECT	Generaldirektion Kommunikationsnetze, Inhalte und Technologien
GD DIGIT	Generaldirektion Informatik
GD HOME	Generaldirektion Migration und Inneres
GIZ	Gesellschaft für Internationale Zusammenarbeit
GMLZ	Gemeinsames Melde- und Lagezentrum

Gruppe der Interessenträger für die Cybersicherheitszertifizierung	
G4C	German Competence Centre against Cyber Crime e. V.
Hessen3C	Hessen Cyber Competence Center
Horizon 2020	
HWP	Horizontal Working Party on Cyber Issues
IMK	Innenministerkonferenz
Initiative IT-Sicherheit in der Wirtschaft	
Initiative Wirtschaftsschutz	
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-Planungsrat	
IT-Rat	
ITSMIG	IT Security made in Germany
ITZBund	Informationstechnikzentrum Bund
KdoCIR	Kommando Cyber- und Informationsraum
KdoITBw	Kommando Informationstechnik
KdoStratAufkl	Kommando Strategische Aufklärung
Kompetenz- und Forschungszentren für IT-Sicherheit	Kompetenz- und Forschungszentren für IT-Sicherheit (CISPA, ATHENE, KASTEL)
Kompetenzzentrum Cybercrime	Kompetenzzentrum Cybercrime (Bayern)
Kooperationsgruppe unter der NIS-Richtlinie	
Länder-CERTs	Computer Emergency Response Teams der Bundesländer: Bayern-CERT, H3C (Hessen), CERT BWL (Baden-Württemberg), CERT NRW (Nordrhein-Westfalen). SAX.CERT (Sachsen), N-CERT (Niedersachsen), CERT-rlp (Rheinland Pfalz), CERT-Brandenburg, Berliner CERT, CERT Nord (Bremen, Schleswig-Holstein, Hamburg und Sachsen-Anhalt), CERT M-V wird (Mecklenburg-Vorpommern), CERT Saarland, *ThüringenCERT*
LSI	Landesamt für Sicherheit in der Informationstechnik (Bayern)
LZ	Nationales IT-Lagezentrum

MeliCERTes	
Nationaler Pakt Cybersicherheit	
NCAZ Cyber-AZ	Nationales Cyber-Abwehrzentrum
Netzverweis.de	Netzverweis.de (Mecklenburg-Vorpommern)
NIS Platform	NIS Public-Private Platform
PESCO	Ständige Strukturierte Zusammenarbeit
PSK	Politisches und Sicherheitspolitisches Komitee
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus	
Sicherheitskooperation Cybercrime	
SKI-Kontaktgruppe	Kontaktgruppe zum Schutz kritischer Infrastrukturen
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	
SN4C	Cyber Crime Competence Center Sachsen
SOG-IS	Senior Officials Group Information Systems Security
SprinD	*Agentur für Sprunginnovationen*
SWP	Stiftung Wissenschaft und Politik
TF-CSIRT	Reference Incident Classification Taxonomy Task Force
TGG	(Common) Taxonomy Governance Group
Transferstelle „IT-Sicherheit in der Wirtschaft“	
Trusted Cloud	Kompetenznetzwerk Trusted Cloud
UniBw	Universität der Bundeswehr München
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen
VCV	Verwaltungs-CERT-Verbund
vzbv	Verbraucherzentrale Bundesverband
ZAC	Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft

ZAC NRW	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen
ZCB	Zentralstelle Cybercrime Bayern
ZCO	Zentrum Cyber-Operationen
ZCS	Zentralstelle Cybercrime Sachsen
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität (Baden-Württemberg)
ZIT	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (Hessen)
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
ZKA	Zollkriminalamt
4C	Cybercrime Competence Center (Sachsen-Anhalt)

Kursiv gedruckte Institutionen sind entweder in der Planung oder im Aufbau befindlich.

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 ist in ihrer Beratungsfunktion vor allem für Policy-Entwicklung und -Implementierung zuständig und spielt eine zentrale Rolle beim Kapazitätsaufbau und bei Sensibilisierungsmaßnahmen. Sie arbeitet daran, die operative Kooperation und das Krisenmanagement innerhalb der EU zu verbessern, für Kohärenz sektoraler Initiativen mit der NIS Directive zu sorgen und den Aufbau von Informationsaustausch- und Analysezentren in kritischen Sektoren zu unterstützen. ENISA ist außerdem Knotenpunkt für Information und Wissen in der Cybersicherheitscommunity. Infolge des Inkrafttretens des Rechtakts zur Cybersicherheit 2019 ist sie beauftragt „European cybersecurity certification schemes" als Grundlage für die Zertifizierung von Produkten, Prozessen und Dienstleistungen zur Unterstützung des digitalen Binnenmarktes zu entwickeln und hat ein permanentes Mandat für die Unterstützung der Mitgliedsstaaten in der Prävention und Abwehr von Cyberangriffen.

ENISA erstattet dem Europäischen Parlament regelmäßig Bericht über ihre Tätigkeiten und arbeitet mit relevanten Behörden der Mitgliedsstaaten 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. Im Jahr 2019 wurde ENISA von „European Network and Information Security Agency" in „European Union Agency for Cybersecurity" umbenannt. Die Abkürzung des ursprünglichen Namens bleibt dabei erhalten.[5]

5 European Commission, State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks.
European Union Agency for Cybersecurity, About ENISA.
European Commission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Bundesamt für Sicherheit in der Informationstechnik, BSI Magazin 2019/1.
Bundesamt für Sicherheit in der Informationstechnik, Cyber-Sicherheit: Nationale und Internationale Zusammenarbeit.

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. Nach einer erfolgreichen Pilotphase wurde es 2012 aufgebaut.

CERT-EU besteht aus Experten zentraler EU Institutionen (Europäische Kommission, Generalsekretariat des Rates, Europäisches Parlament, Europäischer Ausschuss der Regionen, Europäischer Wirtschafts- und Sozialausschuss). Es arbeitet eng mit anderen Computer Emergency Response Teams (CERTs) in den Mitgliedsstaaten zusammen und ist Mitglied des CSIRTs Netzwerks.[6]

(Common) 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".

Letzteres soll durch die Entwicklung einer gemeinsamen Taxonomie die Kooperation zwischen internationalen Strafverfolgungsbehörden und den Computer Security Incident Response Teams (CSIRTs) verbessern und Präventions- und Ermittlungsfähigkeiten stärken. An der Arbeitsgruppe beteiligen sich die ENISA und EC3.[7]

Contractual Public Private Partnership on Cybersecurity (cPPP)
Als Teil der Cybersicherheitsstrategie der EU wurde 2016 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 Cybersicherheits- Indust-

6 European Commission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.
Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
CERT-EU, About Us.

7 Europol, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.
Rossella Mattioli und Yonas Leguesse, Reference Incident Classification Taxonomy Task Force Update.

rie gefördert werden. Die EU wird bis zu 450 Mio. Euro unter dem Schirm des Programms Horizon 2020 investieren.[8]

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 Mitgliedsstaaten beizutragen. Es bildet ein Forum, durch das Mitgliedsstaaten kooperieren und so ihre Fähigkeiten zur Handhabung grenzüberschreitender Cybersicherheitsvorfälle verbessern und eine koordinierte Reaktion erarbeiten können.

Das CSIRTs Netzwerk setzt sich aus Repräsentanten der ernannten CSIRTs der Mitgliedsstaaten sowie des CERT-EU zusammen. 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.[9]

Direktion Krisenbewältigung und Planung (CMPD)
Das Direktorat spielt eine zentrale Rolle in der gemeinsamen Sicherheits- und Verteidigungspolitik der EU und ist verantwortlich für integriertes zivil-militärisches Planen innerhalb des Europäischen Auswärtigen Diensts. Das Ziel solchen strategischen Planens ist es mögliche Handlungsoptionen für die EU zu entwerfen und als Grundlage für Entscheidungen des Rates in internationalen Krisensituationen zu dienen – dabei geht es darum, was zu tun ist, warum, wo und mit wem.

Diese Optionen werden in sogenannten Crisis Management Concepts zusammengefasst und den EU Ministern vorgelegt. Sie bilden die Grundlage für operationale Planungen und Missionsdurchführungen.[10]

ENISA-Beratungsgruppe
Mit dem Cybersecurity Act wurde eine ENISA-Beratungsgruppe eingesetzt, die sich aus anerkannten Experten als Vertreter der einschlägigen Interessenträger zusammensetzt. Dazu gehören etwa die IT-Branche, Kleine und mittelständische Unternehmen, Betreiber „wesentlicher Dienste“, Verbraucherguppen und ausgewählte zuständige Behörden. Die Amtszeit der Mit-

8 ECSO, About the cPPP.

9 European Commission, 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.

10 European Union External Action, The Crisis Management and Planning Directorate (CMPD).

glieder beträgt zweieinhalb Jahre. Sachverständige der Kommission und der Mitgliedsstaaten können an den Sitzungen teilnehmen und an der Arbeit der Beratungsgruppe mitwirken, Vertreter anderer Stellen, können vom Exekutivdirektor der ENISA zur Teilnahme an Sitzungen hinzugerufen werden.

Die Beratungsgruppe berät die ENISA bei der Durchführung ihrer Aufgaben und insbesondere den Exekutivdirektor 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.[11]

EU Hybrid Fusion Cell
Die EU Hybrid Fusion Cell soll einen Fokus auf die Analyse hybrider Bedrohungen setzen und wird innerhalb des Zentrums für Informationsgewinnung und -analyse aufgebaut. Diese Zelle 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 Mitgliedsstaaten, sammeln, analysieren und teilen.

In Zusammenarbeit mit anderen existierenden ähnlichen Körperschaften der EU und der nationalen Ebene, soll die Zelle externe Aspekte hybrider Bedrohungen, die die EU und ihre Nachbarländer betreffen, analysieren um schnell relevante Vorfälle auszuwerten und so die strategische Entscheidungsfindung der EU zu unterstützen.[12]

Eurojust
In Bezug auf innere Sicherheit legt die EU einen besonderen Fokus auf organisierte Kriminalität, Terrorismus, Cyberkriminalität und Menschenschmuggel – Eurojust bildet dabei einen wichtigen Baustein in der operativen Bekämpfung dieser Gefahren. Die Behörde ist dafür zuständig, die Falluntersuchungen zu koordinieren, indem sie Informationsaustausch fördert, Bezüge zwischen laufenden Ermittlungen herstellt, strafrechtliche Strategien entwickelt und gemeinsames Handeln ermöglicht. Zu den Aufgaben von Eurojust gehören unter anderem die Informationsübertragung zu Eurojust zu

11 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).

12 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".

verbessern, eine On-Call Koordination für Notfälle aufzubauen und die Beziehungen zwischen Eurojust und nationalen Behörden, dem Europäischen Justiziellen Netz, Europol, dem Europäischen Amt für Betrugsbekämpfung, Frontex, dem Zentrum für Informationsgewinnung und -analyse und Drittstaaten zu fördern. 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 der Cyberkriminalitätseinheiten sowie auf Cyberkriminalität spezialisierten Strafverfolger zusammen. Zur Zerschlagung des Andromeda-Botnetzes koordinierte Eurojust die beteiligten Staatsanwaltschaften (in Deutschland: Staatsanwaltschaft Verden) und arbeitete dabei auch mit dem BSI zusammen.*[13]

Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA)
Seit 2012 verwaltet die Agentur integrierte IT-Großsysteme, die für die innere Sicherheit in den Schengen-Ländern sorgen, den Schengen-Ländern den Austausch von Visadaten ermöglichen und die Ermittlung, welches EU-Land für die Überprüfung eines bestimmten Asylantrags zuständig ist, leisten. Sie testet außerdem neue Technologien, die helfen sollen, ein moderneres, wirkungsvolleres und sicheres Grenzmanagementsystem in der EU aufzubauen.

Die Agentur arbeitet eng mit den Mitgliedsstaaten sowie auf EU-Ebene mit dem Europäischen Parlament, dem Datenschutzbeauftragten, dem Europäischen Rechnungshof, der EPA, der EASO, der FRAU, Frontex, dem EIGE, der EMCDDA, dem ER, der EK, der ENISA, Eurojust und Europol zusammen.[14]

Europäische Gruppe für die Cybersicherheitszertifizierung
Die Europäische Gruppe für die Cybersicherheitszertifizierung, die sich aus Vertretern der Mitgliedsländer zusammensetzt, trägt als Expertengruppe zur Entwicklung von Zertifizierungsschemata durch die Agentur der Europäischen Union für Netz- und Informationssicherheit bei. Für verschiedene Produkt- bzw. Servicetypen werden dabei spezifische Schemata entwickelt, die unter anderem die Gültigkeitsdauer von Sicherheitszertifikaten beinhalten.

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

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

Sie unterstützt die Kommission dabei, ein europäisches Arbeitsprogramm für Cybersicherheitszertifizierungsschemata aufzubauen. Das Arbeitsprogramm soll es beispielsweise der Industrie als strategisches Dokument erlauben, 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.[15]

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), das 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, HOME und DIGIT. Zudem sind das CERT-EU und das ERCC (ERCC über DG ECHO) bei der Kommission angegliedert.[16]

Europäische Polizeiakademie (CEPOL)
CEPOL ist als EU-Agentur dafür zuständig, Trainings für Gesetzeshüter zu entwickeln, umzusetzen und zu koordinieren. Sie schafft ein Netzwerk an

15 European Commission, 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)

16 Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".
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".
Europäische Kommission, ANHANG zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

Trainingsinstituten für Gesetzeshüter in den Mitgliedsstaaten und unterstützt sie dabei, Trainings zu Prioritäten im Sicherheitsbereich, zu Strafverfolgungskooperation und Informationsaustausch anzubieten. 2019 wurde die CEPOL Cybercrime Academy als Teil des Trainingsportfolios in Budapest eingeweiht. 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.[17]

Europäische Verteidigungsagentur (EVA)
Die Europäische Verteidigungsagentur wurde 2004 gegründet und unterstützt ihre 27 Mitgliedsstaaten (alle EU-Mitglieder außer Dänemark) bei der Entwicklung kooperativer europäischer Verteidigungsprojekte. Ein Ziel der EVA ist der Ausbau der Cyberabwehrfähigkeit. Sie unterstützt Mitgliedsstaaten bei der Entwicklung ihrer eigenen Abwehrfähigkeiten – Cyber Defense 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 hat die EVA 2018 ein Memorandum of Understanding unterzeichnet, mit dem Ziel einen Kooperationsrahmen für die Organisationen zu entwickeln.[18]

Europäischer Auswärtiger Dienst (EAD)
Der Europäische Auswärtige Dienst ist leitend im Bereich Cyberabwehr, Cyberdiplomatie und strategische Kommunikation. Der EAD hat ein eigenes System, um koordiniert auf Krisen und Notfälle (mit externer Dimension), zu reagieren: den Crisis Response Mechanism (CRM). Er wird bei sämtlichen Ereignissen ausgelöst, die tatsächlich oder potenziell die Sicherheitsinteressen der EU oder von Mitgliedsstaaten betreffen. Die Leitung des EAD obliegt dem:r High Representative of the Union for Foreign Affairs and Security Policy, der:die für die gemeinsame Außen- und Sicherheitspolitik sowie die Gemeinsame Sicherheits- und Verteidigungspolitik der Union zuständig und gleichzeitig Vize-Präsident der Europäischen Kommission ist, um kohärente

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

18 European Defense Agency, Four EU cybersecurity organisations enhance cooperation.
European Defense Agency, Our current priorities.
Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Die Europäische Union, Europäische Verteidigungsagentur (EVA).
European External Action Service, Permanent Structured Cooperation – PESCO.

Politik, auch im Bereich der Sicherheitspolitik im Cybersicherheitsbereich, zu garantieren.

Der EAD beherbergt EUMS INT, INTCEN und die dort untergebrachte EU Hybrid Fusion Cell, eine Analyseeinheit für hybride Bedrohungen. Zudem ist dort das CMPD angegliedert. EAD Vertreter haben den Vorsitz im PSK.[19]

Europäischer Rat (ER)
In erster Linie sind die EU-Mitgliedstaaten für ihre eigene Cybersicherheit zuständig. Im Europäischen Rat koordinieren sie sich auf EU-Ebene. 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:r Vertreter:in der Kommission, des Europäischen Auswärtigen Dienstes, der EU-Agenturen und der am meisten betroffenen Mitgliedsstaaten, sowie Expert:innen oder Mitglieder des Kabinetts de:rs Präsidenten:in des Rates beiwohnen können. Der Rat hat außerdem zahlreiche Gremien für Koordinierung und Informationsaustausch eingerichtet.*

Dazu gehört die Horizontale Gruppe „Fragen des Cyberraums“, die 2016 ins Leben gerufen wurde und „strategischel und horizontale Fragen des Cyberraums [koordiniert und] bei der Vorbereitung von Übungen und der Evaluierung ihrer Ergebnisse [hilft].“ Die Gruppe ist verantwortlich für die Koordinierung der Arbeit des Rates zu Cybersicherheitsthemen, insbesondere im Bereich Cyber Policy und gesetzlicher Neuerungen. Sie spielt deshalb, unter dem Vorsitz der rotierenden Präsidentschaft, auf Policy-Ebene gemeinsam mit dem Politischen und Sicherheitspolitischen Komitee eine zentrale Rolle in der Vorbereitung von Entscheidungen über Maßnahmen. Ihr Ziel ist, die interne Koordinierung zu stärken und ein umfassendes und zusammenhängendes EU-Vorgehen im Cyberbereich zu entwickeln. *Die Gruppe kooperiert*

19 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats “EU Playbook”.
Annegret Bendiek, Gemeinsame Außen- und Sicherheitspolitik: von der Transformation zur Resilienz.
IMPETUS, An Integral Element of the EU Comprehensive Approach.
European Union External Action, The Crisis Management and Planning Directorate (CMPD).
Europäischer Rat/Rat der Europäischen Union, Politisches und Sicherheitspolitisches Komitee (PSK).
European Union External Action Service, High Representative/Vice President.

eng mit anderen Gruppen, der Europäischen Kommission, dem EAD, Europol, Eurojust, FRA, EVA und ENISA.

Der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der Inneren Sicherheit (COSI) ist ein Vorbereitungsgremium des Rates. Sein Ziel ist es, operative Maßnahmen im Zusammenhang mit der inneren Sicherheit der EU zu stärken. Dabei „sorgt für eine wirksame operative Zusammenarbeit in Fragen der inneren Sicherheit der EU, nicht zuletzt bei der Strafverfolgung, den Grenzkontrollen und der justiziellen Zusammenarbeit in Strafsachen, beurteilt die allgemeine Ausrichtung und die Wirksamkeit der operativen Zusammenarbeit [und] unterstützt den Rat bei der Reaktion auf Terroranschläge oder Naturkatastrophen oder von Menschen verursachte Katastrophen".

Im Ausschuss beteiligt sind hohe Beamten der Innen- und/oder Justizministerien aller EU-Mitgliedsstaaten, Vertreter der Kommission sowie des EAD. Als Beobachter können Europol, Eurojust, Frontex, CEPOL oder andere einschlägige Gremien eingeladen werden.[20]

Europäisches Kompetenzzentrum für Cybersicherheit (ECCC)
Bereits im September 2018 legte die EU-Kommission eine Verordnung zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren vor. Das Kompetenzzentrum soll laut dieser Verordnung die „Durchführung der betreffenden Teile der Programme „DigitalesEuropa" und „HorizontEuropa", die Vergabe von Finanzhilfen und die Abwicklung der Auftragsvergabe" [21] übernehmen. Um die vorhandenen Mittel für Cybersicherheit innerhalb der Europäischen Union besser zu bündeln, soll das ECCC als

20 Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Europäischer Rat/Rat der Europäischen Union, Horizontal Working Party on Cyber Issues (HWP).
Council of the European Union, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.
Rat der Europäischen Union, Ständiger Ausschuss für die operative Zusammenarbeit im Bereich der Inneren Sicherheit (COSI).
Europäische Kommission, ANHANG zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.
Council of the European Union, The EU Integrated Political Crisis Response – IPCR – Arrangements.
Rat der Europäischen Union, Cyberangriffe: EU plant Gegenmaßnahmen, inklusive Sanktionen.
Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018).

21 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren.

„europäischen Partnerschaft eingerichtet“[22] werden, wodurch „gemeinsame Investitionen durch die Union, die Mitgliedstaaten und/oder die Industrie“[23] vereinfacht werden sollen. Die Etablierung des ECCC verzögert sich aufgrund ausbleibenden Verhandlungserfolgs zwischen EU-Abgeordneten und Regierungen über eine entsprechende Verordnung.

Das ECCC basiert auf einem Vorschlag der EK.[24]

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).[25]

European Cybercrime Center (EC3)
Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Europol wurde 2013 geschaffen, um die Reaktion der Strafverfolgungsbehörden auf Cyberkriminalität in der EU zu 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 zentralen Erkenntnissen und aufkommenden Bedrohungen und Entwicklungen im Bereich Cyberkriminalität. Das EC3 beherbergt die Joint Cybercrime Action Taskforce (J-CAT), deren Aufgabe es ist, informationsgeleitetes und koordiniertes Vorgehen gegen zentrale 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, die EZB sowie die ECTEG. Außerdem stellt das EC3

22 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren.

23 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren.

24 Netzpolitik, Neues EU-Kompetenzzentrum für Cybersicherheit bleibt umstritten.

25 Europol, About Europol.
Europol, European Cybercrime Centre – EC3.

gemeinsam mit dem CERT-EU forensische Analysen und andere technische Informationen für das CSIRTs Netzwerk bereit.[26]

European Cybercrime Training and Education Group (ECTEG)
Das ECTEG setzt sich zusammen aus Strafverfolgungsbehörden der Mitgliedsstaaten sowie Mitgliedsstaaten des Europäischen Wirtschaftsraums, internationalen Institutionen, der Wissenschaft, der privaten Industrie und Experten. Finanziert wird die Gruppe von der Europäischen Kommission. Ihr Ziel ist es, die globale Strafverfolgung auf Cyberkriminalitätsvorfälle vorzubereiten.

Sie arbeitet in enger Abstimmung mit dem EC3 und CEPOL zusammen, um Cyberkriminalitätstrainings grenzübergreifend zu harmonisieren, Wissensaustausch zu ermöglichen, eine Standardisierung von Methoden für Trainingsprogramme voranzubringen, mit Partnern aus der Wissenschaft eine anerkannte akademische Qualifizierung im Bereich Cyberkriminalität zu entwickeln und Trainings- und Lehrmaterial sowie Trainer für internationale Partner zu stellen. Aus Deutschland sind die Polizeiakademie Hessen und die Albstadt-Sigmaringen Universität beteiligt.[27]

European Cyber Security Organisation (ECSO)
Die European Cyber Security Organisation wurde 2016 in Belgien als finanziell unabhängige, selbst finanzierte gemeinnützige Organisation gegründet. Das ECSO verbindet europäische Akteure im Bereich Cybersicherheit innerhalb der EU-Mitgliedsstaaten, so beispielsweise Forschungszentren, aber auch Unternehmen, Endnutzer und Mitgliedsstaaten der Europäischen Wirtschaftsraums sowie Staaten, die mit Horizon 2020 in Verbindung stehen. Zielsetzungen der ECSO sind die Entwicklung eines kompetitiven europäischen Ökosystems, Unterstützung beim Schutz des European Digital

26 Europol, Cybercrime.
Europol, European Cybercrime Center – EC3.
Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Europol, EC3 Partners.
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.

27 ECTEG, European Cybercrime Training and Education Group.
ECTEG, Members.

Single Market mit vertrauenswürdigen Cybersicherheitslösungen und eine Beitragsleistung zur digitalen Autonomie der Europäischen Union.

Das ECSO ist Vertragspartner der Europäischen Kommission und ist in dieser Funktion für die Implementierung der öffentlich-privaten Partnerschaft für Cybersicherheit (cPPP) zuständig.[28]

European Cybersecurity Industrial, Technology and Research Competence Centre (CCCN)
Das European Cybersecurity Industrial, Technology and Research Competence Centre ist ein Teil des europäischen Vorschlags für ein Cybersecurity Competence Network and Centre und soll die europäische Autonomie in der Cybersicherheit stärken sowie den digitalen Binnenmarkt und die Wettbewerbsfähigkeit der europäischen Cybersicherheitsindustrie fördern. Das CCCN stellt das Instrument der Europäischen Union für Investitionen in Forschung, Technologie und industrieller Entwicklung im Bereich der Cybersicherheit dar und soll insbesondere die Koordinierung von Forschung und Innovation in der Cybersicherheit sicherstellen. Es dient ferner als Implementierungsmechanismus für finanzielle Mittel aus den Horizon Europe- und Digital Europe-Programmen, aus denen das Centre neben freiwilligen Beiträgen der EU-Mitgliedsstaaten, hauptsächlich finanziert werden soll. Das Zentrum soll außerdem das National Coordination Centres Network und die Cybersecurity Competence Community aufbauen und koordinieren.[29]

European Government CERTs group (EGC group)
Die European Government CERTs group ist ein informeller Zusammenschluss von Regierungs-CERTs in Europa, deren Mitglieder im Bereich der „incident response“ zusammenarbeiten, indem sie auf gegenseitigem Vertrauen und Ähnlichkeiten hinsichtlich des Arbeitsbereichs und der ihnen begegnenden Problemen aufbauen. Dabei verfolgt die Gruppe einen technischen Fokus und befasst sich nicht mit der Formulierung von Policies.

Deutsches Mitglied ist der CERT-Bund.[30]

28 ECS, About ECSO.

29 European Council, EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres.
European Commission, European Cybersecurity Industrial, Technology and Research Competence Centre.

30 EGC Group, European Government CERTs (EGC) group.

European Judicial Cybercrime Network (EJCN)
Das European Judicial Cybercrime Network wurde 2016 mit dem Ziel gegründet, Kontakte zwischen auf die Herausforderungen durch Cyberkriminalität, „cyber-enabled crime“ und Ermittlungen im Cyberraum spezialisierten Praktikern zu fördern und die Effizienz von Ermittlungen und Strafverfolgungen zu erhöhen. Das EJCN soll den Dialog zwischen verschiedenen Akteuren, die eine Rolle im Erhalt der Rechtsstaatlichkeit im Cyberraum spielen, stärken.

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 Eurojusts Expertise im Bereich internationaler juristischer Kooperation und der operativen und Sachgebietsexpertise der EJCN Mitgliedern zu gewährleisten.[31]

European Judicial Training Network (EJTN)
Das European Judicial Training Network wurde 2000 gegründet und ist die zentrale Plattform für Fortbildung und Wissensaustausch der europäischen Justiz.

Es arbeitete im Bereich Cybersicherheit mit CEPOL an den dort angebotenen Trainings.[32]

European Union Cybercrime Task Force (EUCTF)
2010 wurde die European Union Cybercrime Task Force 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 Mitgliedsstaaten, Vertreter 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.[33]

Generaldirektion Informatik (GD DIGIT)
Die Generaldirektion Informatik ist für die IT-Sicherheit der Systeme der Kommission zuständig. Es ist für einen IT-Betrieb, der andere Kommissionsabteilungen und EU Institutionen bei der täglichen Arbeit unterstützt und

31 Eurojust, European Judicial Cybercrime Network.

32 Emailaustausch mit CEPOL-Verterter:innen im August 2019.
EJTN, About us.

33 Europol, EUCTF.

für eine verbesserte Zusammenarbeit zwischen den Verwaltungen der Mitgliedsstaaten, verantwortlich.[34]

Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD CONNECT)
Die Generaldirektion Kommunikationsnetze, Inhalte und Technologien zeichnet sich verantwortlich für die Entwicklung des digitalen Binnenmarktes – und damit auch für die 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.[35]

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 Cyberkriminalität. Zur Generaldirektion gehört das Strategic Analysis and Response Center (STAR), das Informationen und Einschätzungen, insbesondere Risikoanalysen, zur Verfügung stellt, um die Formulierung von Policies sowie Krisenmanagement, Lagekenntnis und Kommunikation zu unterstützen. Sein Krisenreaktionszentrum befindet sich in einer resilienten und hoch gesicherten Anlage, die es erlaubt, klassifizierte Informationen zu handhaben *und mit Kommissionsdiensten, dem EAD und relevanten Agenturen (v.a. Europol und Frontex) auszutauschen.*[36]

Gruppe der Interessenträger für die Cybersicherheitszertifizierung
Mit Inkrafttreten des Cybersecurity Acts wird eine Gruppe der Interessenträger eingesetzt, deren Mitglieder aus anerkannten Sachverständigen als Vertreter:innen der einschlägigen Interessenträger von der Europäischen

34 Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Commission, Informatics.

35 European Commission, Communication Networks, Content and Technology.

36 European Commission, Policies.
Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".

Kommission auf Vorschlag der Agentur der Europäischen Union für Netz- und Informationssicherheit ausgewählt werden.

Unter anderem soll sie die EK im Zusammenhang mit dem EU-Rahmen für die Cybersicherheitszertifizierung und die ENISA (auf Ersuchen) in Fragen im Zusammenhang mit deren Aufgaben bezüglich des Markts, der Zertifizierung und Normung beraten. Außerdem wird sie die EK in Bezug auf die Notwendigkeit solcher Zertifizierungsschemata, die nicht Teil des fortlaufenden Arbeitsprogramms der Union sind unterweisen. Der Vorsitz wird von Vertreter:innen der Kommission und der ENISA gemeinsam geführt. Die Sekretariatsgeschäfte nimmt die ENISA wahr.[37]

Horizon 2020
Horizon 2020 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.[38]

Horizontal Working Party on Cyber Issues (HWP)
Die Horizontal Working Party on Cyber Issues wurde 2016 vom Rat der Europäischen Union gegründet. Die Aufgabe der Arbeitsgruppe ist die Koordinierung der Arbeit des Rats zu Cyberpolitik und der zugehörigen Gesetzgebung. Die Aufgaben und Ziele der Arbeitsgruppe umfassen unter anderem die Vereinheitlichung bestehender Ansätzen der europäischen Cybersicherheitspolitik, die Verbesserung des Informationsaustausches zu Cyber-Themen zwischen EU-Mitgliedsstaaten und sowie die Festlegung von einheitlichen Prioritäten und strategischen Zielsetzungen der Cybersicherheitspolitik in-

37 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).

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

nerhalb der EU. Sie ist dabei in gesetzgebende und nicht legislative Prozesse eingebunden.

Die Arbeitsgruppe arbeitet mit der Europäischen Kommission, EEAS, Europol, Eurojust, FRA, EDA und ENISA zusammen und steht zudem in einem engen Austausch mit anderen Arbeitsgruppen.[39]

Intelligence Directorate des EU-Militärstabs (EUMS INT)
Das Intelligence Directorate des EU-Militärstabs stellt militärische Lageanalysen und -bewertungen für den Entscheidungsprozess und die Planung von zivilen Einsätzen und militärischen Operationen im Rahmen der Common Security and Defense Policy (CSDP) zur Verfügung.

EUMS INT arbeitet eng mit dem zivilen Lagezentrum INTCEN formalisiert als Single Intelligence Analysis Capacity (SIAC) 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, dem Deutschen Militärischen Vertreter bei der Europäischen Union und dem Kommando Operative Führung Eingreifkräfte zur Verfügung.[40]

Inter-Service Group „Community Capacity in Crisis-Management" (ISG C3M)
Diese Inter-Service Gruppe ist ein Netzwerk, das seit 2008 existiert und regelmäßig alle Kommissionsdienste und EU Agenturen, die im Krisenmanagement tätig sind, zusammenbringt, um Awareness zu stärken, Synergien zu finden und Informationen auszutauschen. Die Gruppe fungiert als Netzwerk der Kontaktpunkte aller operativen Krisen- und Lagezentren.

Der EAD ist bei der ISG C3M beteiligt.[41]

39 The Council of the European Union, Establishment of a Horizontal Working Group on Cyber Issues.
Europäischer Rat, Horizontal Working Party on Cyber Issues (HWP).

40 Pia Seyfried, Red Herring & Black Swan: Five Eyes for Europe.
Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik.
Deutscher Bundestag, Drucksache 19/489: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.

41 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".

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.[42]

Kooperationsgruppe unter der NIS-Richtlinie
Die Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) richtete eine Kooperationsgruppe unter dem Vorsitz der Präsidentschaft des Rats des Europäischen Union ein, die Repräsentant:innen der Mitgliedsstaaten, der Kommission (in der Funktion des Sekretariats) und der ENISA zusammenbringt, die strategische Kooperation und Informationsaustausch zwischen den Mitgliedsländern vereinfachen und Vertrauen aufbauen soll. 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 Mitgliedsstaaten zur Umsetzung der NIS-Richtlinie zu unterstützen, *indem sie für das CSIRTs Netzwerk beratend tätig wird, Mitgliedsstaaten beim Kapazitätsaufbau unterstützt, Informationsaustausch und Best Practices bei Kernthemen wie Cyberawareness fördert.*[43]

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; sein Fokus liegt dabei auf der Erleichterung von grenzüberschreitender Kooperation, die den auf Vertrauen basierenden Austausch von Daten zwischen zwei oder mehr Computer Emergency Response Teams beinhaltet (d.h. ad-hoc Gruppen der Computer Emergency Response Teams, die gegenseitig einer vertrauensbasierten Kooperation zustimmten). 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

42 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats “EU Playbook”.

43 European Commission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.

CERTs durchgeführt werden, vom Vorfallsmanagement bis zur Gefahrenanalyse, umzusetzen.

Die ENISA ist verantwortlich für die Durchführung und Bereitstellung zentraler Aspekte der MeliCERTes Anlage.[44]

NIS Public-Private Platform (NIS Platform)
Die NIS Plattform wurde 2013 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.

Die Ergebnisse der NIS Platform wurden von der EK für ihre Empfehlungen zur Cybersicherheit 2014 berücksichtigt.[45]

Politisches und Sicherheitspolitisches Komitee (PSK)
Das Politische und Sicherheitspolitische Komitee ist für die Gemeinsame Außen- und Sicherheitspolitik der EU (GASP) und die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) zuständig. Es setzt sich zusammen aus den Botschaftern der Mitgliedsstaaten in Brüssel bzw. Vertretern der Außenministerien. Dabei haben Vertreter des Europäischen Auswärtigen Dienstes den Vorsitz inne. Regulär tritt es zweimal wöchentlich, bei Bedarf auch häufiger zusammen. Das Komitee spielt eine zentrale Rolle bei der Entscheidungsfindung bei allen cyberbezogenen diplomatischen Maßnahmen.

Die Aufgaben des PSK sind unter anderem die internationale Lage zu beobachten, dem Rat Empfehlungen zu strategischen Konzepten und politischen Optionen auszusprechen und für die politische Kontrolle und die strategische Leitung von Krisenbewältigungseinsätzen zu sorgen.[46]

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

45 ENISA, NIS Platform.

46 Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Europäischer Rat/Rat der Europäischen Union, Politisches und Sicherheitspolitisches Komitee (PSK).

Reference Incident Classification Taxonomy Task Force (TF-CSIRT)
Die Reference Incident Classification Taxonomy Task Force wurde im Nachgang des „51st TF-CSIRT meeting“ 2017 gegründet. Dort wurde der Bedarf für eine universelle Systematisierung innerhalb der Computer Security Incident Response Teams Community im Bereich Informationsaustausch, Vorfalls-Berichterstattung und Nutzung von automatisierten Mechanismen in der Reaktion auf Vorfälle festgestellt. Das Ziel der Task Force ist die Erstellung eines Referenzdokuments, die Entwicklung eines Mechanismus für Updates und Versionierung, die Verwaltung des Referenzdokuments und die Organisation persönlicher Meetings der Stakeholder.

Mitglieder der Taskforce sind Mitglieder der europäischen CSIRTs, darunter auch CERT-Bund, der Common Taxonomy Governance Group (d.h. Vertreter der ENISA und des EC3), tool-Entwickler und „taxonomy owners“.[47]

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 (basierend auf gemeinsamen Kriterien) und Zertifizierungspolicies zwischen Europäischen Zertifizierungsbehörden zu koordinieren. Sie entwickelt außerdem Schutzprofile, wenn die Europäische Kommission eine Richtlinie erlässt, die in nationale Gesetzte im Bereich IT-Sicherheit umgesetzt werden muss.

Deutsches Mitglied ist das BSI.[48]

SKI-Kontaktgruppe
Die Schutz Kritischer Infrastrukturen Kontaktgruppe ist für die strategische Koordinierung und Kooperation im Bereich des Europäischen Programmes für den Schutz kritischer Infrastrukturen (EPSKI) zuständig, welches europäische kritische Infrastrukturen und den Bedarf zu einem verbesserten Schutz derselben identifiziert. Das Programm sieht außerdem Unterstützung für die Mitgliedsstaaten beim Schutz von nationalen kritischen Infrastrukturen vor.

Die Kontaktgruppe bringt die SKI-Kontaktpunkte der Mitgliedsstaaten unter dem Vorsitz der EK zusammen. Jedes EU-Mitglied entsendet dabei einen

47 ENISA, Building a common language to face future incidents – ENISA and European CSIRTs establish a dedicated task force.
ENISA, Reference Incident Classification Taxonomy.

48 SOGIS, Introduction.

SKI-Kontaktpunkt, der alle SKI-Themen mit den anderen Mitgliedsstaaten, der EK und dem ER koordiniert.[49]

Ständige Strukturierte Zusammenarbeit (PESCO)
Die Ständige Strukturierte Zusammenarbeit wurde 2017 als Rahmen für die Zusammenarbeit von 25 Mitgliedsstaaten geschaffen und beinhaltet auch „die Zusage verstärkter Bemühungen bei der Zusammenarbeit im Bereich Cyberabwehr und damit verbundener Projekte der SSZ". Durch den Aufbau von Cyberabwehrfähigkeiten soll die Zusammenarbeit zwischen den Mitgliedstaaten und die Interoperabilität verbessert werden. 2018 wurden zwei Projektpakete (insgesamt 34 Projekte), mit entsprechenden Listen zur Projektteilnahme, beschlossen, die auch Projekte im Bereich Cybersicherheit beinhalten.[50]

Zentrum für die Koordination von Notfallmaßnahmen (ERCC)
Das Zentrum für die Koordination von Notfallmaßnahmen der Kommission, angesiedelt bei der Generaldirektion Humanitäre Hilfe und Katastrophenschutz (ECHO), unterstützt und koordiniert verschiedene Aktivitäten in den Bereichen „prevention, preparedness and response".

Seit seiner Einführung im Jahr 2013 fungiert das ERCC als zentrale Stelle des Krisenmanagements der Kommission und als zentrale Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) 24/7 Kontaktpunkt.[51]

Zentrum für Informationsgewinnung und -analyse (INTCEN)
Das Zentrum für Informationsgewinnung und -analyse ist eine zivile Analyseeinheit des Europäischen Auswärtigen Dienstes, das aufbereitetes Material aus den Mitgliedsstaaten („finished intelligence") verarbeitet und unter Berücksichtigung anderer, offen zugänglicher Informationen, Berichten aus europäischen Delegationen und Erkenntnisse des EU-Satellitenzentrums nachrichtendienstliche Bewertungen, strategische Lagebeurteilungen oder Sonderberichte und Briefings erstellt und Handlungsoptionen ableitet. Neben dem militärischen Intelligence Directorate des EU-Militärstabs gehört es zu den Krisenmanagementstrukturen des Europäischen Auswärtigen Dienstes. Zum Zentrum gehört auch der EU Situation Room, der dem Euro-

49 Commission of the European Communities, COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection.

50 Rat der Europäischen Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018).
EEAS, Ständige Strukturierte Zusammenarbeit – SSZ.

51 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".

päischen 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. In Brüssel wird derzeit diskutiert, ob und inwiefern das Zentrum die Zurechnung von Cyberangriffen unterstützen und dabei eigene Aufklärungsfähigkeiten nutzen, sowie Vorschläge für Gegenmaßnahmen machen soll.

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. Aus Deutschland tragen BND und BfV Berichte bei und entsenden Mitarbeiter an das INTCEN. INTCEN-Berichte wiederum gehen an das BKAmt, den BND, das AA, das BMVg, den MAD, das BMI und den BfV sowie themenbezogen unter Umständen weitere an Stellen.[52]

52 Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik, SWP-Aktuell 2018/A 66.
Deutscher Bundestag, Drucksache 19/489: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
Matthias Monroy, Europäisches Geheimdienstzentrum vor neuen Aufgaben.
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".
Matthias Monroy, How European secret services organize themselves in "groups" and "clubs".

5. Erläuterung – Akteure auf Bundesebene

Agentur für Innovation in der Cybersicherheit (Cyberagentur)
Die Cyberagentur (Arbeitstitel bis September 2018: „Agentur zur Förderung bedarfsorientierter Forschung an disruptiven Innovationen im Bereich Cybersicherheit und Schlüsseltechnologien", kurz ADIC), unter Federführung des Bundesministeriums des Innern, für Bau und Heimat und des Bundesministeriums der Verteidigung soll nach einer Interimsphase in Halle (Saale) dauerhaft am Flughafen Leipzig-Halle untergebracht werden. Dazu unterzeichneten Bundesinnenminister Seehofer und der Parlamentarische Staatssekretär Tauber am 03.07.2019 eine Absichtserklärung gemeinsam mit den Ministerpräsidenten Kretschmer (Sachsen) und Haseloff (Sachsen-Anhalt). Bis 2022 sollen dort bis zu 100 neue Arbeitsplätze entstehen. Ihre Aufgabe soll es sein, Innovationen zu identifizieren und konkrete Aufträge für die Entwicklung von Lösungsmöglichkeiten zu vergeben: ambitionierte Forschungsvorhaben mit hohem Innovationspotenzial im Bereich Cybersicherheit und diesbezügliche Schlüsseltechnologien für die Bedarfsdeckung des Staates bezüglich innerer und äußerer Sicherheit sollen gefördert werden. Dabei soll die Agentur keine eigene Forschung, Entwicklung und Innovation betreiben, sondern den Bedarf der Sicherheitsbehörden koordinieren und die Kooperation zwischen Bund, Wissenschaft und Wirtschaft verbessern. Sie stellt ein Element der Bundesregierung zum Schutz der Bürger:innen im Cyberraum dar. Die Cyberagentur wird nun als GmbH mit parlamentarischen Kontrollmechanismen und Auflagen gegründet. Diese umfassen beispielsweise ein Berichterstattungsverfahren gegenüber dem Haushaltsausschuss des Bundestags. Unklar ist weiterhin, wohin die Cyberagentur zieht, bevor ihr Hauptsitz am Flughafen Leipzig/Halle bezugsfertig ist. Auch die Personal- und Kompetenzverteilung zwischen dem BMI sowie dem BMVg ist noch nicht abschließend geklärt.

Die Cyberagentur bildet gemeinsam mit der SprinD ein Ökosystem, das vielversprechende Ideen und Innovationen identifizieren, fördern und entwickeln soll – insbesondere um Redundanzen zu vermeiden, gibt es eine enge Abstimmung der Arbeitsprogramme zwischen beiden Agenturen, zum Beispiel durch gegenseitige Beauftragungen bei agenturübergreifenden Themen. Der Aufsichtsrat der Agentur soll zukünftig aus Mitgliedern und Vertretern des Bundestages, des Innenministeriums, Personalräten der Beschaffungsämter

der Bundeswehr und Vertretern des BMVg, BMI, BMF und der Wissenschaft bestehen.[53]

Agentur für Sprunginnovationen (SprinD)

Die Agentur für Sprunginnovationen wurde am 16. Dezember 2019 als „SprinD GmbH" vom Bundesministerium für Bildung und Forschung (BMBF) und durch das Bundesministerium für Wirtschaft und Energie (BMWi) gegründet und dient als staatliches Instrument für die Entwicklung von Innovationen. Der Gründungsprozess war von einer Gründungskomission begleitet worden. Der Standort der „SprinD GmbH" ist Leipzig. Der Aufsichtsrat der Agentur besteht aus zehn Mitgliedern aus Wissenschaft, Ministerien und Politik, die Agentur wird ferner von zwei Geschäftsführer:innen geleitet. 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 Wertschöpfungsketten enthalten".[54] Für ihre Arbeit stehen der Agentur für die ersten zehn Jahre eine Milliarde Euro zur Verfügung.

Die SprinD koordiniert ihre Aufgaben mit der Cyberagentur.[55]

53 Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.
Bundesministerium der Verteidigung, Absichtserklärung zum Standort der Cyberagentur.
Bundesministerium des Innern, für Bau und Heimat, Cyberagentur des Bundes nach Halle/Saale und Leipzig.
Die Bundesregierung, Agentur für Innovation in der Cybersicherheit.
Andre Meister und Anna Biselli, Bundesrechnungshof bezweifelt Sinn der neuen Cyberagentur.
Heise Online, Cyberagentur des Bundes: Geplanter Start verschoben.
Tagesspiegel, Strikte Auflagen für Cyberagentur.

54 Bundesministerium für Bildung und Forschung, Bundesregierung setzt Gründungskommission für die Agentur für Sprunginnovationen ein.

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

Allianz für Cyber-Sicherheit (AfCS/ACS)
Die Allianz für Cyber-Sicherheit (AfCS/ 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 AfCS ist eine Public-Private-Partnership von BSI und BITKOM mit Wirtschaft, Behörden, Forschung und Wissenschaft.[56]

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. Dafür wurde 2011 der „Koordinierungsstab für Cyber-Außenpolitik“ (KS-CA) im Auswärtigen Amt geschaffen.

Das AA ist im Cyber-SR vertreten. Es strebt die Gründung des Deutschen Instituts für Internet Sicherheit (DIIS) an und stellt im Wechsel mit dem BMVg die Leitung der BAKS.[57]

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 teilweise vom BAAINBw eigenständig entwickelt, getestet und betrieben und in anderen Fällen in Auftrag gegeben. Es trägt somit Mitverantwortung dafür, die Bundeswehr bestmöglich vor Cyberangriffen zu schützen.

Das BAAINBw gehört zum Geschäftsbereich des BMVg. Es versorgt die Bw mit Ausrüstung und ist im Steuerungsboard des CIH vertreten.[58]

56 Bundesamt für Sicherheit in der Informationstechnik, Allianz für Cyber-Sicherheit – Über uns.

57 Auswärtiges Amt, Cyber-Außenpolitik.

58 Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, Das BAAINBw.

Bundesakademie für Sicherheitspolitik (BAKS)
Die Bundesakademie für Sicherheitspolitik ist die zentrale 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 und Vizepräsident kommen abwechselnd aus BMVg und AA.[59]

Bundesamt für den Militärischen Abschirmdienst (BAMAD)
Das Bundesamt für den Militärischen Abschirmdienst ist eine Bundesoberbehörde und der militärische Nachrichtendienst des Bundes. Im Rahmen von 2017 durchgeführten Umstrukturierungsmaßnahmen wurde der Militärische Abschirmdienst als BAMAD direkt dem Bundesministerium der Verteidigung unterstellt. Zu den Aufgaben des dritten und kleinsten Nachrichtendienstes, neben dem Bundesnachrichtendienst und dem Bundesamt für Verfassungsschutz, zählen Extremismus- sowie Terrorismusabwehr sowie die Bekämpfung von (Cyber-) Spionage und Sabotage in der Bundeswehr.

Das BAMAD gehört zum Geschäftsbereich des BMVg und ist im Cyber-AZ vertreten.[60]

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.

Die BaFin gehört zum Geschäftsbereich des BMF und ist im Cyber-AZ vertreten.[61]

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe übernimmt eine wichtige Funktion im Gesamtkonzept der nationalen Sicherheitsarchitektur. In diesem Rahmen beschäftigt es sich zunehmend auch mit den Risiken von Cyberangriffen auf kritische Infrastrukturen. Das BBK ist im Cy-

59 Bundesakademie für Sicherheitspolitik, Cyber-Realität zwischen Freiheit und Sicherheit.

60 Bundesamt für den Militärischen Abschirmdienst, Über uns.

61 Bundesanstalt für Finanzdienstleistungsaufsicht, Aufgaben & Geschichte der BaFin.

ber-AZ vertreten und sein Personal besetzt das Gemeinsame Melde- und Lagezentrum.

Die BBK gehört zum Geschäftsbereich des BMI und ist im GMLZ, UP KRITIS und Cyber-AZ vertreten.[62]

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Das Bundesamt für Sicherheit in der Informationstechnik hat die Aufgabe die Sicherheit in der Informationstechnik des Bundes zu stärken. Als Behörde mit höchster technischer Expertise fördert es darüber hinaus die Informations- und Cybersicherheit in Verwaltung, Wirtschaft und Gesellschaft durch zahlreiche Aktivitäten, Kooperationen und Initiativen. Um sich regional noch stärker zu vernetzen, baut das BSI deutschlandweit Verbindungsbüros auf. In einer gemeinsamen Absichtserklärung einigten sich Bundesinnenminister Seehofer und Staatsminister des Innern, Roland Wöller (Sachsen), im Juli 2019 auf die Entstehung eines zweiten Standorts des BSI in Freital bei Dresden. Ein dritter Standort des BSI mit den Schwerpunktthemen KI soll im Saarland entstehen. Das Vorhaben wurde im November 2019 im Anschluss vom Haushaltsausschuss des Bundestages bewilligt. Insgesamt soll dieser dritte Standort rund 30 Mitarbeiter umfassen.

Das BSI hat zur Kooperation mit den Ländern bereits Ansprechpartner 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: BaWü und Bayern), mit der Gründung des Zweitstandorts in Freital soll die Arbeit des Verbindungswesens in der Region Ost (Thüringen und Sachsen) beginnen. Der nächste Standort wird in Saarbrücken aufgebaut.

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

Das BSI gehört zum Geschäftsbereich des BMI. In ihm beherbergt sind unter anderem das Cyber-AZ, AfCS, LZ, CERT-Bund und das Bürger-CERT.[63]

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, politische Desinformation oder Computersabotage zu betreiben. Das BfV versucht Cyberangriffe auf staatliche und private Einrichtungen abzuwehren und aufzuklären.

Das BfV gehört zum Geschäftsbereich des BMI. Es ist im Cyber-AZ und der Initiative Wirtschaftsschutz vertreten und greift auf die Expertise von ZITiS zurück.[64]

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit berät und kontrolliert die Daten- und Informationsverarbeitung der öffentlichen Stellen des Bundes, sowie nicht-öffentlicher Stellen. Sie ist in der Ausübung ihres Amtes unabhängig und unterliegt nur der parlamentarischen Kontrolle durch den Bundestag.

Die BfDI ist im Beirat der DsiN vertreten.[65]

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.

63 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, Zweitstandort der Bundesbehörde BSI entsteht in Freital.
Hintergrundgespräche, 2019.
SecuPedia, Saarland: Zweite BSI-Außenstelle entsteht in Saarbrücken.
Tagesspiegel, BSI bekommt KI-Ableger in Saarbrücken.

64 Bundesamt für Verfassungsschutz, Cyberangriffe.

65 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.

Das BKAmt ist im Cyber-SR vertreten und ihm ist der BND nachgeordnet. Aus seinem Haushalt wird die institutionelle Zuwendung an die SWP gezahlt.[66]

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.

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.[67]

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 Onlinemobbing.

Das BMJV ist im Cyber-SR vertreten.[68]

Bundesministerium der Verteidigung (BMVg)
Das Bundesministerium der Verteidigung ist für die militärische Verteidigung Deutschlands und somit auch für die Verteidigung Deutschlands im Cyberraum verantwortlich. Dafür setzt das BMVg auf nationale und internationale Kooperationen und Partnerschaften, zum Beispiel mit dem Cyber Innovation Hub oder dem Cooperative Cyber Defense Centre of Excellence der NATO. Im Ministerium ist die Abteilung Cyber- und Informationstechnik für den Bereich Cyberverteidigung federführend zuständig.

66 Bundeskanzleramt, Chef des Bundeskanzleramtes.

67 Bundeskriminalamt, Straftaten im Internet.

68 Bundesministerium der Justiz und für Verbraucherschutz, Aufgaben und Organisation.
Bundesministerium der Justiz und für Verbraucherschutz, Schutz von Bürgern und Onlinehandel vor Cyberkriminalität.
Bundesministerium der Justiz und für Verbraucherschutz, Wir dürfen Cybermobbing nicht ignorieren.

Das BMVg ist im Cyber-SR vertreten. Ihm ist die Bw nachgeordnet und die BAKS gehört zu seinem Geschäftsbereich. ADIC soll unter Federführung des BMVg eingerichtet werden.[69]

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. Die vom BMI vorgelegte „Cyber-Sicherheitsstrategie für Deutschland 2016" wurde im November 2016 vom Kabinett verabschiedet und bildet den ressortübergreifenden, strategischen Rahmen der Bundesregierung. Das BMI koordiniert die Umsetzung der Cybersicherheitsstrategie durch den Bundesbeauftragten für Informationstechnik, der auch Vorsitzender des Cyber-Sicherheitsrates ist.

Das BMI ist im Cyber-SR vertreten. Seinem Geschäftsbereich sind BPol, BKA, BSI, BfV und BBK zugeordnet. Auf ein Erlass des BMI hin, wurde 2017 ZITiS gegründet. Das BMI ist in den Initiativen UP KRITIS, DsiN (Beirat), sowie der AfCS vertreten. ADIC soll unter Federführung des BMVg eingerichtet werden.[70]

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.

Das BMBF ist im Cyber-SR vertreten und fördert die Kompetenzzentren für IT-Sicherheit.[71]

Bundesministerium für Finanzen (BMF)
Das Bundesfinanzministerium ist vorrangig für die Steuer-, Haushalts- und Europäische Finanzpolitik zuständig. Es entwickelt zum Beispiel gemein-

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

70 Bundesministerium des Innern, für Bau und Heimat, IT & Cybersicherheit.
Bundesministerium des Innern, für Bau und Heimat, Cyber-Sicherheitsstrategie für Deutschland.
Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land 2018.

71 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.
Fraunhofer SIT, Institutsgeschichte.

sam 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.[72]

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.

Das BMG hat die gematik mit dem Aufbau einer Telematikinfrastruktur beauftragt, die Voraussetzung für eine sichere Vernetzung des Gesundheitswesens ist.[73]

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.[74]

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.

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

73 Bundesministerium für Gesundheit, E-Health-Gesetz.
Bundesministerium für Gesundheit, Aufgaben und Organisation.

74 Bundesministerium für Verkehr und digitale Infrastruktur, Krisenmanagement.

Das BMWi ist im Cyber-SR vertreten. Es hat die Initiative IT-Sicherheit in der Wirtschaft und Trusted Cloud ins Leben gerufen. Es ist im Beirat von DsiN vertreten; die BNetzA gehört zum Geschäftsbereich.[75]

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.[76]

Bundesnachrichtendienst (BND)
Der Bundesnachrichtendienst ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland und handelt im Auftrag der Bundesregierung. Im Ausland erfasst 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. Er ist an der Initiative Wirtschaftsschutz beteiligt und im Cyber-AZ vertreten. Sein Personal wird unter anderem an der UniBw ausgebildet.[77]

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 Eisenbahnen zuständig. Da die Bedeutung von Cybersicherheit in diesen Berei-

75 Bundesministerium für Wirtschaft und Energie, IT-Sicherheit.
Bundesministerium für Wirtschaft und Energie, IT-Sicherheit für die Industrie 4.0.

76 Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Glossar – Digitalisierung und nachhaltige Entwicklung.

77 Bundesnachrichtendienst, Die Arbeit.
Bundesnachrichtendienst, Cybersicherheit.

chen zunehmend an Bedeutung gewinnt, kümmert sich die BNetzA auch um 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.[78]

Bundespolizei (BPol)
Die Bundespolizei übernimmt Aufgaben im Bereich des Grenzschutzes, der Luftsicherheit, Bahnpolizei und Kriminalitätsbekämpfung. Da illegale Aktivitäten immer stärker auch im Internet oder mithilfe von Informationstechnik ausgeübt werden, bekämpft die BPol zunehmend auch Internet-Kriminalität. Sie betreibt ihr eigenes Computer Emergency Response Team (CERT BPol) zum Schutz ihrer Einrichtungen und der Informations- und Kommunikationstechnik.

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.[79]

Bundeswehr (Bw)
Die Bundeswehr ist u. a. für die Landes- und Bündnisverteidigung verantwortlich. Um dieser Aufgabe im digitalen Zeitalter gerecht zu werden, wurde im April 2017 der neue militärische Organisationsbereich Cyber- und Informationsraum aufgestellt. Neben Heer, Luftwaffe und Marine ist die neue Organisation ganzheitlich für die Verteidigung des Cyber- und Informationsraums verantwortlich.

Die Bw gehört zum Geschäftsbereich des BMVg. Sie bildet Teile ihres Personals an der UniBw aus und ist im Cyber-AZ sowie im CERT-Verbund vertreten.[80]

78 Bundesnetzagentur, Aufgaben und Struktur.
Bundesnetzagentur, IT-Sicherheit im Energiesektor.

79 Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Irene Mihalic, Dr. Konstantin von Notz, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 18/13386 –.
Bundespolizei, Startseite.
Bundespolizei kompakt, 04/2015.
Hintergrundgespräche, 2019

80 Bundeswehr, Auftrag und Aufgaben der Bundeswehr.
Bundeswehr, Das Kommando Cyber- und Informationsraum.

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. Im Rahmen des Herkules-Großprojektes wurde die Bundeswehr-IT durch die BWI umfassend modernisiert. An der Gesellschaft und dem Großprojekt waren auch IBM und Siemens beteiligt. Ende des Jahres 2016 endeten jedoch sowohl das Projekt Herkules als auch die Beteiligung der beiden Firmen und die BWI wurde zu einer reinen Bundesgesellschaft. Schwerpunkte der Arbeit sind das Betreiben und Modernisieren von nichtmilitärischen Informations- und Kommunikationstechniken 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. Im Jahr 2019 schlossen das BWI und die Bundeswehr zudem eine Kooperationsvereinbarung mit dem Ziel einer engeren Zusammenarbeit. Diese soll zukünftig ehemaligen Soldat:innen eine Eingliederung und die Arbeit im BWI ermöglichen. Dazu soll die Arbeit des BWI sowie damit einhergehende Berufsperspektiven innerhalb der Bundeswehr beworben sowie Stellenausschreibungen des BWI innerhalb der Bundeswehr veröffentlicht werden.

Die BWI GmbH ist eine Bundesgesellschaft und IT-Systemhaus für Bw und Bund.[81]

CERT-Bund/Bürger-CERT
Das Computer Emergency Response Team des Bundes ist Notfallteam und Anlaufstelle für alle Bundesbehörden im Falle eines sicherheitsrelevanten IT-Vorfalls. Das Bürger-CERT ist ein Warn- und Informationsdienst für Privatpersonen, die vom Bürger-CERT neutral und kostenlos über aktuelle Sicherheitslücken informiert werden.

Das CERT des Bundes ist im BSI aufgehangen und kooperiert im Rahmen des Verwaltungs-CERT-Verbunds (VCV) mit den Länder-CERTs.[82]

CERT-Verbund
Der CERT-Verbund ist eine Allianz deutscher Sicherheits- und Computer-Notfallteams, die sich in Unternehmens-, Kommerziellen-, Akademischen- und

81 Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.
Bundesministerium der Verteidigung, Auf engere Kooperation geeinigt: Bundeswehr und BWI GmbH.

82 Bundesamt für Sicherheit in der Informationstechnik, CERT-Bund.

Verwaltungs-CERTs auf Bundes- und Länderebene zusammengeschlossen haben.

Im CERT-Verbund sind unter anderem die Bw und das BSI (mit dem CERT-Bund) vertreten.[83]

Cyberbündnis mit der Wirtschaft
Im September 2018 unterzeichneten Bundesinnenminister Seehofer und der Präsident des Bundesverbandes der deutschen Industrie e. V. Dieter Kempf ein Memorandum of Understanding zum Aufbau des Bündnisses für Cybersicherheit. Darin verständigen sich das Bundesministerium des Innern, für Bau und Heimat und der Bundesverband der deutschen Industrie auf eine intensivierte Zusammenarbeit bei Cybersicherheitsthemen. Die Notwendigkeit einer solchen engen Kooperation wird mit „der stetig steigenden Bedrohungslage aus dem Cyberraum" begründet. Gemeinsam mit Verbänden, Unternehmen und Bundesbehörden wollen die Partner die Zusammenarbeit zwischen Staat und Wirtschaft stärken – Ziel ist eine bessere Vernetzung beider Sektoren für eine effizientere Gewährleistung von Cybersicherheit – insbesondere auch im internationalen Kontext. Hier soll ein Forum zwischen Bundesbehörden und Wirtschaftsvertreter:innen entstehen, in dem ein Austausch zu internationalen Cybersicherheitsfragen stattfinden kann. 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.[84]

Cyber Innovation Hub (CIH)
Um die Konkurrenzfähigkeit der Bundeswehr im Bereich Cyber und IT zu garantieren, bietet der Cyber Innovation Hub der Bundeswehr eigenen Mitarbeiter:innen in Zusammenarbeit mit Startups eine Plattform zum Erforschen und Weiterentwickeln von innovativen Technologien. Durch die Verknüpfung von Bundeswehr und Startups sollen Ideen schneller verwirklicht und fortschrittliche Technologien besser umgesetzt werden können. Die Soldat:innen arbeiten gemeinsam mit Zivilpersonen vor allem auch an der Entwicklung von disruptiven Technologien für die Bundeswehr.

83 Deutscher CERT-Verbund, Startseite.

84 Bundesministerium des Innern, für Bau und Heimat, Industrie und BMI etablieren Bündnis für Cybersicherheit.

Der CIH ist dem BMVg zugeordnet. Im Januar 2020 wurde der Hub als eigene Abteilung in die BWI und somit in eine Verwaltung mit Weisungsbindung eingegliedert.[85]

Cyber Security Cluster Bonn e. V.
Der Cyber Security Cluster Bonn e. V. ist ein Zusammenschluss von verschiedenen Institutionen, die im Umfeld der Cyber Sicherheit aktiv sind. Geografischen Schwerpunkt hat der Cluster in der Bonner Region, unter anderem durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr und die Polizei Bonn, die alle als Beiräte im Cluster vertreten sind. Die Deutsche Telekom, die Hochschule Bonn-Rhein-Sieg, die Fraunhofer-Gesellschaft sowie große Technologie-Unternehmen wie IBM und Symantec sind neben der IHK Bonn/Rhein-Sieg, der Stadtverwaltung und Vertreter der Bonner Wirtschaft als Mitglieder im Cluster vertreten. Ziel ist es, die thematische und meist geographische Nähe zu nutzen, um die Zusammenarbeit zu intensivieren, Fachkräfte anzuziehen und auch gemeinsam an konkreten Projekten im Bereich der Cybersicherheit zu arbeiten.

Das BSI und das KdoCIR der Bw sind Mitglieder im Beirat des Cyber Security Clusters Bonn e. V. [86]

Cyber-Sicherheitsrat (Cyber-SR)
Der nationale Cyber-Sicherheitsrat wurde 2011 im Zuge der Cybersicherheitsstrategie mit dem Ziel eingerichtet, als strategischer Ratgeber der Bundesregierung langfristige Handlungsnotwendigkeiten und Trends der Cybersicherheit zu identifizieren und entsprechende Impulse anzuregen. Er bringt Vertreter der Bundesebene, der Länder und aus der Wirtschaft zusammen. Im Rahmen der Cybersicherheitsstrategie 2016 gab es eine Überarbeitung der internen Strukturen des Cyber-Sicherheitsrates.

Im Cyber-SR sind BMI, BKAmt, AA, BMVg, BMWi, BMJV, BMF, BMBF und BMVI vertreten.[87]

85 Bundesministerium der Verteidigung, Cyber Innovation Hub.
Die Bundesregierung, Regierungspressekonferenz vom 2. Dezember 2019.
Tagesspiegel, BMVg: Führung springt beim Cyber Innovation Hub ab.
Tagesspiegel, Wehrbeauftragter kritisiert Umwandlung des Cyber Innovation Hub

86 Cyber Security Cluster Bonn, Über uns.
Emailaustausch mit Vertreter:innen des Cyber Security Cluster Bonn e. V. im November 2019.

87 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Die Deutsche Gesellschaft für Internationale Zusammenarbeit hilft der 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.[88]

Deutsches Institut für Internet Sicherheit/Cyber-Sicherheit (DIIS)
In der Cybersicherheitsstrategie für Deutschland 2016 wurde die Gründung eines *Deutschen Instituts für Cybersicherheit* angekündigt. Das Institut soll unterschiedliche Akteure einbeziehen, um an Cybersicherheitsthemen mit Bezug zu internationaler Stabilität und Krisenprävention zu arbeiten. Dabei soll es Regierungen als internationaler Ansprechpartner zur Verfügung stehen.

Das DIIS soll vom AA gegründet werden.[89]

Deutschland sicher im Netz e. V. (DsiN)
Deutschland sicher im Netz e. V. wurde im Rahmen des 1. Nationalen IT-Gipfels gegründet, um die 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.

Das BMI, BMWi, BSI, BKA und BfDI sind im DsiN Beirat vertreten. DsiN kooperiert mit der Initiative IT-Sicherheit in der Wirtschaft.[90]

Forschungsinstitut Cyber Defence (CODE)
Das Forschungsinstitut Cyber Defence (CODE) an der Universität der Bundeswehr wurde vom BMVg mit dem Ziel gegründet, innovative technische Neuerungen für Bundeswehr und Bund zum Schutz von Daten, Software und Systemen zu verwirklichen. Darüber hinaus ist das interdisziplinäre, unabhängige Forschungsinstitut an die wissenschaftliche Aus-, Fort- und Weiter-

88 Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Bundesregierung. Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH.
Hintergrundgespräche, 2018.

89 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.

90 Deutschland sicher im Netz, Presse.

bildung der Universität der Bundeswehr angebunden. Hier baut es ein intersektorales Cybercluster auf.

CODE ist das Forschungsinstitut Cyber Defence an der UniBw, wo Bw Personal wissenschaftlich ausgebildet wird. Es befindet sich in geografischer Nähe zur ZITiS.[91]

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 im Januar 2020, 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. [92]

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.

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 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, des Bundesamts für Sicherheit in der Informationstechnik und des Bundesministeriums für Wirtschaft und Energie.[93]

91 Universität der Bundeswehr München, Forschungsinstitut CODE.

92 Lina Rusch, Digitaler Staat: Agenturen in den Startlöchern.
IT-Planungsrat, FITK.
Tagesspiegel, Rechtlicher Rahmen für FITKO-Start steht.

93 Bundesministerium für Gesundheit, E-Health-Gesetz.
Gematik, Die elektronische Gesundheitskarte.
Gematik, Telematikinfrastruktur.
Gematik, Themen.
Gematik, Über uns.

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 GMLZ übernimmt nachts die Aufgaben des LZ. Das BBK ist im GMLZ vertreten.[94]

German Competence Centre against Cyber Crime (G4C)
Das German Competence Centre against Cyber Crime (G4C) ist ein Verein, der unterschiedliche Akteure in einer strategischen Allianz gegen Cyberkriminalität zusammenbringt. Durch einen täglichen Informationsaustausch zwischen den behördlichen Kooperationspartnern und den Mitgliedern, können diese geeignete Schutzmaßnahmen entwickeln.

Das G4C kooperiert mit dem BKA und dem BSI.[95]

Informationstechnikzentrum Bund (ITZBund)
Das ITZBund ist IT-Dienstleister der Bundesverwaltung. Es ist 2016, als Teil einer Gesamtstrategie mit dem Ziel einer konzentrierten Bündelung der IT-Kapazitäten des Bundes, aus drei Vorgängerbehörden gegründet worden: 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 und soll unter anderem auch den Schutz vor Cyberangriffen verbessern.

Das ITZBund gehört zum Geschäftsbereich des Bundesministeriums der Finanzen.[96]

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. Eine Vielzahl von Aktivitäten werden von der Initiative gebündelt. Die

94 Bundesministerium des Innern, für Bau und Heimat, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.

95 German Competence Centre against Cyber Crime e. V. (G4C), Über uns.

96 Informationstechnikzentrum Bund, Über uns.

Mitglieder des Steuerkreises sind IT-Experten aus Verwaltung, Wissenschaft und Wirtschaft und beraten die Initiative IT-Sicherheit in der Wirtschaft bei der Umsetzung ihrer Projekte.

Die Initiative IT-Sicherheit in der Wirtschaft ist eine Initiative des BMWi. In ihrem Rahmen wird u. a. das „Bottom-Up" Projekt von DsiN betrieben.[97]

Initiative Wirtschaftsschutz
Die Initiative Wirtschaftsschutz hat das Ziel den Schutz wichtiger Unternehmenswerte der deutschen Wirtschaft zu verbessern. Das BMI koordiniert die Zusammenarbeit von staatlichen Stellen und Wirtschaftsverbänden. Die Initiative bietet ein umfangreiches Schutzkonzept aus Maßnahmen, Handlungsempfehlungen und Seminaren.

Die Initiative Wirtschaftsschutz arbeitet auf staatlicher Seite mit dem BND, BfV, BKA und dem BSI zusammen.[98]

Innenministerkonferenz (IMK)
Die Innenministerkonferenz ermöglicht eine regelmäßige länderübergreifende Zusammenarbeit zwischen den Innenministern und -senatoren der Länder. Die Innenministerkonferenz hat zwei Gremien etabliert, die sogenannte „Länderoffene Arbeitsgruppe Cybersicherheit" (LOAG Cybersicherheit) und die für die Polizei etablierte KomSi (AG Kommunikationssicherheit im AK II, UA IuK). Diese Arbeitsgruppen sind für die Verwaltung von beispielsweise Katastrophenschutz oder Cyberkriminalität zuständig.[99]

IT-Planungsrat
Der IT-Planungsrat ist das zentrale Gremium für die föderale 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, steuern E-Government-Projekte und planen und entwickeln das Verbindungsnetz nach dem IT-NetzG. Er setzt sich zusammen aus dem Beauftragten der Bundesregierung für Informationstechnik und aus den Ländern jeweils ein:e für Informationstechnik zuständige Vertreter:innen. Beratend an Sitzungen

97 Bundesministerium für Wirtschaft und Energie, Steuerkreis.
Bundesministerium für Wirtschaft und Energie, Erste Berufsschulen in Niedersachsen setzen auf Bottom-Up für mehr IT-Sicherheit im Mittelstand.

98 Initiative Wirtschaftsschutz, Aktuelles. (Website entfernt)

99 Secupedia, Nationales Cyber-Abwehrzentrum.
Emailaustausch mit Vertreter:innen des BSI im Februar 2020.
Bundesrat, Innenministerkonferenz.

können drei Vertreter:innen der Gemeinden und Gemeindeverbänden, die von den kommunalen Spitzenverbänden auf Bundesebene entsandt werden sowie die 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.

Der Chef 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.[100]

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 den Chef des Bundeskanzleramts wahrgenommen. Stellvertretende Vorsitzende sind die Bundesbeauftragte für Digitalisierung und der Beauftragte der Bundesregierung für Informationstechnik (BfIT).[101]

IT Security made in Germany
Das Vertrauenszeichen „IT Security made in Germany“ wurde 2005 gemeinsam durch das Bundesministerium des Innern, für Bau und Heimat, das Bundesministerium für Wirtschaft und Energie sowie Vertreter der deutschen IT-Sicherheitswirtschaft ins Leben gerufen. Seit 2011 wird der Verein 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.[102]

100 IT-Planungsrat, IT-Planungsrat.
IT-Planungsrat, Aufgaben des IT-Planungsrats.
IT-Planungsrat, Zusammensetzung des IT-Planungsrates.
IT-Planungsrat, Besprechung des Chefs des Bundeskanzleramtes mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder.

101 Der Beauftragte der Bundesregierung für Informationstechnik, IT-Rat.

102 TeleTrust, IT Security made in Germany.

Kommando Cyber- und Informationsraum (KdoCIR)
Das im April 2017 etablierte Kommando Cyber- und Informationsraum führt den Organisationsbereich Cyber- und Informationsraum (CIR) an und soll zur Verbesserung der staatlichen Cybersicherheit ein Lagebild des Cyberraums schaffen. Der Organisationsbereich Cyber- und Informationsraum ist der sechster militärische Organisationsbereichs der Bundeswehr. Er soll bis 2021 voll ausgebaut sein und bis dahin über 14.500 Beschäftigte aufweisen. Als Kommando des CIR leitet KdoCIR die Bereiche und entsprechenden Kommandos „Cyber, ITInformationstechnik, Strategische Aufklärung, Geoinformationswesen der Bundeswehr und Operative Kommunikation“.[103] Vorrangig soll das Kommando jedoch den CIR strukturieren und die Personalführung gewährleisten. Zudem ist es „Dienstsitz des Inspekteurs CIRCyber- und Informationsraum und seines Vertreters, der in seiner Funktion als Chief Information Security Officer die Gesamtverantwortung für die Informationssicherheit der Bundeswehr innehat“.[104] KdoCIR beschäftigt insgesamt ca. 13.500 Soldat:innen und zivile Mitarbeiter:innen. Der Standort des KdoCIR ist in Bonn.

Das KdoCIR ist Teil des Organisationsbereichs CIR der Bw.[105]

Kommando Informationstechnik (KdolTBw)
Das Kommando Informationstechnik ist ein Fähigkeitskommando im Organisationsbereich der Streitkräftebasis und ist mit der Bereitstellung von IT-Services der Bundeswehr befasst. Der Hauptsitz des KdolTBw befindet sich seit der Gründung des Kommandos im Januar 2013 in Bonn. Das Kommando Informationssicherheit stellt sicher, dass bei den Einsätzen die Einrichtung, der Betrieb und der IT-technische Schutz der Elemente gewährleistet sind. Dem Kommando unterstehen sechs „ITInformationstechnik-Battalione“ und diverse Dienststellen wie beispielsweise das Betriebszentrum „ITInformationstechnik-System“ der Bundeswehr.

KdolTBw ist dem KdoCIR der Bw unterstellt und gehört seit Juli 2017 zum Organisationsbereich CIR.[106]

103 Bundesministerium der Verteidigung, FAQ: Cyber-Abwehr.

104 Bundeswehr, Kommando Cyber- und Informationsraum.

105 Bundeswehr, Auftrag des Organisationsbereichs CIR.
Bundesministerium der Verteidigung, FAQ: Cyber-Abwehr.
Bundeswehr, Kommando Cyber- und Informationsraum.

106 Bundeswehr, Kommando Informationstechnik der Bundeswehr.
Bund, Kommando Informationstechnik der Bundeswehr (KdolTBw).

Kommando Strategische Aufklärung (KdoStratAufkl)
Das Kommando Strategische Aufklärung dient der Informationsbedarfsdeckung der Bundeswehr zum Schutz des Personals in Einsatzgebieten sowie zur Krisenfrüherkennung. Zudem betreibt das KdoStratAufkl auch Aufklärung in definierten Bereichen. Die Aufgabenbereiche des Kommandos werden dabe in die Felder „Satellitengestützte Abbildende Aufklärung", „Fernmelde- und Elektronische Aufklärung", den „Elektronischen Kampf" und den Bereich der „Objektanalyse" unterteilt.[107] Ferner arbeitet das Kommando an der Fähigkeit zu Computer-Netzwerk-Operationen. Das Kommando operiert aus der Grafschaft-Gelsdorf in Rheinland-Pfalz.

Seit Juli 2017 ist KdoStratAufkl dem KdoCIR unterstellt.[108]

Kompetenznetzwerk Trusted Cloud (Trusted Cloud)
Das Kompetenznetzwerk Trusted Cloud ist aus dem gleichnamigen Programm des Bundesministeriums für Wirtschaft und Energie entstanden, welches ein Gütesiegel für Cloud Services entwickelt und etabliert hat. Trusted Cloud dient als neutrale und branchenübergreifende Plattform für den Austausch zwischen Cloud-Anbietern und Anwendern.

Trusted Cloud wurde durch das BMWi ins Leben gerufen.[109]

Nationaler Pakt Cybersicherheit
Der Nationale Pakt Cybersicherheit ist eine Initiative des BMI. Sie wurde am 28. Oktober 2019 offiziell auf dem Digitalgipfel der Bundesregierung bekannt gegeben. 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. Der Pakt hat drei Teilbereiche: 1. die Erfassung wesentlicher Akteure der Cybersicherheit in Deutschland in einem Online Kompendium, 2. öffentlichkeitswirksame Auftritte der aus BMI, Deutscher Telekom, Bundesverband Verbraucherzentralen (vzbv) und TU Darmstadt bestehenden „Quadriga" und 3. eine Evaluierung des Vorgehens mit Handlungsempfehlungen für die nächste Legislaturperiode.

Teil des Paktes sind unter anderem das Cyberbündnis mit der Wirtschaft, die Agentur für Innovation in der Cybersicherheit, das IT-Sicherheitskennzeichen

107 Bundeswehr, Kommando Strategische Aufklärung Auftrag.

108 Bundeswehr, Kommando Strategische Aufklärung.
Bund, Kommando Strategische Aufklärung (KdoStratAufkl).

109 Bundesministerium für Wirtschaft und Energie, Das Kompetenznetzwerk Trusted Cloud.

und die Aufnahme des Verbraucherschutzes als neue Aufgabe des BSI – weitere Beiträge von anderen Stakeholdern werden im Laufe der Umsetzung identifiziert. In der „Quadriga" des Nationalen Pakts für Cybersicherheit ist zudem der Vorstand des vzbv als zivilgesellschaftlicher Repräsentant vertreten.[110]

Nationales Cyber-Abwehrzentrum (NCAZ/ 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. Aktuell befindet sich das Cyber-AZ im Umbau, der seit vielen Jahren unter dem Projektnamen „Cyber-Abwehrzentrum Plus" im Gespräch ist.

Das Cyber-AZ ist eine Kooperationsplattform zwischen BSI, BPol, BKA, BfV, BBK, BND, Bw, ZKA, BaFin und BAMAD. Es schickt seinen Jahresbericht an den Cyber-SR.[111]

Nationales IT-Lagezentrum (LZ)
Das Nationale IT-Lagezentrum im Bundesamt für Sicherheit in der Informationstechnik hat die Aufgabe 24 Stunden täglich ein IT-Lagebild zu erstellen, um auftretende IT-Sicherheitsvorfälle für staatliche Stellen und Wirtschaftsunternehmen schnell einschätzen zu können und wenn nötig darauf zu reagieren. Nachts übernimmt das Gemeinsame Melde- und Lagezentrum von Bund und Ländern die Funktion. Cyberangriffe sollen rechtzeitig entdeckt und vorbeugende Maßnahmen früh ergriffen werden. Dies wird über konstantes Monitoring und Auswerten von verschiedenen Quellen erreicht, die in der Gesamtschau eine möglichst umfassende Übersicht zu der IT-Sicherheitlage in der Bundesrepublik liefern. Die Kapazitäten und Strukturen des LZ erlauben es ihm zudem, gegebenenfalls zum IT-Krisenreaktionszentrum aufzuwachsen.

Das LZ arbeitet eng mit dem GMLZ, CERT-Bund und Cyber-AZ zusammen.[112]

110 Bundesministerium des Innern, für Bau und Heimat, Nationaler Pakt Cybersicherheit.

111 Hintergrundgespräche, 2019.
Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.

112 Bundesamt für Sicherheit in der Informationstechnik, Nationales IT-Lagezentrum.

Stiftung Wissenschaft und Politik (SWP)
Die Stiftung Wissenschaft und Politik berät Bundestag und 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.[113]

Transferstelle „IT-Sicherheit in der Wirtschaft“
Die Transferstelle „IT-Sicherheit in der Wirtschaft“ wurde vom Bundeswirtschaftsministerium (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. Dafür stehen Expert:innen aus Wirtschaft, Wissenschaft und Verwaltung bereit. Die Transferstelle wird mit rund 5 Millionen Euro im Jahr bezuschusst.

Die Transferstelle ist Teil der BMWi-Initiative „IT-Sicherheit in der Wirtschaft“. Zudem wird sie durch ein Konsortium betrieben, bestehend aus DsiN, dem DIHK, Fraunhofer FOKUS, der Hochschule Mannheim und IAO.[114]

Umsetzungsplan Kritische Infrastrukturen (UP KRITIS)
Der Umsetzungsplan Kritische Infrastrukturen 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. Da Informations- und Kommunikationstechnik einen immer größerer Bestandteil von Kritischen Infrastrukturen darstellt, kommt ihrem Schutz eine zentrale Rolle zu.

Im Rahmen des UP KRITIS kooperieren von staatlicher Seite BMI, BSI und BBK.[115]

113 Stiftung Wissenschaft und Politik, Cyber-Sicherheit.
Stiftung Wissenschaft und Politik, Über uns.

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

115 Internetplattform zum Schutz Kritischer Infrastrukturen, Zusammenarbeit im Rahmen des UP KRITIS.
Internetplattform zum Schutz Kritischer Infrastrukturen, UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen.

Universität der Bundeswehr München (UniBw)
Die Universität der Bundeswehr München bildet Offiziere und Offiziersanwärter wissenschaftlich aus. Die Studiengänge umfassen aktuell unter anderem Informatik, Cybersicherheit, Mathematical Engineering und Wirtschaftsinformatik.

Die UniBw bildet Bw Personal wissenschaftlich aus und beheimatet CODE als fakultätsübergreifendes Forschungszentrum.[116]

Verbraucherzentrale Bundesverband (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 als unabhängige Instanz zudem Interessen der Verbraucher 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.[117]

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.

Am VCV beteiligt sind das BSI, Länder CERTs, sowie das LSI.[118]

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)
Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich entwickelt, forscht, unterstützt und berät die deutschen Sicherheitsbehörden in

116 Universität der Bundeswehr München, Hintergrundinformationen.

117 Bundesministerium für Justiz und Verbraucherschutz, Verbraucherzentralen.
Verbraucherzentrale Bundesverband, Häufige Fragen (FAQ).
Verbraucherzentrale Bundesverband, Über Uns.

118 Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).

den folgenden Bereichen: Digitale Forensik, Telekommunikationsüberwachung, Krypto- und Big-Data-Analyse. Darüber hinaus arbeitet ZITiS auch zu technischen Fragen im Bereich der Kriminalitätsbekämpfung, Gefahren- und Spionageabwehr.

ZITiS wurde vom BMI gegründet. Sie versorgt BKA, BfV und BPol mit ihrer Expertise. Sie ist auf dem Campus der UniBw angesiedelt und befindet sich so auch in geographischer Nähe zu CODE.[119]

Zentrum Cyber-Operationen (ZCO)
Das Zentrum Cyber-Operationen der Bundeswehr bündelt alle Fähigkeiten zur Planung, Vorbereitung, Führung und Durchführung von militärischen Cyberoperationen zur Aufklärung und Wirkung. Dies umfasst sowohl defensive als auch offensive Operationen. Zudem arbeitet das ZCO an dem Schutz der eigenen IT-Systeme. Im Fall einer IT-Krise kann das ZCO zudem zur Unterstützung des Kommandos Cyber- und Informationsraum (Kdo CIR) hinzugezogen werden. Das Zentrum ging im April 2018 aus dem Kommando Strategische Aufklärung hervor und ist diesem direkt unterstellt. Es besteht aus 100 Soldat:innen und zivilen Mitarbeiter:innen. Standort des ZCO ist die Tomburg-Kaserne in Rheinbach in Nordrhein-Westfalen.

Das ZCO ist Teil der Bw.[120]

Zollkriminalamt (ZKA)
Das Zollkriminalamt (ZKA) gehört zum Geschäftsbereich des Bundesministeriums der Finanzen und 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.[121]

119 Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Aufgaben & Ziele.

120 Bund, Zentrum Cyberoperationen (ZCO).
Bundeswehr, Das Zentrum Cyber-Operationen.

121 Der Zoll, Die Aufgaben des Zolls.

6. Erläuterung – Akteure auf Länderebene

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

- Die Länder-CERTs sind die Computer Emergency Response Teams der einzelnen Bundesländer. Diejenigen, die bereits aufgebaut sind, sind dabei an unterschiedlichen Stellen angegliedert:
- Das Bayern-CERT ist am LSI angesiedelt.
- Das hessische CERT ist mit der Gründung von H3C in dessen Bereich Cybersecurity aufgegangen, der alle Aufgaben des CERT wahrnimmt.
- Das CERT BWL (Baden-Württemberg) ist beim IT-Baden-Württemberg (BITBW) angesiedelt.
- Das CERT NRW liegt beim Landesbetrieb Information und Technik Nordrhein-Westfalen.
- Das SAX.CERT (Sachsen) ist an den Staatsbetrieb Sächsische Informatik Dienste angegliedert.
- Das N-CERT (Niedersachsen) ist beim Ministerium für Inneres und Sport angegliedert.
- Das CERT-rlp gehört zum Landesbetreib Daten und Information.
- Das CERT-Brandenburg wird vom Brandenburgischen IT-Dienstleister (ZIT-BB) betrieben.
- Das Berliner CERT wird vom IT-Dienstleistungszentrum Berlin (ITDZ Berlin) geführt.
- Die Länder Bremen, Schleswig-Holstein, Hamburg und Sachsen-Anhalt haben ein gemeinsames CERT Nord.
- Das CERT M-V wird vom Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ M-V) betrieben.
- Das CERT Saarland wird durch eine Vereinbarung beider Bundesländer vom CERT-rlp bereitgestellt.
- Das ThüringenCERT befindet sich derzeit im Aufbau.

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.[122]

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 Cyberwehr 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 Nationale Cyber-Abwehrzentrum des Bundes 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 wird beim Cyber-Allianz-Zentrum Bayern im Bayerischen Landesamt für Verfassungsschutz etabliert. 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.[123]

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

123 STMI Bayern, Bayern stärkt Cyberabwehr und Digitalfunk.
Tagesspiegel, Cyberabwehr: Neues Lagezentrum in Bayern geplant.
Bayernkurier, Bayern stärkt die Cyber-Abwehr.

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 Infrastruktur im Bereich Prävention und Abwehr elektronischer Angriffe. Das CAZ fungiert als zentrale staatliche Steuerungs- und Koordinierungsstelle in Bayern und vertraulicher Ansprechpartner für betroffene Institutionen: nach der forensischen Analyse und nachrichtendienstlicher Bewertung gibt es eine Antwort mit Handlungsempfehlungen. Außerdem kontaktiert es möglicherweise von einem ähnlichen Angriff betroffene Unternehmen oder Einrichtungen mit Informationen zu den Angriffsmustern (in anonymisierter Form). Das CAZ war die erste institutionelle Säule der 2013 ins Leben gerufenen „Initiative Cybersicherheit Bayern" des Bayerischen Staatsministeriums des Innern, für Sport und Integration.[124]

Cyber-Competence-Center (CCC) – Brandenburg
Das Cyber-Competence-Center wurde 2016 als neue Fachdienststelle im Landeskriminalamt Brandenburg eingerichtet, das personelle und fachliche Kompetenzen zur Bekämpfung und Aufklärung jeglicher Kriminalitätsbereich im Zusammenhang mit dem Internet bündeln soll. Es übernimmt sowohl präventive wie auch repressive Aufgaben und unterstützt Ermittlungen der Polizeidirektionen und -inspektionen zur Bekämpfung der Cyberkriminalität.

Dort wurde auch die ZAC für Wirtschaftsunternehmen und Behörden eingerichtet.[125]

Cyber Crime Competence Center Sachsen (SN4C)
2014 wurde das Cyber Crime Competence Center im Verantwortungsbereich des Landeskriminalamtes Sachsen gegründet. Es fokussiert sich auf die verschiedenen Kriminalitätsfelder, die mit dem Internet in Zusammenhang stehen, zum Beispiel rechtwidrige 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.

124 Bayerisches Landesamt für Verfassungsschutz, Cyber-Allianz-Zentrum Bayern (CAZ).

125 Polizei Brandenburg, Cyber-Competence-Center im Landeskriminalamt.

Das Center übernimmt die Aufgabenbereiche der Zentralen Ansprechstelle für die Wirtschaft.[126]

Cybercrime Competence Center (4C) – Sachsen-Anhalt
Das Competence Center wurde 2012 im Landeskriminalamt Sachsen-Anhalt eingerichtet und bündelt Spezialisten verschiedener Dezernate im Bereich der Cyberkriminalität. Die Mitarbeiter des Landeskriminalamtes werden dabei von Wissenschaftlern unterstützt, für die neue Stellen geschaffen wurden. Das Kompetenzzentrum soll sich landesweit um die komplizierteren Fälle kümmern und die Polizei bei einfacheren Betrugsfällen unterstützen. *Das Center ist auch Zentrale Ansprechstelle für die Wirtschaft.*[127]

Cybercrime-Kompetenzzentrum – Nordrhein-Westfalen
2011 wurde im Landeskriminalamt Nordrhein-Westfalen ein Cybercrime-Kompetenzzentrum eingerichtet, das Ermittlungskommissionen für herausragende Verfahren, Experten für Computerforensik, Telekommunikationsüberwachung, Auswertung, Analyse und Prävention sowie die Zentrale Internetrecherche und die Auswertestelle für Kinderpornografie beherbergt. *Dort ist auch die ZAC für die Wirtschaft angesiedelt.*[128]

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 aber der landesweite Aufbau regionaler Infrastrukturen für die Ersthilfe im Falle einer 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 im Anschluss, wenn gewünscht, Experten bereitstellt, 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

126 Sachsen.de, Cybercrime Competence Center Sachsen (SN4C).
Sachsen.de, Zentrale Ansprechstelle Cybercrime (ZAC) für Unternehmen, Behörden und Verbände des Freistaates Sachsen.

127 Hallelife.de, Sachsen-Anhalt startet Kompetenzzentrum gegen Internetkriminalität.

128 Polizei Nordrhein-Westfalen Landeskriminalamt, Das Cybercrime-Kompetenzzentrum beim LKA NRW.

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.[129]

Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken
Seit 2017 ist bei der Staatsanwaltschaft Saarbrücken ein Sonderdezernat „Cybercrime" angesiedelt, mit dem das saarländische Justizministerium der Kriminalität im Netz entgegentreten will. Das Dezernat soll mit dem Institut für Rechtsinformatik und dem CISPA Helmholtz Center for Information Security speziell geschult werden.[130]

Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern
Das Dezernat 45 des Landeskriminalamts in Mecklenburg-Vorpommern ermittelt mit Cybercrime-Spezialisten in solchen Fällen und beherbergt auch die mecklenburg-vorpommerische 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.[131]

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

129 Cyberwehr, Die Cyberwehr. Baden-Württemberg.de, Landesregierung initiiert „Cyberwehr Baden-Württemberg".

130 Juristisches Internetprojekt Saarbrücken, Neues Dezernat „Cybercrime" bei der Staatsanwaltschaft Saarbrücken.

131 Landeskriminalamt Mecklenburg-Vorpommern, 10. Sicherheitstag im DVZ. Landespolizei Mecklenburg-Vorpommern, LKA-MV: Internationaler Ermittlungserfolg gegen Kinderpornografieplattform im Darknet.

oder organisierten Kriminalität“. Das Dezernat bildet außerdem die ZAC für Wirtschaftsunternehmen.

Das LKA ist seit 2014 Mitglied der Allianz für Cyber-Sicherheit.[132]

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.[133]

Dezernat LPP 222 Cybercrime – Saarland
Die saarländische Kriminalpolizei hat 2013 mit dem Dezernat eine spezialisierte Cybercrime-Dienststelle eingerichtet, die sich mit besonders schwerwiegenden Fällen auseinandersetzt, 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.[134]

EMERGE IoT – Mecklenburg-Vorpommern
EMERGE IoT ist ein Kooperationsprojekt (gefördert durch den Fonds für die Innere Sicherheit der Europäischen Union), das 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-Vorpommerns und die Universität Rostock.[135]

132 Polizei Rheinland-Pfalz, Aufgaben des Dezernates Cybercrime.

133 Heise Online, Cybercrime: Neue Herausforderungen für Thüringer LKA.
Thueringen.de, Internetkriminellen gemeinsam mit den Unternehmen das Handwerk legen.

134 sol.de, Saar-Kripo eröffnet neue „Cybercrime“-Dienststelle. (Website entfernt)

135 Universität Rostock, Universität Rostock unterstützt das Landeskriminalamt Mecklenburg-Vorpommern in Sachen Cyber-Kriminalitätsbekämpfung.

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.[136]

Hessen Cyber Competence Center (Hessen3C)
Das Hessen Cyber Competence Center ist eine Kompetenzstelle, die eine interdisziplinäre Zusammenarbeit und institutionalisierte Kooperation staatlicher Behörden in Hessen ermöglichen soll. Es ging aus der Kompetenzstelle Cybersicherheit, einer Stabstelle im Hessischen Innenministerium, hervor, das vollständig in Hessen3C aufgegangen ist. Hessen3Cs 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 zentraler 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 Cybersicherheit zur Verfügung gestellt werden. Das Hessen3C betreibt seit einer Einführung das CERT-Hessen und leitet das IT-Krisenmanagement der Landesverwaltung.[137]

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 maßgeblich ausgeweitet. ATHENE, ehemals CRISP, wurde erst jüngst in das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE umgewandelt. Seit Anfang 2020 ist es unter dem „Dach der Frau-

136 Polizei Hamburg, Zentrale Ansprechstelle Cybercrime (ZAC).

137 Hessisches Ministerium des Innern und für Sport, Hessen3C.
Emailaustausch mit Vertreter:innen des Hessen Cyber Competence Center im November 2019.

enhofer-Gesellschaft an den beiden Darmstädter Instituten SIT und IGD unter Beteiligung der Technischen Universität Darmstadt und der Hochschule Darmstadt“[138]angesiedelt.

Die drei Kompetenz- und Forschungszentren für IT-Sicherheit werden durch das BMBF gefördert.[139]

Kompetenzzentrum Cybercrime – Bayern
Das Kompetenzzentrum Cybercrime (Dezernat 54) wurde 2014 beim Landeskriminalamt Bayern eingerichtet. Eine seiner Hauptaufgaben ist es, in Krisenstabsübungen mit Unternehmen und Behörden, die für den Erhalt der öffentlichen Ordnung unverzichtbar sind, den Ernstfall, beispielsweise eines Hackerangriffs, zu testen. Darüber hinaus nimmt es sich solcher Fälle von Cyberkriminalität an, die überregionale Bedeutung haben und von den örtlichen Polizeidienststellen nicht bearbeitet werden können.[140]

Landesamt für Sicherheit in der Informationstechnik Bayern (LSI)
Das Landesamt für Sicherheit in der Informationstechnik Bayern hat sich mit seiner Gründung im Dezember 2017 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.[141]

Netzverweis.de – Mecklenburg-Vorpommern
Der Internetauftritt netzverweis.de ist eine gemeinsame Initiative des Landeskriminalamtes Mecklenburg-Vormpommern und der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH unter der Schirmherrschaft des Ministeriums für Inneres und Sport. Sie fungiert als Online-Meldestelle, über die Bürger:innen, wenn gewünscht anonym, Hinweise zum Thema Internetkriminalität angeben können, *die dann an das LKA Mecklenburg-Vorpommerns weitergeleitet werden, dort von Spezialisten bearbeitet und gegebenenfalls auch verfolgt.*[142]

138 Bundesministerium für Bildung und Forschung, ATHENE: Großer Schritt zu mehr IT-Sicherheit.

139 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

140 Heise Online, Bayern: Schwierigkeiten beim Kampf gegen Internetkriminalität.
Julian Hans, Die Polizei, Dein Freund und Hacker.

141 Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.

142 Netzverweis, Online-Meldestelle.

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.[143]

Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus
Seit 2000 ist bei der Staatsanwaltschaft Cottbus die brandenburgische Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer und Datennetzkriminalität eingerichtet.[144]

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.[145]

Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin
Seit 2015 besteht in der Staatsanwaltschaft Berlin eine Spezialabteilung zur Cyberkriminalität. Schwerpunkt der Abteilung ist der Waren- und Warenkreditbetrug im Zusammenhang mit Online-Handel.[146]

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 gemeinsam mit IT-Spezialisten.

Auf Länderebene sind die ZAC meist beim LKA angesiedelt, gegebenenfalls auch bei den dort bereits aufgebauten Cyber-Kompetenzzentren (siehe Be-

143 Justiz Online in Mecklenburg-Vorpommern, Zuständigkeit.

144 Staatsanwaltschaft Cottbus, Schwerpunktstaatsanwaltschaft.

145 Sicherheitskooperation Cybercrime, Aktivitäten.
Sicherheitskooperation Cybercrime, Die Kooperation.

146 Diana Nadeborn, Berliner Staatsanwaltschaft rüstet auf gegen Cyberkriminalität.

schreibungen der Kompetenzzentren). Die ZAC auf Bundesebene ist unter anderem bei der BPol angesiedelt.[147]

Zentralstelle Cybercrime Bayern (ZCB)
Seit 2015 besteht die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, deren Aufgabe herausgehobene Ermittlungsverfahren im Bereich der Cyberkriminalität in ganz Bayern sind. In Abstimmung mit dem Bayerischen Justizministerium arbeitet die Zentralstelle auch zu verfahrensunabhängigen Fragestellungen im Bereich 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 AfCS.[148]

Zentralstelle Cybercrime Sachsen (ZCS)
Die seit 2016 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.[149]

Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität – Baden-Württemberg
Im Juli 2011 wurde bei der Generalstaatsanwaltschaft Stuttgart eine Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität 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

147 Der Polizeipräsident in Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.
Bundeskriminalamt, Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft.

148 Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB).
Bundesamt für Sicherheit in der Informationstechnik, Teilnehmerliste der Allianz für Cyber-Sicherheit.

149 Staatsministerium der Justiz, Sächsisches Justizministerialblatt Nr. 5/2018.
MDR Sachsen, Sachsen fehlen Polizisten fürs Netz. (Website entfernt)

Ermittlungsinstrumente 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.[150]

Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) – Hessen

Die Zentralstelle wurde 2010 als Außenstelle der Generalstaatsanwaltschaft Frankfurt (a.M.) in Gießen errichtet. Sie ist operative Zentralstelle bei besonders aufwändigen und umfangreichen Ermittlungsverfahren in den Bereichen, Kinderpornographie und sexueller Missbrauch von Kindern mit Bezug zum Internet, Darknet-Kriminalität und anderer Cyberkriminalität.

Die ZIT ist erster Ansprechpartner des BKAs für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland und bei Massenverfahren gegen mehrere Tatverdächtige deutschlandweit. Sie ist außerdem Gründungsmitglied im Judicial Cybercrime Network.[151]

Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)

Die Zentral- und Ansprechstelle Cybercrime in NRW (nicht zu verwechseln mit der nordrhein-westfälischen Zentralen Ansprechstelle Cybercrime der Polizei für Wirtschaftsunternehmen, in der Grafik als ZACs, die beim Landeskriminalamt angesiedelt ist) ist seit April 2016 bei der Staatsanwaltschaft Köln die landesweit zuständige Cybercrime-Einheit der Justiz. Sie ist bundesweit die größte Cybercrime-Einheit der Justiz, ihr obliegt die Verfahrensführung in herausgehobenen Ermittlungsverfahren der Cyberkriminalität, die Wahrnehmung der Aufgaben einer zentralen 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.[152]

150 Ministerium der Justiz und für Europa Baden-Württemberg, Zentralstelle für die Bekämpfung von informations- und Kommunikationskriminalität eingerichtet.

151 Staatsanwaltschaften Hessen, Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT).

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

7. 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. Die Damen und Herren dort sind Montag bis Freitag von 8:00 Uhr bis 18:00 Uhr unter 0800 274 1000 erreichbar.[153]

IT-Sicherheit versus Cybersicherheit: IT-Sicherheit hat eine relativ enge Definition. Diese folgt dem; der Schutz der Vertraulichkeit *(Confidentiality)*, Integrität *(Integrity)* und Verfügbarkeit *(Availability)* von Daten.[154] Im Verlauf der letzten Dekade nahm vor allem im anglo-amerikanischen, aber auch europäischen Raum der Gebrauch des Wortes im Vergleich zu IT-Sicherheit zu. *Cybersicherheit* ist breiter angelegt als *IT-Sicherheit* und umfasst zusätzlich auch sozio-kulturelle, politische, rechtliche und weitere Dimensionen.[155]

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 offensiven Cyberwerkzeugen zur Herstellung der öffentlichen Sicherheit verstanden – unter anderem durch den *Einsatz des Bundestrojaners*[156] oder *Aktiver Cyberabwehr.*[157]

Es heißt jetzt Cybersicherheit ohne Bindestrich. Die Bundesregierung hat bis circa 2016/2017 bei Begriffen mit den Bindestrich verwendet, dies geht unter anderem aus dem Glossar der *Cyber-Sicherheitsstrategie für Deutschland 2016* hervor.[158] Spätestens seit 2018 werden Begriff mit Cyber zusammengeschrieben, wie die Benennung der neuen Referate in der Abteilung Cyber- und Informationssicherheit im Bundesministerium des Innern, für

153 Bundesamt für Sicherheit in der Informationstechnik, BSI für Bürger.

154 Bundesamt für Sicherheit in der Informationstechnik, Glossar.

155 Sven Herpig, Anti-War and the Cyber Triangle.

156 Netzpolitik.org, Bundestrojaner.

157 Sven Herpig, Hackback ist nicht gleich Hackback.

158 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.

Bau und Heimat[159] oder der *Agentur für Innovation in der Cybersicherheit* belegen.[160]

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. Erstellung präventiver Handlungsempfehlungen zur Schadensvermeidung, Hinweisen auf Schwachstellen in Hardware- und Software-Produkten, Unterstützung bei der Reaktion auf IT-Sicherheitsvorfälle oder Empfehlungen zur Schadensbegrenzung oder -beseitigung. Inhaltlich gibt es keinen 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 FIRST Dachverband vertreten.[161]

Cyberveranstaltungen. Mit der wachsenden Relevanz des Themas IT- und Cybersicherheitspolitik steigt auch die Anzahl der Veranstaltungen in dem Bereich. Schon allein für Deutschland ist es schwer die Vielzahl an Konferenzen und weiteren Ereignissen zu überblicken. Um hier etwas mehr Übersicht zu schaffen, hat die Stiftung Neue Verantwortung hierfür einen entsprechenden Kalender online gestellt. Er ist unter cyber-veranstaltungen.de 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.

159 Bundesministerium des Innern, Organisationsplan.

160 Bundesministerium der Verteidigung, Technologiesouveränität erlangen – die neue Cyberagentur.

161 FIRST, About FIRST.
Bundesamt für Sicherheit in der Informationstechnik, CERT-Bund.
Carnegie Mellon University, Software Engineering Institute.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autor:innen

Sven Herpig

Sven Herpig ist Leiter für Internationale Cyber-Sicherheitspolitik. Hierzu gehört das transatlantische Expert:innen-Netzwerk Transatlantic Cyber Forums (TCF), das von der Europäischen Kommission geförderte EU Cyber Direct (EUCD) und die dauerhafte Analyse der deutschen Innen-, Sicherheits- und Verteidigungspolitik im Cyber-Raum.

Bei der SNV befasst Sven sich vorrangig mit der deutschen Cyber-Sicherheitsarchitektur, 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.

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

Rebecca Beigel

Rebecca Beigel ist Projektmanagerin für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung. Ihre Arbeitsschwerpunkte liegen auf der deutschen Cybersicherheitspolitik sowie auf nationalen Cybersicherheitsstrategien.

So erreichen Sie die Autorin
Rebecca Beigel
Projektmanagerin Internationale Cybersicherheitspolitik
rbeigel@stiftung-nv.de
+49 (0) 30 403 676 983

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

Free Download:
www.stiftung-nv.de